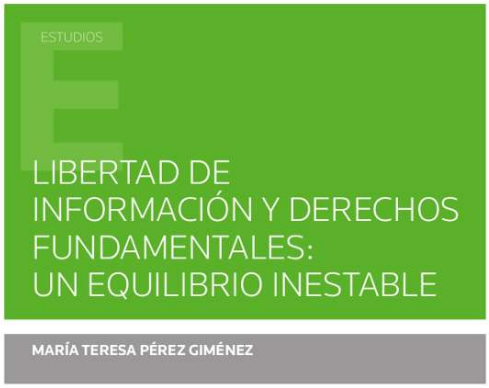
ESTUDIOS
LIBERTAD DE INFORMACIÓN Y DERECHOS FUNDAMENTALES: UN EQUILIBRIO INESTABLE
MARÍA TERESA PÉREZ GIMÉNEZ
PRÓLOGO DE CARLOS LASARTE ÁLVAREZ
THOMSON REUTERS
ARANZADI

Índice sistemático

CAPÍTULO III

Protección de datos y libertad de información

1.CONSIDERACIONES GENERALES: EL DERECHO A LA INTIMIDAD Y EL DERECHO A LA PROTECCIÓN DE DATOS

Como veíamos en el capítulo anterior, Internet ha supuesto una verdadera revolución en el mundo de la información; esto ha provocado que la mayoría de las industrias de la comunicación se estén transformando y redefiniendo, por razón de su influencia, ya que nos encontramos en un ámbito de poder casi ilimitado en el que las coordenadas tiempo y espacio son muy tenues.

El problema se plantea porque al mismo tiempo que apenas existen límites materiales a la comunicación, lo que refuerza los derechos a la libertad de información y de expresión, la puesta en práctica y el auge de las nuevas tecnologías hacen frágiles esas y otras libertades y derechos que se ven desafiados por complejos sistemas de control de datos; fundamentalmente el derecho a la intimidad y a la privacidad, pero también los derechos a la imagen y al honor.

Volvemos a situarnos en el punto de salida, de modo que conociendo cuáles son los límites que se imponen a la libertad de información en un Estado democrático como el nuestro, vamos a analizar de qué manera estos afectan a la misma, en un ámbito absolutamente diferente y muchísimo más evolucionado que aquél para el que fueron inicialmente pensados; ello requiere indagar cuáles son las coordenadas en las que debe desenvolverse la actuación del periodismo y los medios de comunicación en la actualidad y estudiar en qué medida las mismas se ven afectadas por la nueva regulación sobre protección de datos.

Para conseguir lo anterior, se examinarán los principios del nuevo marco europeo para la protección de datos con la finalidad de exponer con claridad el concepto y contenido de este nuevo derecho y su repercusión en el ámbito de la información; como paso previo se hace necesario distinguirlo del derecho a la intimidad, que ya hemos analizado, para lo que tendremos en cuenta que esta materia ya ha sido abordada por el Tribunal Constitucional.

Se puede considerar que va con los tiempos que vivimos el hecho de que en los últimos años se haya generado tanta información como en toda la historia de la humanidad; pero la preocupación no es ésta. Lo que intranquiliza es que las tecnologías actuales permiten penetrar en la *caja negra* que constituye el razonamiento propio de cada individuo, prisionero de las huellas que ha dejado, pudiéndose establecer así el modo en que cada persona realiza sus operaciones y confecciona conclusiones, incluso predictivas. Si la información es poder, su tratamiento y control lo es en grado sumo. En atención a lo anterior, lo jurídico debe tener en toda esta materia un papel destacado (173).

La sentencia del Tribunal Constitucional de 30 de noviembre de 2000 (174) realiza un análisis profundo de lo que tienen en común pero también de las diferencias entre el derecho a la intimidad y a la protección de datos. Su contenido es muy interesante; por ello y porque nos servirá de base y fundamento de todo lo que vendrá después, dedicaré las siguientes páginas a esquematizar los argumentos que contiene.

Naturaleza jurídica: Se trata de dos derechos recogidos en la Constitución como derechos fundamentales; por una parte, el derecho al honor, intimidad personal y familiar e imagen en el artículo 18.1 y, por otra parte, el artículo 18.4 establece que 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. Es en sí mismo un derecho o libertad fundamental frente a potenciales agresiones provenientes de un uso ilegítimo del tratamiento mecanizado de datos frente a la libertad informática (175).

Razón de su inclusión en la Constitución: Los avances tecnológicos entrañan graves riesgos para la incolumidad de la esfera privada e íntima de los individuos pues la informática ofrece infinitas posibilidades para el tratamiento, almacenamiento y entrecruzamiento de datos personales.

Insuficiencia del artículo 18.1 CE: El derecho a la intimidad no aporta por sí solo una protección suficiente frente a la nueva realidad derivada del progreso tecnológico. El legislador quiso garantizar mediante el actual artículo 18.4 no sólo un ámbito de protección específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el artículo 18.1. Contiene un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos.

Derecho autónomo: Existe un específico derecho fundamental a la protección de datos personales reconocido por nuestra Constitución a partir del derecho a la intimidad del artículo 18.1 y del mandato del artículo 18.4 (176), cuyo sentido y alcance han de determinarse, entendiendo que la protección de datos va referida a la persona física y no a la jurídica (177), siendo su ámbito de aplicación los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento y toda modalidad de uso posterior de esos datos por los sectores público y privado.

Concepto: Se trata de un derecho de control sobre los datos relativos a la propia persona, pues la garantía de su vida privada y su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho a la intimidad.

Semejanzas y diferencias: Ambos derechos comparten el objetivo de ofrecer una eficaz protección constitucional de la vida personal y familiar. Difieren en su distinta función, objeto y contenido.

Función: La función del derecho a la intimidad es proteger frente a cualquier invasión en el ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad. El derecho a la protección de datos persigue garantizar un poder de control sobre sus datos personales, sobre su uso y destino para impedir su tráfico ilícito y lesivo para la dignidad y derechos del afectado.

Objeto: Su objeto es más amplio que el de la intimidad pues extiende su garantía no sólo a la intimidad en la dimensión del artículo 18.1, sino a cualquier dato que sea relevante o tenga incidencia en el ejercicio de cualquier derecho de la persona. No se reduce a los datos íntimos sino a cualquier tipo de dato personal cuyo conocimiento o empleo por terceros pueda afectar a sus derechos. Nos referimos a cualesquiera datos que permitan la identificación de la persona pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole; también si sirven para cualquier otra utilidad que, en determinadas circunstancias, pueda constituir una amenaza para el individuo y no necesariamente una violación de la vida privada.

Contenido: En cuanto a su contenido también difieren. El artículo 18.1 confiere el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido. El derecho a la protección de datos, sin embargo, atribuye un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros determinados deberes; así:

–Que se requiera el previo consentimiento para la recogida y uso de los datos personales; el titular de los datos tiene la facultad de consentir o no su comunicación o cesión a terceros; garantía necesaria para salvaguardar su intimidad y poder ejercer libremente sus derechos.

–El derecho a saber y ser informado sobre el destino y uso de esos datos. El poder de disposición que se

le atribuye no tendría valor si el afectado desconoce qué datos son los que se poseen, quiénes los poseen y con qué fin.

–El derecho a acceder, rectificar y cancelar esos datos. Comprende entre otros aspectos la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención.

Autodeterminación informativa: En conclusión, su contenido fundamental consiste en el poder de disposición y control sobre sus datos que faculta a la persona para decidir cuáles proporciona a terceros, el Estado o particulares, y cuáles puede este tercero recabar, pudiendo oponerse a esa posesión o uso; exigiendo además su rectificación o cancelación. Es una garantía fundamental para el ciudadano poder controlar el flujo de información relativa a su persona, para lo que resulta indispensable conocer y consentir su almacenamiento y su uso.

Límites: Ninguno de los dos derechos es absoluto; por ello, la Ley puede imponerles límites con el fin de proteger otros derechos constitucionales o bienes constitucionalmente protegidos, siempre que esos límites sean necesarios, proporcionados y respetuosos con el contenido esencial del derecho, evitando hacerlo impracticable (178).

2.NUEVO MARCO EUROPEO SOBRE PROTECCIÓN DE DATOS PERSONALES: EL REGLAMENTO EUROPEO Y LA LO 3/2018

El Reglamento UE 2016/679 que entró en vigor el 25 de mayo de 2016, si bien su plena aplicación se produce desde el 25 de mayo de 2018, vino a proteger y velar por el correcto tratamiento de los datos personales de los usuarios permitiendo su libre circulación en la Unión Europea.

Su intención fundamental ha sido sentar los cimientos de una normativa única en materia de privacidad que se acomode a la tecnología hoy presente, pues si bien considera que los objetivos y principios de la derogada Directiva 95/46/CE siguen siendo válidos, la fragmentación en su aplicación ha generado inseguridad jurídica y una percepción generalizada de que existen riesgos importantes para las personas físicas, en relación con las actividades *on line,* que deben ser afrontados.

La adaptación del Reglamento a la normativa española implicó la elaboración de una nueva Ley orgánica que sustituyó a la anterior con la finalidad de procurar una mayor seguridad jurídica, integrando el ordenamiento europeo en el interno de manera suficientemente clara y pública, lo que permite su pleno conocimiento tanto por los operadores jurídicos como por los ciudadanos. Se trata, en definitiva, teniendo en cuenta el carácter directamente aplicable de los reglamentos de la Unión Europea, de una norma interna complementaria que hace plenamente efectiva su aplicación, desarrollándolo y completándolo. Pero, además, es su objetivo garantizar los derechos digitales de la ciudadanía (179).

En atención a lo anterior, el Reglamento será de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un *fichero* (180)*,* entendiendo por tal todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica (181) y tanto si está integrado en una base de datos electrónica o informática como si se encuentra en formato papel.

Con base en lo anterior, el Reglamento será de aplicación tanto a las empresas, responsables o encargados del tratamiento de datos con domicilio social en la Unión Europea, con independencia de que el tratamiento de aquéllos tenga lugar dentro o fuera de ella; como cuando se trate de actividades de un responsable o encargado no establecido en la Unión pero que esté referido a datos personales de interesados que sí residan en ella (182).

Aclarado lo anterior, se hace necesario abordar cuáles han sido las principales transformaciones que ha introducido el nuevo Reglamento Europeo; podemos afirmar que las claves de la actual regulación se centran en el deber de información, el consentimiento, la transparencia, la seguridad, el análisis del impacto de privacidad y garantizar, en definitiva, los derechos de los ciudadanos en relación con la protección de su privacidad.

Los datos personales deben ser tratados de manera lícita, leal y transparente; deben ser recogidos para fines determinados, explícitos y legítimos y no ser tratados posteriormente de manera incompatible con dichos fines; serán adecuados, pertinentes y limitados a lo necesario en función de los fines para los que son tratados; serán exactos y se actualizarán, pues si son inexactos con respecto a los fines para los que se tratan deberán ser suprimidos o rectificados sin dilación; se mantendrán durante el tiempo estrictamente necesario en función de los fines para los que se han requerido y se tratarán de manera que se garantice la seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental mediante la aplicación de medidas técnicas y organizativas apropiadas (183). Para que todo esto se cumpla, el responsable del tratamiento debe tener una actitud proactiva, consciente y diligente, pues no sólo ha de cumplirlo sino que también ha de ser capaz de demostrarlo (184).

Siendo objetivo prioritario fortalecer el derecho a la protección de datos y haciéndolo uniforme en los Estados miembros, el Reglamento que es consciente del impacto de las nuevas tecnologías, refuerza el control que cada interesado puede tener sobre sus propios datos, aumentando la transparencia (185). Para ello se adoptan las siguientes medidas:

A)LOS CONOCIDOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN SE COMPLETAN CON LOS DERECHOS DE SUPRESIÓN, OPOSICIÓN A LA ELABORACIÓN DE PERFILES, LIMITACIÓN DEL TRATAMIENTO Y PORTABILIDAD DE DATOS

El derecho de supresión, también conocido como *derecho al olvido* (186), se recoge en el artículo 17 del Reglamento y en base al mismo el interesado puede obtener sin dilaciones indebidas la supresión de los datos personales que le conciernan si estos datos ya no son necesarios en relación con los fines para los que fueron recogidos, si retira su consentimiento, si hubieran sido tratados ilícitamente, si deben suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión, o si se han obtenido en relación con la oferta de servicios de la sociedad de la información a menores que no reúnen los requisitos de edad o complemento de capacidad establecidos en el artículo 8 que vimos en el capítulo anterior. Para hacerlo operativo, el responsable del tratamiento debe adoptar medidas razonables, incluidas de carácter técnico, para informar de esta solicitud a quienes estén tratando los datos personales.

Como paso previo, el responsable del tratamiento estará obligado al *bloqueo de los datos* (187) que supone la identificación y reserva de los mismos de manera que se impida su tratamiento y visualización, salvo que fuera para ponerlos a disposición de la autoridad judicial, Ministerio Fiscal o Administraciones públicas, en el marco de la exigencia de posibles responsabilidades y sólo por el plazo de prescripción de las acciones, transcurrido el cual se procederá a su destrucción.

No obstante, este derecho no se aplicará cuando el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública, si se trata de fines de investigación científica, histórica o estadística, si es necesario para la formulación, el ejercicio o la defensa de reclamaciones o para ejercer los derechos a la libertad de expresión e información, cuestión que trataremos en un epígrafe posterior.

Por su parte el *derecho a la portabilidad* (188) de los datos consiste en que el interesado tendrá derecho a recibir los datos personales propios que haya facilitado a un responsable del tratamiento, en un formato

estructurado, de uso común y lectura mecánica para transmitírselos a otro responsable del tratamiento; sin que el primero pueda negarse a ello cuando ese tratamiento estuvo basado en el consentimiento y se efectuó por medios automatizados. Siendo técnicamente posible, la transmisión se realizará directamente de responsable a responsable. Esta operación en ningún caso podrá afectar a derechos y libertades de otros.

El derecho de oposición, por su parte, implica la posibilidad de oponerse en cualquier momento a que datos personales sean objeto de un tratamiento basado en el consentimiento dado con anterioridad, incluida la elaboración de perfiles (189); destacando además que cuando el consentimiento se solicita para una pluralidad de finalidades es preciso que conste de manera específica e inequívoca que se otorga para todas ellas. El responsable del tratamiento actuará en consecuencia salvo que pueda acreditar motivos legítimos e imperiosos para que el tratamiento deba prevalecer frente a los derechos y libertades del interesado.

B)EL MODO DE OBTENER EL CONSENTIMIENTO (190)

Esta es una de las cuestiones más relevantes pues se pretende que el titular del mismo tenga la misma libertad para darlo que para retirarlo, teniendo en cuenta que si lo presta será porque ha sido perfecta y previamente informado y quien lo recoge debe ser capaz de demostrar que efectivamente éste ha existido, dado que el consentimiento ha de ser expreso e inequívoco y como cualquier manifestación de voluntad debe ser libre y específica. Para que el consentimiento se considere informado, quien lo da debe conocer como mínimo los fines del tratamiento a los cuales están destinados sus datos, la base jurídica del mismo, la referencia al ejercicio de sus derechos y la identidad del responsable del tratamiento (191).

No se admite con esta nueva regulación el silencio o que sea tácito porque el titular de los derechos no se oponga expresamente al mismo; puede tratarse de una declaración o de una clara acción afirmativa. La solicitud del consentimiento debe distinguirse tajantemente de cualquier otro asunto y se ha de utilizar un lenguaje claro y sencillo que evite confusiones, pues por ejemplo, no se puede supeditar la ejecución de un contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no tengan ningún vínculo con la relación contractual en cuestión (192). El cumplimiento del deber de información exige evitar las fórmulas especialmente farragosas y que incorporan remisiones a textos legales.

Y no sólo en el ámbito del tratamiento de los datos, sino también en el de la cesión o transferencia de aquéllos es necesario el consentimiento, aunque éste se obtenga en un mismo acto o momento para ambas actividades, siempre que se especifique y se informe rotundamente al respecto (193); por lo que el consentimiento además de inequívoco, en estos casos ha de ser explícito (194).

Si el consentimiento tácito se hubiera prestado con anterioridad a la entrada en vigor del Reglamento, deberá adaptarse para ser acorde a la nueva normativa. Para ello, lo más adecuado sería hacer una nueva solicitud de consentimiento; si bien sería posible mantenerlo en caso de existir algún interés legítimo que lo sostuviera, aunque esto dependerá de cada caso concreto lo que exigirá la ponderación de las circunstancias específicas del mismo (195).

C)LA EVALUACIÓN DEL IMPACTO (196)

Se trata de identificar los riesgos que pueden afectar a la privacidad; de modo que si un tratamiento de datos, sobre todo porque utiliza nuevas tecnologías, por su naturaleza, alcance o fines, puede entrañar un alto riesgo para los derechos y libertades, el responsable debe realizar antes del tratamiento una evaluación del impacto que tendrá en la protección de los datos personales. El responsable del tratamiento, que puede llevar a cabo esta actuación asistido por personal interno o externo, puede recabar para ello el asesoramiento del delegado de protección de datos. Se trata de adoptar las medidas de prevención adecuadas para la protección del

usuario frente a abusos en el tratamiento de sus datos y así poder asegurar los principios de protección, vistos anteriormente, garantizando los derechos y libertades de los interesados.

La evaluación debe incluir la descripción sistemática de la actividad de tratamiento prevista; la evaluación de la necesidad y proporcionalidad del tratamiento en relación con su finalidad; la evaluación de los riesgos y las medidas de seguridad y garantías previstas para afrontarlos. El análisis del riesgo puede variar en función de los tipos de tratamiento, la cantidad y variedad de tratamientos que realice una misma organización, la naturaleza de los datos y el número de interesados afectados.

Tras ello, se elaborará un informe de conclusiones con el resultado obtenido y el plan de actuación que se llevará a cabo en el que se incluirán las medidas de control que se deben implantar para poder gestionar adecuadamente los riesgos identificados. Si la evaluación muestra que las operaciones de tratamiento entrañan un alto riesgo que no se puede mitigar en términos de tecnología disponible y costes de aplicación, se deberá consultar con la autoridad de control antes del tratamiento.

Toda esta actuación se debe llevar a cabo de manera objetiva para que sea posible concebir y ejecutar un plan de acción efectivo y que consiga el fin de protección que se persigue. A ello se suele añadir una actividad de supervisión y revisión englobable en un proceso de mejora continua.

D)PRIVACIDAD POR DEFECTO Y PRIVACIDAD DESDE EL DISEÑO (197)

La primera de ellas implica que el responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas para garantizar que por defecto sólo sean objeto de tratamiento los datos personales necesarios para los fines específicos del tratamiento. Se trata de una obligación aplicable tanto a la cantidad de datos recogidos como a su extensión, plazo de conservación y accesibilidad.

La segunda tiene por finalidad aplicar de forma efectiva los principios de protección de datos integrando las garantías necesarias desde el principio, de modo que se tiene en cuenta la privacidad en todo el ciclo desde que se recogen los datos y hasta que se cancelan. El objetivo, en ambos casos, es garantizar que los datos no sean accesibles a un número indeterminado de personas sin la intervención activa del interesado y lo que es más importante, se colabora en la cultura de la protección al obligar a las empresas a actualizar sus procesos internos para adaptarse a estos requerimientos. Son, en definitiva, medidas de responsabilidad proactiva.

E)EL DELEGADO DE PROTECCIÓN DE DATOS (198)

Se trata de una de las novedades que incorpora el Reglamento. Nos referimos a la persona, física o jurídica, responsable de supervisar de manera independiente el respeto de las normas sobre protección de datos. Podrá formar parte de la empresa en cuestión o bien ser un servicio externo. Para su designación se atenderá a sus cualidades profesionales y en particular el conocimiento especializado del Derecho y la práctica en esta materia; también a su capacidad para desempeñar las funciones que le corresponden (199).

Una vez nombrado, los responsables y encargados del tratamiento comunicarán en el plazo de 10 días a la Agencia Española de protección de datos, o bien a las autoridades autonómicas las designaciones, nombramientos y ceses de los mismos, para que puedan mantener una lista actualizada accesible por medios electrónicos.

Entre sus funciones destacan la de información y asesoramiento, entre otras cosas, en la evaluación del impacto; supervisión del cumplimiento del Reglamento; cooperación con la autoridad de control, actuando como interlocutor ante la Agencia Española de Protección de datos y las autoridades autonómicas, la realización de consultas y emitir recomendaciones. Todas ellas, deberá realizarlas prestando la debida atención a los riesgos

asociados a las operaciones de tratamiento en función de su naturaleza, alcance, contexto y fines. No obstante, podrá desempeñar otras funciones y cometidos siempre que ello no genere conflictos de intereses.

Para mantener su independencia, se establecen una serie de obligaciones para el responsable y el encargado del tratamiento; así, garantizar que participará de forma adecuada y en tiempo oportuno en las cuestiones que le atañen, le facilitarán los recursos necesarios para el desempeño de las mismas y el acceso a los datos y operaciones de tratamiento. No deben darle ninguna instrucción en lo que respecta al desempeño de dichas funciones y no podrá ser ni sancionado ni destituido por ellos, a no ser que incurra en dolo o negligencia grave; su rendición de cuentas se llevará a cabo directamente al más alto nivel jerárquico del responsable o encargado.

Los interesados podrán contactar con él en relación con todo lo relativo al tratamiento de sus datos personales y al ejercicio de sus derechos y también en el caso de plantear alguna reclamación con carácter previo a su presentación ante la Agencia española de protección de datos o las autoridades autonómicas.

Se trata pues, de una de las figuras clave del Reglamento como garante del cumplimiento de la nueva normativa, si bien la responsabilidad sobre dicho cumplimiento recae en el responsable o encargado; por esta razón, si el delegado de protección de datos apreciara la existencia de alguna vulneración relevante de la protección de datos deberá documentarla y comunicarla inmediatamente a aquéllos.

F)LIMITACIONES (200)

Todo tratamiento de datos debe apoyarse en una base que lo legitime. El Reglamento, en su artículo 6, considera como tales el consentimiento, una relación contractual, el cumplimiento de una obligación legal para el responsable, el interés público o el ejercicio de los poderes públicos o intereses legítimos prevalentes del responsable o terceros (201).

Existiendo esa base jurídica, el mecanismo de protección se pone en marcha si bien el derecho a la protección de datos se puede limitar a través de medidas legislativas siempre que se respeten en lo esencial los derechos y libertades fundamentales y se trate de una medida necesaria y proporcionada para salvaguardar en una sociedad democrática la seguridad del Estado, la defensa, la seguridad pública, la protección de la independencia judicial, la prevención, investigación y enjuiciamiento de infracciones de normas deontológicas en profesiones reguladas, la protección del interesado y la ejecución de demandas civiles (202).

En cualquier caso, si existen estas limitaciones, la medida legislativa que las adopte deberá contener como mínimo la finalidad del tratamiento, categorías de datos personales de que se trate, alcance de las limitaciones para evitar accesos o transferencias ilícitos o abusivos, los plazos de conservación y garantías aplicables, los riesgos que se perciben para los derechos y libertades y el derecho de los interesados a ser informados sobre la limitación salvo si fuera perjudicial a los fines de ésta.

G)SEGURIDAD DE LOS DATOS PERSONALES. ANÁLISIS DE RIESGOS (203)

El responsable y el encargado del tratamiento deben aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que presente el tratamiento de los datos (204); de igual modo, tomarán medidas para garantizar que cualquier persona que bajo su autoridad tenga acceso a datos personales sólo pueda tratarlos siguiendo sus instrucciones, salvo que exista alguna norma que establezca lo contrario.

En caso de violación de la seguridad de los datos personales, bien porque se ocasione la destrucción, pérdida o alteración accidental o ilícita de los mismos o se produzca la comunicación o acceso no autorizados a dichos

datos, el encargado del tratamiento notificará sin dilación al responsable del tratamiento esta brecha de seguridad y éste la notificará a su vez a la autoridad de control competente a más tardar 72 horas después de tener constancia de ella. En la notificación se describirá su naturaleza, número de interesados afectados, datos del delegado de protección de datos, consecuencias previsibles, medidas propuestas y adoptadas.

Si esa violación genera además un alto riesgo para los derechos y libertades de las personas físicas, se debe comunicar también al interesado a la mayor brevedad posible, describiendo en un lenguaje claro y sencillo lo acontecido.

H)CÓDIGOS DE CONDUCTA (205)

Se promueve la elaboración de códigos de conducta, como mecanismos de autorregulación, destinados a contribuir a la correcta aplicación del Reglamento, teniendo en cuenta las características especiales de los distintos sectores y las necesidades específicas de las micro, pequeñas y medianas empresas, con la finalidad de completar el marco regulatorio existente y aportar un valor añadido de garantía y confianza. Su promoción corresponderá a las asociaciones y otros organismos representativos de responsables o encargados del tratamiento, empresas, Administraciones públicas, organismos de supervisión y de resolución extrajudicial de conflictos y serán vinculantes para quienes se adhieran a los mismos.

El proyecto de código de conducta se presentará a la autoridad de control, la Agencia española de protección de datos o autoridad autonómica, para que dictamine su coherencia y conformidad con el Reglamento y por ende su aprobación, registro y publicación. Los registros estarán interconectados entre sí, coordinados con el registro gestionado por el Comité Europeo de protección de datos y serán accesibles a través de medios electrónicos.

El código de conducta debe tener peso y entidad propia para que desempeñe una función práctica positiva y si bien debe someterse a la normativa vigente no debe limitarse a reproducirla; debe confeccionarse como una especie de traje a medida para lo que deberá tener en cuenta la protección de los datos en el sector específico al que quiere aplicarse. Tendrá que incluir, además, mecanismos de control obligatorio de su cumplimiento. Ha de ser coherente y consistente.

El cumplimiento del código será supervisado por un organismo que tenga el nivel adecuado de pericia en relación con su objeto y que haya sido acreditado para tal fin por la autoridad de control competente; organismo cuya existencia debe ser prevista por el propio código. Si el código se infringe por el responsable o por el encargado del tratamiento, se podrán tomar las medidas oportunas, incluidas su suspensión o exclusión, informando a la autoridad de control competente.

I)DERECHO A LA TUTELA EFECTIVA (206)

Al margen de los recursos administrativos o judiciales que correspondan (207), el interesado podrá presentar una reclamación ante la autoridad de control, en nuestro caso la Agencia española de protección de datos, si el tratamiento de datos personales infringe el Reglamento; de igual modo, si la autoridad de control no da curso a su reclamación o no le informa debidamente.

La Agencia española de protección de datos antes de llevar a cabo ninguna actuación debe examinar su competencia y determinar el carácter nacional o transfronterizo del procedimiento que debe seguirse. Si considera que no tiene la condición de autoridad de control principal remitirá la reclamación formulada a quien considere competente quien deberá darle el curso oportuno, notificando esta circunstancia a quien reclamó. Ello implicará el archivo provisional del procedimiento para la Agencia. Todo esto en el marco del principio de cooperación recogido por el artículo 60 del Reglamento.

No obstante lo anterior, debemos tener en cuenta que las Comunidades Autónomas pueden asumir competencias en materia de protección de datos personales y en este caso atender también a su propia normativa (208), lo que es perfectamente acorde con la organización territorial del Estado español reflejada en la Constitución española y quizá sea positivo que al limitar el ámbito territorial de competencia se pueda concentrar la actuación de defensa de los derechos de los particulares en esta materia; ahora bien, no se puede perder de vista que la norma de referencia es el Reglamento de la Unión Europea y que cualquier norma nacional o autonómica debe asumir y plegarse a lo dispuesto en él, admitiéndose precisiones o desarrollos que no lo contradigan.

J)DERECHO A INDEMNIZACIÓN Y RESPONSABILIDAD (209)

Toda persona que haya sufrido daños, materiales o inmateriales, como consecuencia de las infracciones del Reglamento tendrá derecho a recibir del responsable o del encargado del tratamiento una indemnización.

El responsable responderá por el incumplimiento del Reglamento, el encargado lo hará en relación con las obligaciones que específicamente le atañen o si lo ha hecho al margen o en contra de las instrucciones del anterior. Si hay varios responsables o encargados participantes en la misma operación se establece su responsabilidad solidaria a fin de garantizar la indemnización efectiva del interesado, teniendo derecho a reclamar de los demás la parte de indemnización correspondiente a su parte de responsabilidad.

La acción se ejercitará ante los tribunales del Estado en el que el responsable o el encargado tengan un establecimiento. Alternativamente donde tengan su residencia habitual. En el caso de las Administraciones públicas, se exigirá de acuerdo con la regulación sobre responsabilidad patrimonial (210).

K)RÉGIMEN SANCIONADOR (211)

Corresponde a los Estados miembros establecer la normativa aplicable en materia de sanciones en los casos de infracción del Reglamento, en particular las que no se sancionen con multas administrativas, adoptando las medidas necesarias para que se garantice su observancia. Las sanciones y las multas, en su caso, serán efectivas, proporcionadas y disuasorias (212).

La LO 3/2018 establece un catálogo de infracciones, con carácter enumerativo o ejemplificativo, donde diferencia las consideradas *muy graves* que prescribirán a los tres años, así por ejemplo la utilización de los datos para una finalidad que no sea compatible con aquélla para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello; *graves* que prescribirán a los dos años, como por ejemplo, el tratamiento de datos personales de un menor de edad sin recabar su consentimiento cuando tenga capacidad para ello o del titular de la patria potestad o la tutela y *leves* que prescribirán en el plazo de un año, así en el caso de que se incumpla la obligación de documentar cualquier violación de seguridad (213).

Las multas administrativas se impondrán en función de cada caso individual, a título adicional o sustitutivo de otras medidas. Para calcular su cuantía se tendrán en cuenta los criterios que señala el artículo 83 y entre ellos: naturaleza, gravedad y duración de la infracción; categoría de los datos afectados, daños y perjuicios sufridos; intencionalidad o negligencia; medidas tomadas para paliar los efectos negativos; si se han cometido infracciones anteriores; grado de cooperación con la autoridad de control; la adhesión a códigos de conducta; etc.

Será posible, complementaria o alternativamente, la adopción cuando proceda de otras medidas correctivas. Así, no sólo las exigencias de seguridad y garantía de control de sus datos por los interesados, sino también las

elevadas sanciones recomiendan que se adopten posturas preventivas y de cumplimiento responsable de la normativa.

L)REGISTRO DE LAS ACTIVIDADES (214)

Cada responsable debe llevar adelante un registro de las actividades de tratamiento que se han efectuado bajo su responsabilidad que contendrá la información requerida; entre otras cosas, la identificación del responsable y del delegado de protección de datos, a quien, en su caso, se le han de comunicar las adiciones, modificaciones o exclusiones en el contenido del registro; los fines del tratamiento; categorías de interesados y de datos personales; destinatarios de los datos, incluidos los de terceros países; plazos previstos para la supresión de las categorías de datos; descripción de las medidas técnicas y organizativas de seguridad.

Los registros constarán por escrito, inclusive en formato electrónico y en su caso, se pondrán a disposición de la autoridad de control que lo solicite. No se llevarán a cabo, cuando se trate de empresas y organizaciones que empleen a menos de 250 personas salvo que ese tratamiento pueda entrañar un riesgo adicional para los derechos y libertades, no sea ocasional o incluya categorías especiales de datos personales tales como el origen étnico, opiniones políticas, convicciones religiosas, datos relativos a la salud o a la vida sexual, la afiliación sindical, datos genéticos o biométricos, o datos personales relativos a condenas e infracciones penales; por lo que en realidad, en la práctica, la mayoría de responsables y encargados del tratamiento aun empleando a un número de personas inferior al reflejado, llevan a cabo el registro en cuestión.

M)PERSONAS FALLECIDAS (215)

Es una de las novedades que introduce el artículo 3 de la LO 3/2018, pues permite que las personas vinculadas al fallecido por razones familiares o de hecho, o sus herederos puedan solicitar el acceso a los datos, su rectificación o supresión en su caso, de acuerdo con las instrucciones que aquél hubiera dejado, que también podrían ir destinadas a la prohibición de esta posibilidad. Estas instrucciones podrán dejarse también al albacea testamentario y en ningún caso podrán afectar a los datos de carácter patrimonial del causante.

Tratándose de menores estas facultades podrán ejercerlas sus representantes legales o el Ministerio Fiscal en el marco de sus competencias quien podrá actuar de oficio o a instancia de persona física o jurídica interesada.

De igual modo, y tratándose de personas con discapacidad, estas facultades podrán llevarse a cabo además de por los anteriores, por los designados para ejercer funciones de apoyo, si ésta en concreto se encontrara entre las mismas. En cualquier caso, se trata de garantizar que dichos datos no sean tratados *sine die*.

N)LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (216)

Es una autoridad administrativa independiente, de ámbito estatal, con personalidad jurídica y plena capacidad pública y privada. Se relaciona con el gobierno a través del Ministerio de Justicia. A ella corresponde supervisar la aplicación del Reglamento y de la LO 3/2018, de acuerdo con las funciones que tiene encomendadas.

La presidencia ostenta su representación y será auxiliada por un adjunto en quien podrá delegar sus funciones que deberán ser ejercidas con plena independencia y objetividad, aun siendo nombrados por el Gobierno, a propuesta del Ministerio de Justicia por ser personas de reconocida competencia en esta materia (217). El gobierno remitirá al Congreso de los Diputados la propuesta para estos cargos acompañada de un informe que justifique la misma; ésta será ratificada por la Comisión de Justicia en votación pública por mayoría de 3/5 de sus miembros en primera votación o por mayoría absoluta en segunda; en este último caso los votos favorables

deben proceder de diputados que pertenezcan, al menos, a dos grupos parlamentarios diferentes. Finalmente, serán nombrados mediante real decreto por el Consejo de Ministros, para un periodo de cinco años, renovable por el mismo periodo de tiempo.

Entre otras actuaciones, le compete dictar las resoluciones e instrucciones que requiera el ejercicio de sus funciones; la coordinación con las autoridades autonómicas; la representación de la Agencia en el ámbito internacional y las correspondientes funciones de gestión, teniendo en cuenta que los actos y disposiciones dictados por la presidencia de la Agencia Española de protección de datos ponen fin a la vía administrativa y se pueden recurrir directamente ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional.

El Consejo Consultivo de la Agencia Española de protección de datos se encargará de su asesoramiento. Sus miembros serán nombrados por orden del Ministerio de Justicia entre expertos que acrediten los conocimientos que se exigen por su perfil profesional y académico. Se reunirá una vez al semestre y siempre que lo disponga la presidencia de la Agencia Española. Sus decisiones son orientativas; no tienen carácter vinculante.

Ñ)EL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS [(218)]

Con sede en Bruselas se crea este Comité, con personalidad jurídica, como organismo de la Unión. Está compuesto por una autoridad de control de cada Estado miembro y el Supervisor europeo de protección de datos, que se encargará de la Secretaría. Actuará con total independencia e imparcialidad en el desempeño de sus funciones y competencias, siendo la más relevante garantizar la aplicación coherente del Reglamento; para ello, pueden adoptar directrices generales para clarificar los términos de la legislación europea de protección de datos proporcionando a todos los interesados una interpretación congruente de sus derechos y obligaciones.

Tendrá que elaborar un informe anual que será público y se transmitirá al Parlamento Europeo, al Consejo y a la Comisión, sobre la protección de las personas físicas en lo que respecta al tratamiento en la Unión y si procede, en terceros países y organizaciones internacionales. Tomará sus decisiones por mayoría simple de sus miembros, como regla general y con este quórum elegirá un presidente y dos vicepresidentes para un periodo de cinco años, renovables una vez. Sus debates serán confidenciales.

O)CERTIFICACIÓN EN MATERIA DE PROTECCIÓN DE DATOS [(219)]

Se promueve a nivel de la Unión la creación de mecanismos de certificación en materia de protección de datos, sellos y marcas de protección de datos con el fin de demostrar el cumplimiento de lo dispuesto en el Reglamento en las operaciones de tratamiento de los responsables y encargados, lo que genera gran confianza en los ciudadanos y las empresas.

La certificación será voluntaria y se llevará a cabo a través de un proceso transparente, teniendo en cuenta los criterios de acreditación aprobados por la autoridad de protección de datos correspondiente. Será expedida por los organismos de certificación o por la autoridad de control competente. Cuando los criterios sean aprobados por el Comité europeo dará lugar a una certificación común, el Sello Europeo de protección de datos o Sello Europeo de Privacidad [(220)].

Para ello, los responsables o encargados facilitarán toda la información y el acceso necesario a sus actividades. La certificación, en su caso, tendrá un periodo de duración de tres años y podrá ser renovada. De igual modo, podrá ser retirada si se dejan de cumplir los requisitos exigidos.

El Comité registrará todos los mecanismos de certificación, sellos y marcas de protección de datos y los pondrá a disposición pública.

P)LOS NUEVOS DERECHOS DIGITALES

La LO 3/2018 de protección de datos personales y *garantía de los derechos digitales*, incorpora un novedoso Título X, que tiene por objeto la determinación y regulación, como su propio nombre indica, de un sistema de garantía de derechos digitales que si bien no se encuentran recogidos en el Reglamento, lo que podría suponer un problema si no existiera armonización a nivel europeo en su interpretación y regulación, se incorporan a la misma como el propio preámbulo explica, porque Internet se ha convertido en una realidad en la vida personal y colectiva de los ciudadanos.

El nuevo panorama permite identificar con bastante claridad los riesgos que se generan y por esta razón, los poderes públicos consideran que deben impulsar políticas que hagan efectivos los derechos de la ciudadanía y el pleno ejercicio de los derechos fundamentales en la realidad digital. La transformación digital se impone en la actualidad y la normativa debe reforzar estos derechos.

Ahora bien, el propio apartado IV del preámbulo considera deseable una futura reforma de la Constitución que la actualice a la era digital y eleve a rango constitucional esta nueva generación de derechos digitales; no obstante, y en tanto en cuanto esta actualización se lleva a cabo el legislador aborda en esta Ley su reconocimiento, partiendo del mandato impuesto en el artículo 18.4 de la Constitución y tomando en consideración los perfiles ya establecidos por la jurisprudencia ordinaria, constitucional y europea.

El capítulo comienza afirmando, lo que a mi juicio se presupone, que los derechos y libertades previstos en la Constitución son plenamente aplicables en Internet y que por tanto, los prestadores de servicios de la información y los proveedores de servicios de Internet deben contribuir a garantizar su aplicación. En la batería de derechos que se reconocen hay algunos que se incluyen por primera vez y otros que, como hemos tenido oportunidad de ver en los capítulos anteriores, se amparan en el derecho a la intimidad.

La regulación se establece en los artículos 79 a 97, preceptos que, sin perjuicio de lo visto con anterioridad, podemos agrupar en cuatro grandes bloques:

a)Derechos digitales de los ciudadanos en general: se recogen derechos tales como el *derecho de acceso universal*, asequible y de calidad a Internet; el *derecho a la neutralidad* de Internet mediante una oferta transparente de servicios y el *derecho a la seguridad digital* en relación con las comunicaciones que se transmiten y reciben. Para favorecerlos, se llevarán a cabo por el Gobierno central y las Comunidades Autónomas políticas de impulso de los derechos digitales.

b)Derechos de los menores: se incluyen el *derecho a la educación digital*, el *derecho a la protección* de los menores para garantizar su desarrollo y preservar su dignidad y derechos fundamentales; el *derecho a la protección de sus datos* en Internet. Para hacerlo viable y garantizarlo se llevarán a cabo los planes de actuación que explicamos anteriormente.

c)Derechos en el ámbito laboral: destacan como tales el *derecho a la intimidad en el uso de los dispositivos digitales* que pone a su disposición el empleador; el derecho a la desconexión digital en el ámbito laboral; el *derecho a la intimidad frente al uso de dispositivos de videovigilancia* y grabación de sonidos en el lugar de trabajo; *derecho a la intimidad ante la utilización de sistemas de geolocalización* en el ámbito laboral.

d)Medios de comunicación: se regulan especialmente *el derecho de rectificación* en Internet y el *derecho a la actualización de informaciones* en los medios de comunicación digitales.

Partiendo del reconocimiento del derecho a la libertad de expresión y el derecho a comunicar y recibir libremente información veraz en Internet, el art. 85 LO 3/2018, exige a los responsables de redes sociales y servicios equivalentes, que adopten los protocolos necesarios para que, en su caso, se pueda ejercitar el

derecho de rectificación cuando se difundan contenidos que puedan atentar contra el honor y la intimidad personal y familiar en Internet atendiendo a los requisitos y procedimiento previstos en la Ley orgánica reguladora de este derecho, que vimos en un capítulo anterior.

Los medios de comunicación digitales deberán publicar en sus archivos digitales un aviso aclaratorio que ponga de manifiesto que la noticia original no se corresponde con la realidad; este aviso deberá aparecer en un lugar visible junto a la misma (221).

Además, se puede solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible cuando la información contenida en la noticia original no refleje ya la situación actual causando algún tipo de perjuicio; en particular, si la noticia se refiere a actuaciones policiales o judiciales.

3.LA PROTECCIÓN DE DATOS EN LOS MEDIOS DE COMUNICACIÓN

Como tuvimos oportunidad de explicar en los capítulos anteriores el problema de la conciliación de la libertad de expresión e información con los derechos al honor, la intimidad personal y familiar y la imagen es complejo de resolver; la realidad es muy similar y de nuevo nos encontramos ante una situación de tensión cuando nos referimos a esos mismos derechos pero en su relación con el derecho a la protección de datos de carácter personal, dado que seguimos en el ámbito de derechos fundamentales y nos encontramos con una reciente regulación a la que los medios de comunicación deben adaptarse en un doble ámbito, el de la organización de las empresas de comunicación y el profesional, propio y específico de la labor desarrollada por los periodistas y medios de comunicación.

El propio Reglamento en su considerando 4, considera que el derecho a la protección de datos no es un derecho absoluto sino que con arreglo al principio de proporcionalidad debe mantener el equilibrio con otros derechos fundamentales y en particular, entre otros que menciona, en relación con la libertad de expresión y de información (222); por ello se permite que los Estados puedan, a través de sus Leyes nacionales, conciliar el derecho a la protección de los datos personales por las vías previstas en el Reglamento, con los derechos a la libertad de expresión e información, incluido el tratamiento con fines periodísticos o lo que es lo mismo, los Estados pueden decidir cuándo y cómo se puede excluir, por ser necesario, la aplicación de la normativa sobre protección de datos.

Es por esta razón que se permite que se establezcan excepciones a los principios generales, a los derechos de los interesados, en relación con el responsable y el encargado del tratamiento, la transferencia de datos a terceros países, las autoridades de control, los principios de cooperación y coherencia y las disposiciones relativas a situaciones específicas de tratamientos de datos, siempre que sea necesario para poder compatibilizar ambos derechos (223); lo que se presenta como un punto de partida absolutamente lógico pues la aplicación estricta y rigurosa de todas las cautelas contenidas en la normativa europea y nacional sobre protección de datos al tratamiento realizado por los medios de comunicación supondría un impedimento y un freno considerable para el ejercicio de las libertades informativas.

La cuestión que ahora nos planteamos es cómo llevar a cabo la conciliación de ambos derechos habida cuenta de las especiales dificultades que plantea el desarrollo de las tecnologías de la información y la comunicación en Internet y si las normas, opiniones doctrinales y decisiones jurisprudenciales que se vienen aplicando para dirimir los conflictos con los derechos la honor, a la intimidad y a la imagen sirven también en el ámbito de la protección de datos o si por el contrario, debemos atenernos a nuevas indicaciones.

No se puede dudar del gran impacto que la protección de datos ha supuesto prácticamente en todos los ámbitos y por supuesto también para la labor periodística que se mueve y se nutre de todas las noticias y novedades que pueden interesar a la generalidad pero que al mismo tiempo pueden, en la mayoría de las ocasiones,

afectar a la privacidad de las personas pues los datos son el elemento fundamental y básico con el que el trabajo de los medios de comunicación se despliega. El dato sustenta el proceso comunicativo y las empresas conocen el valor inmenso que posee como mercancía en el tráfico jurídico; los datos son la savia de la información y su recogida, almacenamiento y difusión son actividades inherentes al ejercicio de las labores informativas (224).

La armonía a la que nos referimos es necesaria pues si bien es cierto que la libertad de información y de expresión son la garantía de una opinión pública libre, el derecho fundamental a la protección de datos desempeña también el papel de garante del Estado democrático y de derecho; además seguramente mantener una visión conciliadora entre ambos derechos facilite que el ejercicio legítimo de cada uno de ellos redunde en beneficio del otro y potencie, a su vez, su ejercicio (225).

De acuerdo con lo anterior, la normativa europea insta a los ordenamientos jurídicos de los Estados miembros a conciliar las normas que rigen la libertad de expresión e información, incluida la expresión periodística con el derecho a la protección de los datos personales; así cuando el tratamiento de los datos personales lo sea con fines *exclusivamente periodísticos* puede estar sujeto a excepciones o exenciones que faciliten la tarea de comunicación e información; en particular en el ámbito audiovisual y en los archivos de noticias y hemerotecas. El fin último es conseguir equilibrar ambos derechos fundamentales, destacando la importancia del derecho a la libertad de expresión en cualquier sociedad democrática y la libertad que en última instancia representa el periodismo (226).

No obstante, el considerando 41 del Reglamento explica que cuando en su seno se hace referencia a una base jurídica o a una medida legislativa, esto no exige necesariamente un acto legislativo adoptado por un parlamento, sin perjuicio de los requisitos de conformidad del ordenamiento constitucional del Estado en cuestión. En cualquier caso, dicha base jurídica o medida legislativa debe ser clara y precisa y su aplicación previsible para sus destinatarios de conformidad con la jurisprudencia del TJUE y del TEDH (227).

La pregunta siguiente es: ¿tenemos esa base jurídica dado que carecemos de esa medida legislativa? ¿Qué requisitos deben darse para poder aplicar la conocida como excepción periodística?

España no recoge la excepción periodística en la LO 3/2018 y tampoco lo hacía en la anterior LOPD de 1999, si bien esta última en su artículo 3 j) consideraba como *fuentes accesibles al público*, aquellos ficheros cuya consulta puede ser realizada por cualquier persona, cuando no está impedida por una norma limitativa o si no hay más exigencia que, en su caso, el abono de una contraprestación. Ser una fuente accesible al público legitima que los datos se puedan tratar aún sin existir el consentimiento del interesado siempre que no exista ninguna vulneración de sus derechos y libertades (228).

Esta no regulación puede entenderse de dos maneras; de un lado, considerar que la actividad periodística se encuentra sometida a toda la normativa de protección de datos o bien, de otro lado, entender que el Ordenamiento jurídico español tiene la base jurídica suficiente, idea a la que me adhiero, para como ya se hace en los casos de colisión entre el derecho a la información y los derechos al honor, intimidad e imagen, realizar el correspondiente juicio de ponderación de ambos derechos y determinar cuáles son los requisitos que se deben exigir para, en su caso, mantener la prevalencia cuando proceda de la libertad informativa frente al derecho a la protección de datos.

Para hacerlo correctamente y partiendo de la necesaria distinción entre las libertades de expresión y de información (229), debemos acudir a la doctrina jurisprudencial interna, del Tribunal Constitucional y del Tribunal Supremo y también externa, de los tribunales de Justicia de la Unión Europea y Europeo de derechos humanos; estos dos últimos además, deberán iluminar con los criterios que se adopten, la amplitud que deja el Reglamento a los distintos Estados miembros en relación con esta materia ya que se provocarán, seguramente, importantes problemas de carácter transfronterizo y de inseguridad jurídica, pues se puede dar lugar a legislaciones muy heterogéneas que podrán oscilar desde el establecimiento de la primacía global de la libertad

de expresión a través de amplias exenciones, hasta sistemas que contengan elementos equivalentes a la censura previa (230).

En conclusión podemos afirmar que el Reglamento general insta a los Estados a conciliar el derecho a la protección de los datos personales con la libertad de expresión y de información; que además permite que los Estados puedan adoptar normas específicas en sus ordenamientos para armonizar ambos derechos y que en el supuesto de no llevarlo a cabo, como es nuestro caso, cobra una especial importancia el papel de los órganos jurisdiccionales a quienes corresponde realizar un ejercicio de ponderación para conciliarlos habida cuenta de que nuestro Ordenamiento jurídico cuenta con los resortes suficientes para dentro de la base jurídica a la que hace referencia el Reglamento y respetándolo, adoptar una posición al respecto que garantice el equilibrio. Por esta razón, dedicamos el epígrafe siguiente a analizar los requisitos que exigen los tribunales nacionales e internacionales para compatibilizar ambos derechos y si el resultado nos permite afirmar, dentro de las limitaciones, la prevalencia del derecho a la libertad de información.

4.¿PREVALENCIA DE LAS LIBERTADES INFORMATIVAS?

Aplicar a rajatabla las disposiciones sobre protección de datos impediría, en la mayoría de las ocasiones, el ejercicio de las libertades informativas. Es por ello que la legislación vigente permite el establecimiento de limitaciones bajo determinados presupuestos; en nuestro caso, se trata de ponderar el ejercicio de la libertad de información y el derecho a la protección de datos.

A)REQUISITOS PARA IMPONER LIMITACIONES EN LA DOCTRINA DEL TEDH Y EL TJUE

Las condiciones para limitar la protección de los datos personales están recogidas en el artículo 52 de la Carta y en el artículo 8 del CEDH, además del Reglamento y se han desarrollado gracias a la interpretación que el TEDH y el TJUE han hecho de los mismos en su jurisprudencia donde se refieren a menudo a sus respectivas sentencias como parte del diálogo constante entre ambos tribunales en busca de una interpretación armonizada de la normativa de protección de datos (231).

El Ordenamiento jurídico de la Unión Europea permite la limitación de un derecho fundamental, en nuestro caso la protección de datos de carácter personal, si se dan una serie de requisitos que pasamos a exponer:

–Debe realizarse de conformidad con la Ley.

Las limitaciones, que se impongan, tienen que tener un fundamento jurídico que permita que los interesados las conozcan para poder adecuar su conducta a las mismas, evitando con ello injerencias arbitrarias (232).

–Respetar la esencia del derecho.

Cualquier limitación debe respetar el contenido esencial de tales derechos. No se admiten limitaciones tan invasivas que anulen el derecho fundamental al vaciarlo de su contenido básico. La limitación no puede, en su caso, exceder de lo estrictamente necesario pues el propio derecho dejaría de tener sentido.

–Aplicar el principio de proporcionalidad.

Sólo se pueden introducir limitaciones que sean necesarias, entendiendo que lo son cuando haya que adoptarlas para alcanzar un objetivo de carácter general y siempre que sean menos invasivas que otras medidas para alcanzar el mismo objetivo. Así, siendo la limitación estrictamente necesaria también ha de ser proporcionada, lo que implica que las ventajas derivadas de la limitación deben ser superiores a las desventajas que acarree para el ejercicio de los derechos en cuestión. Para reducir las desventajas y los riesgos es importante que vayan acompañadas de garantías adecuadas.

–Finalidad de interés general reconocida por la Unión o necesidad de proteger los derechos de los demás.

El derecho a la protección de datos suele interactuar con otros derechos fundamentales. En esa interactuación la limitación se permite cuando obedece a objetivos de interés general reconocidos por la Unión, tales como promover la paz, el bienestar de los pueblos, la protección social, la creación de espacios de libertad, seguridad y justicia donde se garantice la libre circulación de las personas, la igualdad, la solidaridad, la diversidad, el desarrollo sostenible del planeta, la erradicación de la pobreza, entre otros (233). En cualquier caso, el objetivo debe estar bien definido y ser explicado con el debido detalle para que no quepa duda de la necesidad, pues este requisito está estrechamente ligado a la proporcionalidad de la limitación. Ha de ser un fin legítimo y necesario en un Estado de Derecho.

Por otra parte, la necesidad de proteger los derechos y libertades de los demás es uno de los criterios utilizados para determinar la licitud de la limitación del derecho a la protección de los datos personales (234). Es frecuente, de hecho, la interacción del mismo con otros derechos como la libertad de expresión y el derecho a dar y recibir información, que nos ocupa, pues sin medios de comunicación libres, el Estado de Derecho no se sostiene y la información se convierte en propaganda.

Teniendo en cuenta los requisitos anteriores y que la excepción de las normas de protección de datos con fines periodísticos tiene por objeto permitir que los periodistas obtengan, recopilen y traten datos para poder realizar su labor periodística que no es otra que divulgar al público la información, tanto el TJUE como el TEDH han establecido en numerosas ocasiones cuáles son los criterios por los que deben regirse las autoridades nacionales para llevar a cabo una ponderación equilibrada de ambos derechos, pues cuando está en juego el discurso político o un debate sobre una materia de interés público, existe escaso margen para limitar el derecho a recibir y comunicar información, ya que el público tiene derecho a ser informado y este es un derecho esencial en cualquier sociedad democrática (235).

Entre los factores que deben tenerse en cuenta para hacer un ejercicio de ponderación equilibrado, el TJUE ha destacado los siguientes (236):

–La naturaleza de la información en cuestión es un factor especialmente importante que justifica otorgar al público en general acceso a la misma.

–Que exista un interés público en la disponibilidad de la información porque ésta sea relevante.

–Que nos encontramos ante figuras públicas.

–El modo en que se ha obtenido la información.

–Que la información sea fiable.

B)TRATAMIENTO CON FINES *EXCLUSIVAMENTE* PERIODÍSTICOS

Teniendo en cuenta los requisitos para imponer limitaciones en los derechos fundamentales y expuestos los criterios que a la hora de hacer la correspondiente ponderación tienen en cuenta los tribunales mencionados, nos queda aún por comentar la expresión *tratamiento con fines periodísticos* que utiliza el artículo 85 del Reglamento o *exclusivamente periodísticos* de su considerando 153.

Se desprende del precepto que para poder aplicar la excepción, el tratamiento de datos debe tener una finalidad concreta, la de informar. Ahora bien, ¿esta tarea de información corresponde exclusivamente a los medios de comunicación conocidos, ya lo hagan a la manera tradicional o bien *on line* o se puede ampliar a los tratamientos de datos realizados por ciudadanos que sin tener la cualificación necesaria llevan a cabo

actuaciones pseudo-informativas en el ejercicio de su libertad de expresión?, ¿se puede considerar como actividad periodística cualquiera que vaya encaminada a divulgar información, opiniones o ideas o queda ésta reservada para las empresas y medios de comunicación?, ¿el concepto periodismo se puede interpretar en un sentido amplio dando cabida al conocido como *periodismo ciudadano*?

La ya derogada Directiva 95/46/CE planteaba dos cuestiones fundamentales que fueron objeto de crítica y que considero que se deben comentar pues se reproducen en el Reglamento:

b.1)La consideración de la excepción periodística por la legislación de los diferentes Estados puede dar lugar a normativas absolutamente diferentes

Esto es cierto y realmente la apreciación de la misma en las legislaciones nacionales que quisieron cumplir con la finalidad de la Directiva dio lugar a que se abordara la cuestión de maneras muy diferentes: a) En países como Bélgica, España o Portugal la normativa de protección de datos no contempla exención alguna expresa de la aplicación de sus disposiciones a los medios de comunicación (en nuestro caso, tampoco actualmente tras la aparición del Reglamento); b) En casos como Francia, Austria, Italia o Finlandia, los medios de comunicación están exentos de la aplicación de algunas disposiciones de la normativa de protección de datos; c) En otros supuestos, los medios quedan exceptuados de la normativa general de protección de datos y se regulan por disposiciones específicas para este ámbito. Es el caso de Dinamarca para todos los medios de comunicación y de Alemania en relación con las empresas públicas de radiodifusión (237).

No obstante, la diferencia esencial entre el régimen de la Directiva y el del Reglamento viene marcada por el carácter estrictamente obligatorio de este último en todos sus elementos y para todos los Estados miembros. Ello quiere decir que el Reglamento como norma directamente aplicable ya tiene por sí mismo eficacia normativa sin necesidad de ningún acto de transposición o adaptación al Derecho interno, siendo su aplicación prevalente frente a los Derechos nacionales si existiera alguna contradicción; lo que quiere decir que cuando los diferentes Estados apliquen el artículo 85 y la excepción periodística a los medios de comunicación tendrán por delante una tarea de conciliación en el marco de sus derechos internos pero no podrán en ningún caso contrariar lo dispuesto en él. La uniformidad para los Estados la da, por tanto, la legislación reglamentaria; la adecuación, si fuera necesaria, la legislación nacional, pero el objetivo es el mismo para todos, de lo que considero se puede deducir la posición preferente de la libertad de información también frente a la protección de datos si bien con las cautelas necesarias.

En conclusión, puede haber variedad de consideraciones y adaptaciones, pero en todo caso, partiendo de esa posición preferente se debe buscar un necesario y reconocido equilibrio entre el derecho a la protección de datos y los derechos a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos, poniendo en evidencia la importancia que en las Constituciones democráticas tienen las normas relativas a la libertad de expresión y de prensa (238).

Desde este punto de vista, considero que nuestro Ordenamiento tiene la base jurídica suficiente para realizar de manera adecuada la ponderación expresada, pues ya se han reconocido, como veíamos en el capítulo I, las particularidades de los medios de comunicación en relación con otros derechos fundamentales, como son el honor, la intimidad personal y familiar y la imagen; lo que nos debe llevar a considerar que el alcance efectivo de la excepción que nos ocupa, siempre dentro de las actividades editoriales, no se debe realizar de manera abstracta, aunque como en el caso anterior se puedan extraer unas pautas generales, sino caso por caso y en la medida concreta en la que las normas de protección de datos tengan relación directa con las actividades de los medios.

Del mismo modo que los medios de comunicación partiendo de una posición preferente en el caso de colisión entre el derecho a la información y los derechos al honor, a la imagen y a la intimidad, están obligados a respetar determinadas normas como tuvimos oportunidad de comprobar en el capítulo primero; de alguna

manera, esa misma normativa y la abundante e interesante jurisprudencia que existe en esta materia, han generado una relación entre la libertad de información y aquellos derechos que sin lugar a dudas, pueden y deben tenerse en cuenta trasladándose a la nueva relación que se genera con la protección de datos. Todo lo que hemos considerado para la protección de la intimidad cuando ésta se ve atacada por los medios de comunicación, todas las garantías específicas con las que contamos en relación con los medios, se pueden actualizar al caso de la protección de datos, y a partir de ahí y sin olvidar las peculiaridades de este derecho, ir avanzando en los requisitos y presupuestos necesarios para llevar a cabo la conciliación de ambos derechos con éxito.

Por lo tanto, que el Ordenamiento español no refleje la excepción periodística como tal de una manera expresa, no debe suponer una traba para que la jurisprudencia española la considere implícitamente reconocida en el mismo.

Siendo esto así, se puede afirmar que:

–La normativa relativa a la protección de datos se debe aplicar, en principio, a los medios de comunicación.

–Es posible aplicar la excepción periodística en los supuestos contemplados en el Reglamento, en tanto en cuanto se perfila, si se considera necesario, a través de normativa interna.

–La excepción va referida únicamente al tratamiento con fines periodísticos (editoriales), cuando es llevado a cabo por profesionales de la información y medios de comunicación institucionalizados y tanto si es una publicación tradicional como si lo es electrónica.

–Es necesario el ajuste al principio de proporcionalidad, de lo que se deduce que sólo se podrá tener en cuenta la excepción, si la normativa sobre protección de datos afectare a la libertad de información y manteniendo siempre el equilibrio.

–La ponderación exige que no se desvelen innecesariamente datos personales que no resulten significativos para la información.

–La ética profesional y los códigos de autorregulación tienen especial importancia a la hora de evaluar la excepción en los casos concretos.

Se puede concluir por tanto, aun no existiendo en nuestro Ordenamiento jurídico ninguna norma que regule de manera específica qué ha de entenderse por excepción periodística y cuáles son sus presupuestos y limitaciones, que la normativa de protección de datos no se puede aplicar en su plenitud a los medios de comunicación por la especial relevancia que en nuestro Estado democrático y de Derecho tienen las normas constitucionales relativas a la libertad de expresión, de información y de prensa [(239)]; y que para determinar el alcance de la excepción periodística debemos atender a la normativa vigente, los principios generales del derecho y la importante labor de la jurisprudencia como complemento del sistema de fuentes; todo ello limita, de hecho, el cumplimiento estricto de las normas de protección de datos y permitirá que la conciliación de ambos derechos y el ejercicio compatible de los mismos sea una realidad.

b.2)Si se aplica al tratamiento de datos para fines exclusivamente periodísticos se reduce considerablemente el ámbito de los sujetos que pueden beneficiarse de la misma pues nos referíamos únicamente a periodistas y medios de comunicación institucionalizados

Para acogerse a la excepción periodística el Reglamento exige que el tratamiento se realice exclusivamente con fines periodísticos, es decir, enfatiza el fin al que está destinado el mismo; ahora bien, la duda que se nos plantea es ¿podemos disociar el fin del sujeto que lo lleva a cabo?, ¿puede existir un fin periodístico sin profesionales de la información?, ¿la excepción ampara los tratamientos de datos que puedan llevar a cabo ciudadanos o más bien se consagra como una prerrogativa de los periodistas y medios de comunicación en los

que, en su caso, prestan sus servicios?

Es evidente que Internet favorece el desarrollo de la comunicación pues apenas existen barreras y cualquiera puede intervenir y participar enviando contenidos, compartiendo datos e imágenes, vídeos, *reviews*, opiniones, ideas y reenviando información; de modo que lo que antes se hacía en pequeños y controlados círculos, hoy se ha ampliado de manera desenfrenada aumentando no sólo el volumen de información sino también la magnitud y características de las personas que intervienen en este nuevo ámbito de relaciones favorecido, sobre todo, por las redes sociales.

Nos resulta fácil en igualdad de condiciones técnicas crear contenidos para una audiencia global. La intervención de los particulares en un gran porcentaje está relacionada con contenidos de actualidad, políticos, sociales y económicos que de alguna manera pueden influir en la opinión pública. Es en este contexto donde se acuña la expresión periodismo ciudadano, periodismo democrático o periodismo 3.0 para definir la situación en la que los ciudadanos participan en el proceso de elaboración y transmisión de la información. La horizontalidad es la enseña de esta nueva manera de comunicar en la que cualquiera puede convertirse en un canal de difusión de la actualidad a través de blogs, *webs*, comentarios en foros y *post* en las redes sociales y también se fomenta este tipo de participación en muchos medios digitales. El debate está servido pues es una actividad que cumpliendo algunas de las pautas de la información periodística, no es profesional.

Este tipo de información presenta, a mi juicio, algunas ventajas e importantes inconvenientes (240). Entre las primeras, la colaboración ciudadana ofrece otro punto de vista de la misma realidad, pone al alcance de todos información de primera mano y en tiempo real, sobre todo en relación con sucesos de ámbito local; además, y por esa misma razón, al tratarse de noticias independientes actuarán como un contrapeso o contrapoder, función que en ocasiones han perdido los medios tradicionales, que actúan precisamente al revés, alineándose con el mismo.

En cuanto a los inconvenientes, se podrían destacar fundamentalmente la falta de contextualización, rigor, profundidad y contraste de fuentes lo que genera en muchas ocasiones debates sobre hechos falsos pues es innegable que Internet crea una grieta importante en este sentido, dado que se actúa sin los filtros que suponen los intermediarios de la industria de los medios de comunicación lo que, sin lugar a duda, empobrece la calidad y afecta a la credibilidad y objetividad de la noticia.

El profesional de la comunicación tiene una formación académica y técnica determinada de la que carecemos los ciudadanos y está sometido a un rigor ético, que si bien pudiera ser aplicable a cualquiera, está especialmente determinado a través de los códigos de autorregulación para quienes ejercen esta profesión y es voluntaria y específicamente aceptado por los mismos; son normas éticas que incumben a los periodistas y comunicadores y que reflejan en última instancia su compromiso con la verdad y un interés superior en la verificación de la noticia que remarca la diferencia esencial entre información y opinión al llevar a cabo una tarea primordial de selección, valoración y jerarquización de las novedades y datos que se transmiten para el conocimiento de la generalidad.

En atención a todo lo anterior, considero que no se debería hablar de periodismo ciudadano, sino más bien de *colaboración ciudadana* (241) entendiendo que la actividad que en este sentido podamos desarrollar los ciudadanos puede ser complementaria y tener un importante valor como fuente para que después los profesionales preparados para ello elaboren, contextualicen y difundan las noticias. Es aventurado considerar que nos convertimos en periodistas de manera automática por esta cooperación, sin objetar nada a su consideración como información valiosa que luego deba ser tratada por aquéllos a quienes corresponde para que no se deteriore un ápice el derecho a dar y recibir información veraz en un contexto en el que el exceso de información al que nos vemos sometidos dificulta considerablemente la identificación de la información fiable para separarla de la falsa, la que intoxica y las *fake news* (242) que realmente suponen una amenaza y se han convertido en una preocupación global que obliga a posicionarse contra el *todo vale,* pues ni los medios ni la opinión pública deben alejarse de la verdad pues sin ella tampoco hay libertad.

No se puede negar que en ocasiones nos podemos encontrar con que esta colaboración del ciudadano es de calidad, y que de manera puntual y en circunstancias especiales y de gravedad, poder disponer de determinada información es absolutamente necesario como herramienta, inclusive, para la defensa de los derechos humanos, pero incluso en estos casos considero que la colaboración debe enmarcarse en el ámbito más genérico de la libertad de expresión (243).

Por entender que esta actividad ciudadana puede englobarse dentro de la periodística, hay quien considera que la excepción periodística no se consagra como un privilegio exclusivo para los medios de comunicación sino que resulta también aplicable a los tratamientos de datos realizados por ciudadanos siempre que se lleven a cabo en el ejercicio del periodismo, atendiendo a que la libertad de expresión e información se configuran como derechos universales predicables no sólo de los medios de comunicación o de los profesionales de la información sino de todas las personas (244).

En mi opinión, sin embargo, y sin desmerecer la importancia que en el presente y sobre todo en el futuro pueda tener el llamado periodismo ciudadano, considero que el equilibrio en estos casos debe buscarse en la relación que se pueda plantear entre la libertad de expresión y la protección de datos de carácter personal. La excepción periodística debe aplicarse únicamente cuando encontremos en colisión este último derecho con el derecho a la información considerando como tal el que desarrollan los profesionales de la comunicación y los medios de comunicación institucionalizados, siempre que la información a la que se incorporan aquellos datos sea veraz y relevante para la formación de la opinión pública (245). El equilibrio fruto de la correspondiente ponderación deberá conseguirse, en su caso, por los tribunales quienes acudirán a la base jurídica que les brinda nuestro Ordenamiento.

En conclusión, se puede afirmar la prevalencia de la libertad de información frente a la protección de datos de carácter personal aunque en la medida imprescindible para que la información, que goza de la relevancia pública necesaria, pueda ser conocida por los ciudadanos, y por eso, únicamente a estos casos debe aplicarse la excepción periodística; todo lo demás no debe quedar exento de la aplicación de la normativa de protección de datos, lo que además redundará en beneficio de la privacidad pues cada vez son más invasivos los modos en los que la información personal y de otros se maneja y difunde públicamente en Internet por la ciudadanía; y además redundará en beneficio de una más correcta aplicación de ambos derechos, en este caso, la libertad de expresión y la protección de datos.

5.PROPUESTA DE REGLAMENTO E-PRIVACY (246)

Además de toda la legislación referida, muy brevemente queremos mencionar la existencia de una propuesta de Reglamento, el Reglamento de privacidad electrónica, con el que la Unión Europea quiere instaurar una política de privacidad en Internet válida para los ciudadanos de todos los Estados miembros con el objetivo de proteger los datos de un modo más estricto, favorecer la confianza de los ciudadanos en los canales de comunicación digital y fortalecer el mercado único digital pues la Directiva de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas se entiende desfasada dado que se han producido importantes cambios de índole tecnológica y económica en los mercados, que dan lugar a comunicaciones que se consideran desprovistas de protección (247).

Si finalmente entra en vigor, sustituirá a la Directiva siendo de aplicación directa en todos los Estados miembros; por su contenido más específico, se considera *lex specialis* respecto del Reglamento 679/2016 y supondrá un paso más en relación con las comunicaciones electrónicas y los datos personales digitales, pues la mayoría de los Estados ha reconocido la necesidad de que la protección de las comunicaciones constituya un derecho fundamental diferenciado (248), favoreciendo la armonización. Ambos Reglamentos son normas complementarias, y si bien este último se considera necesario para conseguir una casi absoluta protección de los datos, su aparición está sufriendo un considerable retraso debido a que algunos de sus preceptos podrían

influir en un cambio drástico del modelo de negocio de muchas compañías tecnológicas (249).

La propuesta se estructura en siete capítulos que versan sobre los siguientes aspectos que pueden afectar tanto a los usuarios particulares como a las empresas:

Capítulo I: contiene las disposiciones generales. Objeto, ámbito de aplicación material y territorial y definiciones. Se trata de proteger la privacidad en todas las comunicaciones electrónicas cuyos usuarios finales estén en la Unión Europea, aplicándose a las empresas que lleven a cabo cualquier tipo de servicio o tecnología de seguimiento *on line* o se dediquen a la comercialización electrónica directa (250).

Capítulo II: incluye las principales disposiciones para garantizar la confidencialidad de las comunicaciones electrónicas, limita los fines autorizados y establece las condiciones para el tratamiento de esos datos de comunicaciones. Aborda la protección de los equipos terminales y establece importantes consideraciones en relación con el consentimiento de los usuarios finales.

Capítulo III: presenta los derechos que asisten a los usuarios finales en materia de control del envío y recepción de comunicaciones electrónicas a fin de proteger su privacidad. Contempla posibles riesgos en materia de seguridad y prevé la obligación de los proveedores de servicios de comunicaciones electrónicas de alertar a los usuarios finales en caso de que surja un riesgo concreto que pueda comprometer la seguridad de sus redes y servicios.

Capítulo IV: se refiere a las funciones de supervisión y ejecución del Reglamento que se confían a las mismas autoridades de control encargadas del RGPD. Se amplían las funciones del Comité Europeo de protección de datos y se ratifica la aplicación del mecanismo de cooperación y coherencia previsto en el RGPD para los asuntos transfronterizos.

Capítulo V: describe las distintas vías de recurso al alcance de los usuarios finales y las sanciones que pueden imponerse y en particular, las condiciones para la imposición de multas administrativas.

Capítulo VI: trata la adopción de actos delegados y actos de ejecución.

Capítulo VII: contiene las disposiciones finales; deroga la Directiva sobre privacidad y comunicaciones electrónicas; hace referencia a la supervisión y evaluación, la entrada en vigor y la aplicación.

En relación con lo anterior y teniendo en cuenta que esta normativa afectará a más empresas que cualquier otra anterior, algunos de los aspectos más conflictivos son:

Cookies (251)*:* el consentimiento se debe obtener con anterioridad a su establecimiento, excepto las estrictamente necesarias. Debe ser otorgado de manera libre e inequívoca, por lo que la información sobre ellas ha de ser expuesta en un lenguaje claro y comprensible. Los *banners* informando de su uso, que inducen a aceptarlas o que impiden la navegación si no se aceptan, ya no serán válidos. Los navegadores deberán contener control de *cookies* y los usuarios elegirlos, como parte del proceso de instalación, para que la seguridad en Internet empiece con la acción del propio usuario. El objetivo principal es reducir la saturación de las políticas de cookies de las páginas web y que sea el propio navegador quien garantice nuestra privacidad y una navegación más segura convirtiéndose en gestor del consentimiento.

Metadatos: son aquellos datos que describen otros datos, es decir, la información que dejamos y creamos al navegar por la red; este tipo de información personal como la geolocalización, el historial de visitas, las fechas y horas de conexión y conversaciones, sólo podrá ser tratada por razones de seguridad, para evitar fraudes o detectar fallos técnicos. Se trata de información de un enorme valor comercial, lo que puede verse afectado si no se otorga el consentimiento.

Publicidad: será necesario el consentimiento libre, específico, explícito, informado e inequívoco de los usuarios

para poder llevar a cabo la misma en espacios *on line*; lo que afectará considerablemente a las técnicas vigentes de marketing.

Aspectos fundamentales y en definitiva, razones que han provocado que el texto esté aún en fase de debate y que aunque a todas luces su protección sea más notable y específica para el entorno digital, se deba esperar a que un mayor consenso permita su publicación y puesta en marcha.

6.LA RESPONSABILIDAD DE LOS PRESTADORES DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN

La extraordinaria expansión de las redes de telecomunicaciones y de Internet como vehículo de transmisión e intercambio de todo tipo de información ofrece innumerables ventajas pero también tropieza con algunas incertidumbres jurídicas que es preciso aclarar para generar en todos los intervinientes la confianza necesaria en este nuevo medio pudiendo determinar, en el caso de que fuera necesario, la responsabilidad en la que cada cual puede incurrir y especialmente en el caso de los prestadores de servicios que no infringen de forma directa la normativa sino que son más bien el vehículo utilizado por otros que pueden llegar a cometer infracciones relacionadas con los derechos al honor, la intimidad, la imagen y la protección de datos y en materia de propiedad intelectual (252).

Esta es la finalidad de la Ley 34/2002 (253) que como ella misma indica acoge un concepto amplio de lo que son los *servicios de la sociedad de la información,* para englobar en el mismo de un lado, la contratación de bienes y servicios por vía electrónica y el suministro de información por dicho medio, como el que efectúan los periódicos o revistas que se pueden encontrar en la red y de otro lado, las actividades de intermediación relativas a la provisión de acceso a la red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, al alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios, así por ejemplo, la descarga de archivos o vídeos, siempre que represente una actividad económica para el prestador.

Los servicios mencionados son llevados a cabo por operadores de telecomunicaciones, proveedores de acceso a Internet, portales, motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades indicadas.

El lugar de establecimiento del prestador de servicios es un elemento esencial pues de él depende que sea de aplicación la normativa española y la determinación de las autoridades competentes para el control de su cumplimiento. El prestador del servicio se entiende establecido en el lugar desde el que se dirige y gestiona la actividad económica que desarrolla (254).

La cuestión que queremos plantear ahora es si los prestadores de servicios de intermediación, como personas físicas o jurídicas que proporcionan alguno de los servicios antes mencionados, pueden incurrir en responsabilidad civil, dado que desde su posición colaboran en la divulgación a través de la red de contenidos de los que no son autores y que en ocasiones tampoco conocen, pero que pueden ocasionar daños a terceros cuando vulneran sus derechos al honor, a la intimidad, a la imagen o a la protección de datos o si por el contrario, esta responsabilidad incumbe exclusivamente al autor material del contenido en cuestión, ya sea un particular, un profesional de los medios o un medio de comunicación institucionalizado (255). Cobra, además, especial transcendencia esta cuestión en relación con el derecho a la supresión de datos y los motores de búsqueda, que trataremos en el capítulo siguiente.

Los artículos 13 a 17 de la LO 34/2002 regulan el régimen de responsabilidad de los prestadores de servicios a quienes se considera sujetos a la responsabilidad civil, penal o administrativa correspondiente, para lo que se

aplicará la normativa vigente, sin perjuicio de la responsabilidad específica prevista por esta norma, que establece un particular régimen de exención de responsabilidad al que nos vamos a referir inmediatamente, para los prestadores de servicios por el ejercicio de actividades de intermediación y no en otro caso (256).

Así, el artículo 16, para el caso de los servicios de intermediación consistentes en albergar los datos proporcionados por el destinatario del servicio, (257) establece que *no serán responsables* de la información almacenada a petición del mismo siempre que se den dos requisitos; de un lado, que no tuvieran conocimiento efectivo de que esa actividad o información almacenada es ilícita o lesiona bienes o derechos de un tercero; y por otro lado, si tuvieran dicho conocimiento, que hubieran actuado con la diligencia necesaria para retirar los datos o bien hacer imposible el acceso a los mismos.

Analicemos los dos presupuestos que se exigen para que se tenga en cuenta la exención de responsabilidad. En primer lugar, debemos plantearnos cómo saber si el prestador del servicio tiene el conocimiento efectivo de haber alojado un contenido ilícito y posteriormente considerar qué debemos entender por actuar con la diligencia necesaria.

Si hacemos una interpretación literal de la norma, el mismo artículo explica que se entiende que hay un conocimiento efectivo cuando ya un órgano competente ha declarado la ilicitud de los datos, ha ordenado su retirada, que se imposibilite el acceso a los mismos o ha declarado la existencia de la lesión y el prestador conociera la correspondiente resolución. Es un medio seguro de conocimiento y de imputación del mismo al intermediario pero que puede causar importantes perjuicios en los derechos que estamos tratando.

Ahora bien, si hacemos una interpretación sistemática y más acorde a la finalidad de la directiva y de la propia LO 34/2002, que no es otra que generar la confianza necesaria en el empleo de Internet, se puede deducir que fuera del caso anterior, cabe presumir *iuris tantum* que el prestador no tiene dicho conocimiento efectivo y en su caso, si este conocimiento se alegare por el perjudicado deberá poder acreditarlo para que se impute a aquél la correspondiente responsabilidad (258); dicha acreditación vendrá de la mano de la existencia de hechos o circunstancias a partir de las cuales un intermediario diligente debiera deducir ese carácter ilícito, incluyendo su propia investigación, la notificación de terceros o de la propia víctima, o que la ilegalidad sea evidente, obvia y manifiesta, sin necesidad de esperar la correspondiente resolución que la declare (259); todo ello con la finalidad fundamental de, en su caso, aminorar los perjuicios que se pueden ocasionar a terceros pues si la única fuente de conocimiento fueran las sentencias y resoluciones de organismos competentes, llevaría demasiado tiempo dar satisfacción a las víctimas, se incrementarían los perjuicios y no se evitaría que en el ínterin se cometieran nuevas infracciones (260). Sólo bajo este prisma tiene sentido la exención de responsabilidad, pues reducir injustificadamente la posibilidad de demostrar la obtención del conocimiento efectivo de la ilicitud de los contenidos almacenados, amplia correlativamente el ámbito de la misma, en perjuicio de quienes ven lesionados sus derechos (261).

La jurisprudencia del Tribunal Supremo ha profundizado en esta cuestión que es abordada con detalle, entre otras, en la sentencia de 7 de enero de 2014. (262) En ella, tras analizar los artículos 13 y 16 de la LO 34/2002, se exponen dos interpretaciones doctrinales del concepto *conocimiento efectivo*. La primera, basada en su propia literalidad y en los antecedentes legislativos y prelegislativos de la Ley, sostiene que sólo podrá afirmarse su concurrencia, en presencia de una previa resolución de un órgano competente acerca de la ilicitud de los datos en cuestión. La segunda considera que la directiva, de la que procede la Ley, no excluye que pueda probarse la existencia de conocimiento efectivo de cualquier otra manera; entendiendo que su prueba puede hallarse no solamente en la notificación de la parte afectada sino también en la forma e información que rodean la actividad de alojamiento o enlace.

En el caso concreto que se valora, la difusión de expresiones insultantes y vejatorias a través del foro de la web de una conocida revista de vídeo juegos contra el propietario de un negocio de informática, se tienen en cuenta dos circunstancias; de un lado, que los contenidos son graves, que su ilicitud es evidente por sí sola, que su

ilegalidad es patente y que incluso pudieran tipificarse penalmente y de otro lado, que el contenido pudo razonablemente conocerse, pues las conversaciones se mantuvieron durante un largo periodo de tiempo, con el consistente número de entradas producidas.

Se concluye que hubo dicho conocimiento en atención a que quedó probado: 1. Si bien no se podía filtrar a priori la información que se iba incorporando en los foros de Internet, contaba en su web con sistemas de control, detección y moderación de su contenido que no se activaron o no funcionaron correctamente. 2. Al no cuestionarse que las manifestaciones vertidas atentaban contra el honor, se debió reaccionar frente a aquellas opiniones y prohibir el acceso a la página 3. Tenía medios para identificar y localizar al autor de las opiniones vertidas y adoptar medidas al respecto. 4. La circunstancia de no haber una resolución declarando la ilicitud no debe ser un obstáculo, pues la facilidad y rapidez en la difusión de las opiniones, siendo la intromisión en el honor tan notoria, multiplicaría los perjuicios ocasionados pudiendo llegar a ser irreparables. Así, al conocimiento efectivo se debe añadir el no haber actuado con la diligencia debida. En atención a ambas circunstancias, entiende el juzgador que no procede aplicar la exención de responsabilidad recogida en la norma.

Por otra parte y en cuanto a la obligación de actuar con la diligencia necesaria debería ésta poder exigirse en dos momentos diferentes; de un lado, para retirar los datos o hacer imposible el acceso a los mismos una vez que se tiene conocimiento de que la actividad o la información almacenada es ilícita o lesiona bienes o derechos de un tercero susceptibles de indemnización; para ello se habrá de actuar con prontitud, respetando el principio de libertad de expresión; pero además también como indica el considerando 48 de la directiva, se debe exigir a los prestadores de servicios una diligencia natural y razonable para detectar y prevenir determinados tipos de actividades ilegales. No se trata de una obligación general de supervisión que el artículo 15 de la directiva no considera viable (263), pero sí de trasladar a quienes realizan este tipo de actividades la necesidad de compatibilizarlas con el respecto a los derechos fundamentales de todos (264). Adquieren en este aspecto especial dimensión los códigos de conducta, aun siendo de carácter voluntaria su elaboración y libre la adhesión a los mismos.

Las exenciones previstas y con los requisitos explicados sólo se aplicarán, por tanto, a aquellos casos en los que la actividad del prestador de servicios desempeña un papel neutro, realiza una actividad meramente técnica, automática y pasiva; no tiene el control del contenido ni del negocio pues sólo facilita el acceso a una red de comunicación; y en este sentido, se pueda afirmar que no tiene conocimiento ni control de la información que se almacena o transmite, cuestión de hecho que corresponderá determinar, en su caso, a la autoridad judicial (265).

A modo de conclusión de todo lo expuesto, considero que si está en la mente del legislador europeo elaborar una nueva directiva sobre esta materia que refleje de una manera más acorde a la realidad la situación dinámica de las plataformas, debe hacerlo teniendo en cuenta que ese papel neutral o pasivo en muchas ocasiones da lugar a la comisión de delitos (266) y puede generar importantes intromisiones en los derechos que estamos analizando; por ello, una de las prioridades debiera ser actualizar el régimen jurídico de las exenciones siendo uno de sus objetivos la adopción de medidas de prevención que eleven el nivel de diligencia exigida y que a ser posible, sin interferir en los derechos a la libertad de expresión e información, lo que no es fácil (267), consigan en la medida de lo admisible evitar que aquéllas se conviertan en fuente de actuaciones generadoras de responsabilidad civil, penal y administrativa.

No obstante lo anterior y si en aras de una mayor prevención, se optare por eliminar las exenciones, determinar la responsabilidad de los intermediarios dependería de cada legislación nacional; si nos ceñimos al ámbito civil, como es lógico, la eliminación de la exoneración no equivaldría a una correlativa y automática imputación de responsabilidad, sino que deberíamos acudir a la LO 1/82 o al Reglamento 679/2016 así como a las reglas de los artículos 1902 y siguientes del Código civil, para según el caso, poder determinar la correspondiente responsabilidad; entendiendo que si a través de estas plataformas se produjera la intromisión en los derechos estudiados, esta se identificaría con el daño, quedando a merced de la autoridad judicial la determinación de la parte de responsabilidad de la que deberían responder aplicando las normas generales, de un lado, los titulares

de los contenidos ofensivos y de otro lado, los servicios de intermediación (268). Para estos casos cobraría una especial trascendencia el haber extremado la diligencia en su actuación por parte de estos últimos.

Si las exenciones desaparecen, los servicios de intermediación se verán obligados a tener conocimiento cierto del contenido para el que prestan sus herramientas y acreditar la diligencia debida se convertirá en el *quid* de la cuestión en muchas ocasiones. Esto redundará en mayor prevención y menores daños, pero de un algún modo desvirtuará la naturaleza propia de dichos servicios.

BIBLIOGRAFÍA

-ARMADA VILLAVERDE, María Elena y LÓPEZ BUSTABAD, Ignacio Javier (2019). "El Reglamento general de protección de datos ante el fenómeno del *Big Data*". *Revista Aranzadi de Derecho y nuevas tecnologías*, núm. 51, págs. 1 a 26.

-ARROYO AMAYUELAS, Esther (2020). "La responsabilidad de los intermediarios en Internet, ¿Puertos seguros a prueba de futuro?". *Cuadernos de Derecho Transnacional*. Vol. 12, núm. 1, págs. 808 a 837.

-BELLO JANEIRO, Domingo (2015). "Comentario a la sentencia de 17 de septiembre de 2014". *Revista Cuadernos Civitas de Jurisprudencia civil*. Núm. 98, págs. 1 a 14. BIB 2015, 2019.

-BERROCAL LANZAROT, Ana Isabel (2019). *Estudio jurídico-crítico sobre la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. Análisis conjunto del Reglamento UE 2016/679 y de la LO 3/2018.* Reus. Madrid.

-BOTANA GARCÍA, Gema Alejandra (2016). "Crónica anunciada de un Reglamento de protección de datos en la Unión Europea". *Actualidad Civil*, núm. 6, págs. 1 a 22.

-COTINO HUESO, Lorenzo (2015). "El conflicto entre las libertades de expresión e información en Internet y el derecho a la protección de datos. El derecho al olvido y sus retos: un falso derecho a juzgar por un falso tribunal". *Derecho de la información: El ejercicio del derecho a la información y su jurisprudencia.* Centro de estudios políticos y constitucionales. Madrid, págs. 391 a 433.

-DAVARA RODRÍGUEZ, Miguel Ángel (2016). "Reglamento europeo sobre protección de datos". *Actualidad Administrativa*, núm. 7, págs. 1 a 6.

-DE MIGUEL ASENSIO, Pedro (2013). "Responsabilidad de los intermediarios en Internet y Ley aplicable en la reciente jurisprudencia del Tribunal Supremo". Disponible en: http://pedrodemiguelasensio.blogspot.com/ (27 de mayo de 2013).

-DÍAZ ALABART, Silvia (2020). La protección de los datos y contenidos digitales de las personas fallecidas. Reus, Madrid.

-ESPIRITUSANTO NICOLÁS, Óscar (2013). "Periodismo ciudadano: colaboración y evolución positiva". *Cuadernos de periodistas*. *Revista de la Asociación de la prensa de Madrid*, núm. 27, págs. 57 a 65.

-GUICHOT, Emilio (2019). "El reconocimiento y desarrollo del derecho al olvido en el Derecho europeo y español". *Revista de Administración pública*, núm. 209, págs. 45 a 92.

-LORENTE LOPEZ, María Cristina (2014). "Los derechos al honor, a la intimidad personal y familiar y a la propia imagen en la jurisprudencia más reciente". *Los derechos a la intimidad y a la privacidad en el siglo XXI*. Dykinson. Madrid, págs. 131 a 155.

-MAESTRE RODRÍGUEZ, Javier (2017). "La responsabilidad de los prestadores de servicios de la Sociedad de

la información y el concepto de público nuevo". *Revista Derecho & Sociedad*, núm. 49, págs. 77 a 86.

-MARTÍNEZ-MARTÍNEZ, Silvia (2014). "El derecho a la intimidad en el periodismo participativo". *Los derechos a la intimidad y a la privacidad en el siglo XXI*. Dykinson. Madrid, págs. 157 a 180.

-MORETÓN SANZ, María Fernanda (2020). "El contenido personal de las redes sociales y voluntades digitales: Historia digital, disposiciones testamentarias y tutela de la privacidad". *Nuevas tecnologías y responsabilidad civil*. Reus. Madrid, págs. 193 a 247.

-NOGUEIRA BLANCO, José (2018). "Reglamento General de protección de datos y Big Data". *Actualidad Civil*, núm. 5, págs. 1 a 12.

-PAUNER CHULVI, Cristina (2015). "La libertad de información como límite al derecho a la protección de datos personales: la excepción periodística". *Teoría y realidad constitucional*. UNED, núm. 36, págs. 377 a 395.

-PAUNER CHULVI, Cristina (2014). "Implicaciones del futuro Reglamento europeo sobre protección de datos en la libertad de información". *Los derechos a la intimidad y a la privacidad en el siglo XXI*. Dykinson. Madrid, págs. 181 a 198.

-PLAZA PENADÉS, Javier (2018). "El nuevo marco normativo de la protección de datos". *Actualidad Civil*, núm. 5, págs. 1 a 12.

-RECIO GAYO, Miguel (2018). "Los nuevos y renovados derechos en protección de datos en el RGDP, así como sus limitaciones". *Actualidad Civil*, núm. 5, págs. 1 a 18.

-SÁNCHEZ RODRÍGUEZ, Gabriel (2013). "El valor de la información verdadera". *Cuadernos de periodistas*. *Revista de la Asociación de la prensa de Madrid,* núm. 27, págs. 66 a 71.

-SEMPERE NAVARRO, Antonio Vicente (2020). "Un apunte sobre la grabación mediante cámaras (Al hilo de la STS-CIV 600/2019, de 7 de noviembre)". *Revista Aranzadi Doctrinal*, págs. 1 a 6.

-VIVAS TESÓN, Inmaculada (2020). "La protección de datos personales en el ámbito de los registros de la propiedad, mercantil y de bienes muebles". *Nuevas tecnologías y responsabilidad civil*. Reus. Madrid, págs. 147 a 191.

-YANGUAS GÓMEZ, Roberto (2012). *Contratos de conexión a Internet, Hosting y búsqueda*. Civitas, Madrid.

173.SEMPERE NAVARRO, Antonio V (2020). "Un apunte sobre la grabación mediante cámaras (Al hilo de la STS-CIV 600/2019, de 7 de noviembre)". *Revista Aranzadi Doctrinal*, pág. 4. Como dice VIVAS TESÓN, Inmaculada (2020). "La protección de datos personales en el ámbito de los registros de la propiedad, mercantil y de bienes muebles". *Nuevas tecnologías y responsabilidad civil*. Reus. Madrid, pág. 147, es innegable que nuestros datos personales se han convertido en una poderosa fuente de energía renovable del mundo globalizado y digital del siglo XXI, pues son la base de la toma de innumerables decisiones y un recurso clave para el impulso económico, científico y tecnológico. Sin embargo, su tratamiento, uso y destino puede, en ocasiones, resultar nocivo para su titular cuando resulta violada su privacidad, dado que este desnudo no consentido de su yo (personal o patrimonial), puede acarrearle consecuencias perjudiciales e irreparables.

174.STC 292/2000. Resuelve un recurso de inconstitucionalidad promovido por el Defensor del Pueblo frente a determinados artículos de la LO 15/99, de 13 de diciembre de protección de datos de carácter personal.

175.Recogido también en el art. 8 de la Carta de derechos fundamentales de la Unión Europea.

176.En el reconocimiento de este carácter autónomo ha tenido decisiva importancia la labor del TJUE. A nivel legislativo, por su parte, se consideró su condición independiente en la Directiva 95/46/CE y en la Carta de derechos fundamentales de la UE.

177.Para PLAZA PENADÉS, Javier (2018). "El nuevo marco normativo de la protección de datos". *Actualidad Civil*, núm. 5, pág. 5, la exclusión de las personas jurídicas con carácter general, más allá de que tiene su acomodo en el principio de dignidad humana, parte de una concepción excesivamente dogmática, en la que se cree que todos los datos de las empresas son públicos y en el que se desconoce tanto la existencia de datos que las empresas y personas jurídicas quieren mantener en secreto, de forma reservada y bajo su control, como que el daño derivado del tratamiento erróneo de los datos es el mismo en las personas físicas que en las jurídicas.

178.La STC al hablar de los límites se refiere al art. 105 b) CE que dice que la Ley regulará el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecta a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas.

179.Para BOTANA GARCÍA, Gema Alejandra (2016). "Crónica anunciada de un Reglamento de protección de datos en la Unión Europea". *Actualidad Civil*, núm. 6, pág. 2, la necesidad de una nueva regulación para toda la Unión Europea era más que evidente sobre todo en dos ámbitos: el uso de las redes sociales y el acceso de las autoridades públicas a los datos transferidos bajo los términos del *Escudo de privacidad* que conforma el nuevo marco para las transferencias internacionales de datos personales con fines comerciales a empresas de Estados Unidos.

180.Art. 2 Reglamento. El art. 4 considera *tratamiento* cualquier operación realizada sobre datos personales, como la recogida, registro, organización, estructuración, conservación, adaptación, modificación, extracción, consulta, utilización, difusión, comunicación por transmisión, cotejo o interconexión, limitación, supresión o destrucción; y considera *datos personales* a toda información sobre una persona física identificada o identificable.

181.El art. 4 del Reglamento considera *responsable del tratamiento* a la persona física o jurídica, autoridad pública, servicio u otro organismo que solo o junto con otros determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la UE o de los Estados miembros. Considera, por otra parte, *encargado del tratamiento* a la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. A las obligaciones de ambos se refiere el art. 28 LO 3/2018.

182.Art. 3 Reglamento. Debemos tener en cuenta que nos encontramos en presencia de dos ordenamientos jurídicos distintos que se han desarrollado en paralelo, si bien se ha intentado asegurar la coherencia y compatibilidad de los mismos; de un lado, los Estados que no son miembros de la UE y sí lo son del Consejo de Europa y parte del CEDH y del Convenio 108 con su protocolo adicional de 2001 y de otro lado, los que sí forman parte de la misma, que además de aquella legislación deben atender a la Carta de los derechos fundamentales de la Unión Europea del año 2000, al Tratado de funcionamiento de la Unión Europea, a la Directiva 95/46/UE ya derogada y al Reglamento 2016/679. También es de interés la Directiva 2002/58/CE relativa al tratamiento de los datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento 2001/45 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por instituciones y organismos comunitarios y a la libre circulación de estos datos. En atención a esta distinción, es importante también acudir al corpus de jurisprudencia del TEDH y del TJUE.

183.Art. 5 Reglamento. Este precepto hace referencia a los principios de licitud, lealtad y transparencia; el principio de limitación de la finalidad; principio de minimización de datos; principio de exactitud; principio de limitación del plazo de conservación; principios de integridad y de confidencialidad. Según el art. 5.2 de la LO 3/2018, la obligación de confidencialidad será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

184.El principio de *accountability* o responsabilidad proactiva exige la capacidad de demostrar que se cumple con el RGPD por el responsable del tratamiento. Para NOGUEIRA BLANCO, José (2018). "Reglamento General de protección de datos y Big Data". *Actualidad Civil*, núm. 5, pág. 2, este principio se basa en que no existen simplemente normas materiales que cumplir, sino que cada organización ha de dotarse de sus propias normas de cumplimiento en función de la intensidad y la escala de tratamientos de datos que realice; por ello, además, se pone el foco en la elaboración de códigos de conducta como mecanismos de autorregulación de las organizaciones.

185.*Vid.* arts. 12 a 14 del Reglamento y art. 11 LO 3/2018. DAVARA RODRÍGUEZ, Miguel Ángel (2016). "Reglamento europeo sobre protección de datos". *Actualidad Administrativa*, núm. 7, pág. 6, destaca como premisa básica que quienes tratan datos deben tener siempre presente que los datos que se tratan pertenecen a su titular y no a quien está operando con ellos, que tendrá el derecho a procesarlos si obtuvo el correspondiente consentimiento, lo que debería hacerse siempre desde la base de una cultura de protección. Para RECIO GAYO, Miguel (2018). "Los nuevos y renovados derechos en protección de datos en el RGDP, así como sus limitaciones". *Actualidad Civil*, núm. 5, pág. 2, el Reglamento tiene por

objeto que el interesado tome el control de sus datos personales a través de una serie de derechos clave que le conceden mayor poder para protegerse. Al reforzar los derechos en materia de protección de datos se pretende también generar o impulsar la confianza, por una parte en la economía digital en particular en el Mercado Digital único y por otra parte, garantizar un alto nivel de protección de datos igual para todos los ciudadanos y consumidores europeos.

186.*Vid.* considerando 65 y art. 17 del Reglamento; también art. 15 LO 3/2018 y arts. 93 y 94 LO 3/2018, en relación con las búsquedas en Internet y servicios de redes sociales y equivalentes. Para GUICHOT, Emilio (2019). "El reconocimiento y desarrollo del derecho al olvido en el Derecho europeo y español". *Revista de Administración pública*, núm. 209, pág. 38, en el Reglamento se regula ya el derecho al olvido como sinónimo de derecho de supresión, denominaciones que sustituyen al anteriormente llamado derecho de cancelación.

187.*Vid.* art. 32 LO 3/2018. El incumplimiento de esta obligación se considera infracción muy grave en el art. 72 LO 3/2018.

188.*Vid.* art. 20 del Reglamento y arts. 17 y 95 LO 3/2018.

189.*Vid.* arts. 21 y 22 del Reglamento y art. 18 LO 3/2018. Se tratará en el capítulo IV para relacionarlo con el derecho al olvido. La elaboración de perfiles o *profiling* consiste en el tratamiento automatizado de datos personales para evaluar determinados aspectos relativos a características intrínsecas de las personas que permiten analizar y predecir sus intereses y comportamiento. Se reconoce, además, el derecho de cualquier interesado a oponerse a las decisiones basadas únicamente en el tratamiento automatizado de sus datos cuando puedan afectarle de alguna manera.

190.*Vid.* arts. 7 y 8 del Reglamento y arts. 6 y 7 LO 3/2018. El art. 8 de la Carta de los derechos fundamentales de la Unión Europea considera el consentimiento como una de las dos fuentes de legitimación, junto a la Ley, del tratamiento o la cesión de los datos.

191.El contenido del derecho de información se ha ampliado considerablemente con la nueva legislación. Los datos mencionados corresponderían a una primera capa o nivel de carácter básico que se produce en el mismo momento en que se recogen los datos. En una segunda capa o información más detallada se incluirían, por ejemplo, los datos del responsable y del delegado de protección de datos; plazos y criterios de conservación de los datos; destinatarios y categorías de los mismos; descripción ampliada de los fines del tratamiento; detalles de la base jurídica del tratamiento; derecho a retirar el consentimiento prestado; derecho a reclamar ante la autoridad de control; cómo ejercer los derechos de acceso, rectificación, supresión, portabilidad de datos; garantías y normas corporativas vinculantes.

192.*The Guidelines 05/2020 on consent under Regulation 679/2016* (apartados 38 a 41), en relación con la interpretación del art. 7.4 del Reglamento considera que supeditar la celebración de un contrato o la prestación de un servicio al consentimiento al tratamiento de datos personales no necesarios es determinante para considerar que el consentimiento no se ha prestado libremente.

193.Dice PLAZA PENADÉS, Javier (2018). "El nuevo marco normativo de la protección de datos". *Actualidad Civil*, núm. 5, pág. 7, que se trata de dos ámbitos totalmente distinguibles y separables que requieren consentimiento específico, por lo que realizar una cesión o transferencia sin consentimiento puede ser un ilícito muy grave y desde luego un ilícito civil que en caso de generar daños obligaría a su reparación. Por otra parte, y en relación con la transferencia internacional de datos, *vid.* arts. 44 a 50 del Reglamento y arts. 40 a 43 LO 3/2018.

194.A juicio de ARMADA VILLAVERDE, María Elena y LÓPEZ BUSTABAD, Ignacio Javier (2019). "El Reglamento general de protección de datos ante el fenómeno del *Big Data*". *Revista Aranzadi de Derecho y nuevas tecnologías*, núm. 51, pág. 8, cabe la forma implícita del consentimiento, pues si sólo pudiera ser explícito, el legislador lo hubiera establecido así, tal y como lo exige en el supuesto de tratamiento de categorías especiales de datos en el art. 9. 2 a) del Reglamento.

195.El art. 6. 1. f) del Reglamento recoge la llamada *regla del interés legítimo*. Tratamientos que pueden estar fundados en el interés legítimo son los relativos a *la libertad de información y expresión*, la prevención del fraude o mal uso de servicios, finalidades científicas, estadísticas o de investigación y datos de contacto y relativos a la función o puesto desempeñado por personas físicas que presten servicios en una persona jurídica, entre otros.

196.*Vid.* arts. 35 y 36 del Reglamento. No llevar a cabo esta evaluación del impacto en los supuestos en los que es exigible se considera como infracción grave en el artículo 73 de la LO 3/2018.

197.*Vid.* art. 25 del Reglamento. El objetivo de la *Privacy by design* y la *Privacy by default* es que los principios de protección de datos estén incluidos dentro de las organizaciones de manera que estén presentes a lo largo de toda la vida del tratamiento, desde el momento en que se diseña, se pone en marcha y hasta que se suprime o finaliza. (Considerando

78 del Reglamento).

198.*Vid.* arts. 37 a 39 del Reglamento y arts. 34 a 37 LO 3/2018. El art. 34 señala los supuestos en los que su designación es obligatoria; así, entre otros, los colegios profesionales, los centros docentes y Universidades, los prestadores de servicios de la sociedad de la información, los establecimientos financieros de crédito, las entidades aseguradoras y reaseguradoras, empresas de servicios de inversión reguladas por la legislación del mercado de valores, distribuidores y comercializadores de energía eléctrica y gas natural, centros sanitarios legalmente obligados al mantenimiento de historias clínicas, empresas de seguridad privada, federaciones deportivas que traten datos de menores de edad, operadores que desarrollan actividades de juego a través de canales electrónicos, informáticos y telemáticos conforme a la normativa de regulación del juego. Fuera de estos casos, se puede designar de manera voluntaria.

199.Consciente de la necesidad de identificar a profesionales competentes para desempeñar estas funciones, la AEPD ha puesto en marcha la posibilidad, con carácter voluntario, de obtener la correspondiente certificación de delegado de protección de datos, que implica el reconocimiento para el desarrollo de estas competencias de acuerdo con lo dispuesto en el Reglamento. Para ello se han de cumplir unos requisitos de formación y superar un examen.

200.*Vid.* art. 13 Directiva 95/46/CE y arts. 23 y 24 de la LO 15/99 (Disposición adicional 14 y Disposición derogatoria única LO 3/2018). *Vid*. art. 23 y considerando 73 del Reglamento. Las limitaciones deben ajustarse a lo dispuesto en el art. 52 de la Carta, en el art. 8.2 CEDH y art. 11 Convenio 108.

201.Es fundamental determinar la base legal del tratamiento pues el art. 9 del Reglamento lo prohíbe cuando revele el origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, la afiliación sindical, datos genéticos, datos biométricos, datos relativos a la salud o a la orientación sexual; con las excepciones que en el mismo precepto se contemplan.

202.Así por ejemplo, la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo establece en su art. 32.3 que no será de aplicación al tratamiento de estos datos la obligación de información, ni las normas referidas al ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

203.Por otra parte, el art. 82 LO 3/2018, recoge el *derecho a la seguridad digital,* en función del cual los usuarios tienen, además, derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet.

204.Según NOGUEIRA BLANCO, José (2018). “Reglamento General de protección de datos y Big Data”. *Actualidad Civil*, núm. 5, pág. 7, un riesgo se puede materializar en amenazas de tres tipos: acceso ilegítimo a los datos, modificación no autorizada y eliminación de los mismos; lo que atenta contra la confidencialidad, la integridad y la disponibilidad de aquéllos. Así, por ejemplo, *hackeos* de sistemas informáticos, el borrado accidental de registros o la pérdida de dispositivos electrónicos.

205.*Vid.* arts. 40 a 43 del Reglamento y arts. 38 y 39 LO 3/2018. *Vid.* también art. 63 del Reglamento, sobre el mecanismo de coherencia.

206.*Vid.* arts. 63 a 69 LO 3/2018 en relación con los procedimientos tramitados por la AEPD. Estos procedimientos se rigen por lo dispuesto en el Reglamento, en la propia LO, disposiciones reglamentarias que se dicten en su desarrollo y con carácter subsidiario por las normas generales sobre los procedimientos administrativos. También se puede hacer uso de los mecanismos de mediación, procedimientos extrajudiciales y otros procedimientos de resolución de conflictos previstos por el art. 40 del Reglamento.

207.Se puede tratar de responsabilidad penal, por ejemplo, por la difusión y cesión a terceros de imágenes o vídeos que menoscaban la intimidad de una persona física sin su consentimiento; responsabilidad en el ámbito laboral, por ejemplo, en relación con el derecho a la desconexión digital; y responsabilidad civil por los perjuicios y daños morales y patrimoniales causados a la persona afectada.

208.En el caso de Andalucía esta previsión normativa ha quedado materializada en la Orden de 1 de agosto de 2019 por la que se determina el inicio del ejercicio de las funciones en materia de protección de datos de carácter personal por el Consejo de la Transparencia y la protección de datos de Andalucía, quedando limitado su ámbito competencial al ámbito territorial de la Comunidad Autónoma. Este Consejo fue creado por el art. 43 de la Ley 1/2014, de 24 de junio, de Transparencia pública de Andalucía y se configura pues como la autoridad independiente de control en materia de protección de datos. Tiene la consideración de Administración institucional, por lo que posee personalidad jurídica y plena independencia y autonomía en el ejercicio de sus funciones. Sus Estatutos fueron aprobados por el Decreto 434/2015, de

29 de septiembre. Actualmente está presidido por Manuel Medina Guerrero, quien actúa asistido por la Comisión Consultiva de la transparencia y la protección de datos. Por su parte, en Cataluña existe la Autoridad catalana de protección de datos y en el País Vasco, la Agencia vasca de protección de datos.

209.*Vid*. art. 82 del Reglamento. El Considerando 146 del Reglamento dice que el concepto de daños y perjuicios debe interpretarse en sentido amplio a la luz de la jurisprudencia del Tribunal de Justicia, con la finalidad de que se respeten plenamente los objetivos del Reglamento. Los interesados deberán recibir una indemnización total y efectiva por los daños y perjuicios sufridos. La vía judicial para reclamar las indemnizaciones que correspondan dependerá del ámbito, público o privado, en que se realice el tratamiento de datos que ocasiona los daños.

210.*Vid.* Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, art. 32. 1 y 2. La reclamación deberá agotar la vía administrativa para poder acudir ante el tribunal contencioso-administrativo.

211.*Vid.* arts. 83 y 84 del Reglamento y arts. 70 a 78 LO 3/2018. El Reglamento endurece el régimen de sanciones pues la infracción de las disposiciones previstas en el artículo 83. 5 se sancionará con multas administrativas que pueden llegar hasta los 20.000.000 de euros, o tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total global del ejercicio financiero anterior, optándose por la de mayor cuantía. En España la potestad sancionadora la tiene la AEPD que impuso sanciones de 300.000 € a *WhatsApp* y *Facebook* pues la primera comunicó datos a la segunda que posteriormente los trató para sus propios fines y en ambos casos sin el consentimiento necesario. Recientemente la empresa sueca H&M ha sido sancionada con una multa de 35.3 millones de euros por guardar información de sus empleados del centro de *Nuremberg*; desde datos inocuos, hasta datos familiares y relativos a creencias religiosas para tener un perfil detallado de cada trabajador para la toma de decisiones relativas a su empleo. Es la multa más alta, hasta ahora, de las impuestas en este país por violación del Reglamento 679/2016. Todo ello a instancia de una investigación llevada a cabo por el Comisionado Estatal de protección de datos de Hamburgo.

212.*Vid.* considerandos 148, 149 y 150 del Reglamento.

213.El art. 78 LO 3/2018, determina el plazo de prescripción de las sanciones en función de su importe. Así si es igual o inferior a 40.000 €, el plazo será de un año; entre 40.001 y 300.000 €, será de dos años, y de tres, si el importe de la sanción es superior a 300.000 €.

214.*Vid.* art. 30 Reglamento y art. 31 LO 3/2018. No disponer de este registro, se considera infracción grave en el art. 73 del Reglamento. Este registro se puede organizar a partir de los *ficheros* que tienen notificados los responsables en el RGPD detallando todas las operaciones que se realizan sobre cada conjunto estructurado de datos o configurarlo *ex novo* con arreglo a criterios determinados.

215.Sobre esta materia, *vid*. DÍAZ ALABART, Silvia (2020). *La protección de los datos y contenidos digitales de las personas fallecidas*. Reus, Madrid. El considerando 27 del Reglamento dice que éste no se aplica a la protección de datos personales de personas fallecidas, si bien deja el margen necesario a los Estados para que establezcan normas en este sentido. El art. 96 LO 3/2018 regula el derecho al testamento digital. Sobre este tema, *vid.* MORETÓN SANZ, María Fernanda (2020). “El contenido personal de las redes sociales y voluntades digitales: Historia digital, disposiciones testamentarias y tutela de la privacidad”. *Nuevas tecnologías y responsabilidad civil*. Reus. Madrid, págs. 193 a 247.

216.*Vid.* arts. 44 a 56 LO 3/2018. El RD 428/1993, de 26 de marzo, aprueba el Estatuto de la Agencia Española de protección de datos.

217.Actualmente la directora de la Agencia española de protección de datos es Mar España Martí.

218.Sustituye al conocido como *Grupo de trabajo del art. 29*. *Vid*. arts. 68 a 76 del Reglamento. Actualmente la presidencia la ostenta Andrea Jelinek. Un memorando de entendimiento define las condiciones de la cooperación entre el Comité y el Supervisor.

219.*Vid.* arts. 42 y 43 del Reglamento. Los organismos de certificación deben tener conocimientos adecuados en esta materia y estar acreditados por la AEPD, la Entidad Nacional de acreditación o por el Comité europeo de protección de datos.

220.La obtención de esta certificación implica el reconocimiento de calidad en la gestión de los datos, el respeto por las normas europeas en esta materia y la implicación en la defensa de la seguridad y control de los datos personales por los titulares de los mismos. Establece un estándar europeo de privacidad.

221.Lo explicamos en el primer capítulo, pero quizá en este tenga aún mayor vigencia la consideración de la diferencia esencial entre los derechos al honor y la intimidad cuando se trata de la rectificación de la información publicada, pues si bien es cierto que es viable y aconsejable cuando se trata del derecho al honor, albergamos grandes dudas cuando se trata del derecho a la intimidad, aunque sea como dice BELLO JANEIRO, Domingo, (2015). "Comentario a la sentencia de 17 de septiembre de 2014". *Revista Cuadernos Civitas de Jurisprudencia civil*. Núm. 98, pág. 7, para dar la versión de la víctima que seguramente no querrá revelar más hechos privados ni incidir en aspectos que nunca se debieron hacer públicos. Si a ello añadimos el formidable difusor que supone Internet, nos encontramos con un aviso aclaratorio junto a una noticia que atenta contra la intimidad, consiguiendo seguramente el efecto contrario del que se pretende.

222.La Carta de los derechos fundamentales de la Unión Europea recoge en su art. 8 el derecho a la protección de datos de carácter personal y en el art. 11 los derechos a la libertad de expresión y de información y a la libertad de los medios de comunicación y su pluralismo. Por su parte, el art. 52.1, establece que cualquier limitación del ejercicio de los derechos y libertades reconocidos en la misma, debe ser establecida por Ley respetando al mismo tiempo el contenido esencial de dichos derechos y libertades, pues sólo se podrán introducir limitaciones necesarias y que respondan a objetivos de interés general, respetando al mismo tiempo el principio de proporcionalidad. En el mismo sentido la Directiva 95/46/CE en sus considerandos 17 y 37 y art. 9.

223.El art. 85.2 del Reglamento permite excepciones a prácticamente todo el articulado del mismo; únicamente quedan fuera de este ámbito los capítulos I (Disposiciones generales), VIII (Recursos, responsabilidad y sanciones), X (Actos delegados y actos de ejecución) y XI (Disposiciones finales).

224.PAUNER CHULVI, Cristina (2015). "La libertad de información como límite al derecho a la protección de datos personales: la excepción periodística". *Teoría y realidad constitucional*. UNED, núm.36, pág. 378.

225.PAUNER CHULVI, Cristina (2015). "La libertad de información como límite al derecho a la protección de datos personales: la excepción periodística". *Teoría y realidad constitucional*. UNED, núm. 36, pág. 378.

226.*Vid.* considerando 153 y art. 85 del Reglamento. Es importante distinguir como hace PAUNER CHULVI, Cristina (2014). "Implicaciones del futuro Reglamento europeo sobre protección de datos en la libertad de información". *Los derechos a la intimidad y a la privacidad en el siglo XXI*. Dykinson. Madrid, pág. 188, los tratamientos que sirven a funciones de dirección y administración de las empresas y aquéllos que se orientan a la labor editorial o productora; en el primer caso los datos serán almacenados en ficheros que se utilizarán para la gestión de la compañía mientras que en el segundo los datos están destinados a su publicación y difusión como elementos de la noticia o información. Sólo a estos últimos y bajo determinadas condiciones se les puede aplicar la *excepción periodística*; los anteriores se someten plenamente a las disposiciones reguladoras del derecho de protección de datos.

227.Como dice BERROCAL LANZAROT, Ana Isabel (2019). *Estudio jurídico-crítico sobre la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*. Reus. Madrid, pág. 380, dicha exigencia normativa no tiene mucho sentido, si partimos de la aplicación directa del Reglamento, pues no es preciso como en el caso de las directivas una transposición efectiva para completar su eficacia plena; si bien no cabe duda de la obligatoriedad de su cumplimiento y las consecuencias de su no adopción a los efectos de una eventual demanda judicial. A mi juicio, el requerimiento está más en la línea de que esas normas internas complementen y hagan plenamente efectiva su aplicación desarrollando lo dispuesto en el Reglamento.

228.Se consideran como tales el censo promocional, los repertorios telefónicos, las listas de personas pertenecientes a grupos de profesionales, los diarios y boletines oficiales y los medios de comunicación.

229.Se debe tener presente que existen diferencias importantes entre los países a la hora de considerar el concepto, contenido y límites de la libertad de expresión y, además, en ocasiones se funde y confunde este derecho con el derecho a dar y recibir libremente información.

230.PAUNER CHULVI, Cristina (2014). "Implicaciones del futuro Reglamento europeo sobre protección de datos en la libertad de información". *Los derechos a la intimidad y a la privacidad en el siglo XXI*. Dykinson. Madrid, pág. 192.

231.Sobre esta materia, *vid. Manual de legislación europea en materia de protección de datos* (2018). Disponible en: https://www.echr.coe.int/Documents/Handbook_data_protection_SPA.pdf.

232.En la jurisprudencia del TEDH se hace referencia a *injerencias lícitas*.

233.*Vid*. art. 3 Tratado de la Unión Europea.

234.*Vid*. art. 23. 1 i) del Reglamento. En este sentido, el *Informe 624/2009 del Gabinete jurídico de la AEPD, sobre protección de datos y libertad de expresión e información*, cita la sentencia de la Audiencia Nacional de 12 de enero de 2001.

235.TEDH 27 de junio de 2017: *Satakunnan Markkinapörssi Oy Satamedia Oy contra Finlandia*.

236.TJUE, 13 de mayo de 2014: *Google Spain y Google Inc., contra AEPD y Mario Costeja González*.

237.*Vid. Recomendación de 25 de febrero de 1997*, del Grupo de Trabajo del art. 29 sobre la normativa de protección de datos y los medios de comunicación.

238.La expresión "*incluido* el tratamiento con fines periodísticos", creo que nos permite diferenciar: de un lado, la libertad de expresión que tenemos todos los ciudadanos y la libertad de información como un subtipo de aquélla cuando es ejercida por cualquiera de nosotros y que por tanto se incluiría dentro del concepto genérico de libertad de expresión y de otro lado, la libertad de información entendida como aquélla que llevan a cabo los profesionales de la información y los medios de comunicación institucionalizados a la que se refiere en última instancia la excepción periodística. En este sentido, el art. 10 CEDH.

239.En este sentido, *Vid.* el *Informe 624/2009 del Gabinete jurídico de la AEPD, sobre protección de datos y libertad de expresión e información*. En él se citan numerosas sentencias del TC que avalan la posición preferente de la libertad de información frente a otros derechos constitucionales; dicha doctrina quedó reflejada en el capítulo I de este estudio.

240.Recomiendo la lectura del Informe sobre la transformación de los medios de comunicación. En él se explican con gran claridad los argumentos a favor por ESPÍRITUSANTO NICOLÁS, Óscar (2013). "Periodismo ciudadano: colaboración y evolución positiva". *Cuadernos de periodistas*. *Revista de la Asociación de la prensa de Madrid*, núm. 27, págs. 57 a 65 y los argumentos en contra por SÁNCHEZ RODRÍGUEZ, Gabriel (2013). "El valor de la información verdadera". *Cuadernos de periodistas*. *Revista de la Asociación de la prensa de Madrid,* núm. 27, págs. 66 a 71.

241.MARTÍNEZ-MARTÍNEZ, Silvia (2014). "El derecho a la intimidad en el periodismo participativo". *Los derechos a la intimidad y a la privacidad en el siglo XXI*. Dykinson. Madrid, pág. 161, define el *periodismo participativo* como el tipo de prácticas de colaboración y acción colectiva entre usuarios o ciudadanos y los profesionales que trabajan en una redacción.

242.Anglicismo que se utiliza para designar los bulos o contenidos pseudoperiodísticos difundidos a través de portales de noticias, redes sociales, prensa, radio, televisión cuyo objetivo es la desinformación. Se emiten con la intención deliberada de inducir a error, manipular, desprestigiar o enaltecer.

243.Por poner algún ejemplo, en el caso de las protestas en Birmania en 2007, muchos birmanos acudieron a Internet para a través de sus vídeos y fotos alertar al mundo de cuál era la situación real en su país o en 2009, la fotografía del rescate de los pasajeros tras el amerizaje de urgencia del vuelo 1549 en el río Hudson.

244.COTINO HUESO, Lorenzo (2015). "El conflicto entre las libertades de expresión e información en Internet y el derecho a la protección de datos. El derecho al olvido y sus retos: un falso derecho a juzgar por un falso tribunal". *Derecho de la información: El ejercicio del derecho a la información y su jurisprudencia.* Centro de estudios políticos y constitucionales. Madrid, pág. 396, sostiene que las libertades informativas se reconocen a toda persona (aunque no sea empresa de comunicación o periodista) que emita información veraz o exprese opiniones. PAUNER CHULVI, Cristina (2014). "Implicaciones del futuro Reglamento europeo sobre protección de datos en la libertad de información". *Los derechos a la intimidad y a la privacidad en el siglo XXI*. Dykinson. Madrid, pág. 190. Por su parte, en la pág. 198 afirma que el RGPD asume esta perspectiva e impone una interpretación extensiva del término periodismo, sin exclusividades por razón del sujeto que comunica ni del soporte en que se difunde la información, lo que resulta acorde con el desarrollo de Internet y la proliferación de blogs y páginas personales en las que cualquier persona, y no únicamente los profesionales de la información, tiene la capacidad de informar y trasladar esa información al conjunto de la sociedad.

245.La STC de 15 de octubre de 2015 (LA LEY 139641/2015), que analizaremos en el capítulo IV, afirma que la garantía de las libertades informativas se vincula a la actividad de los medios de comunicación, debiendo integrarse en esta denominación, la prensa escrita, la radio y la televisión, sea cual sea el soporte a través del cual se difunda su actividad periodística, como los medios de comunicación exclusivamente digitales. Todos ellos desempeñan un papel innegable en orden a garantizar la plena eficacia del pluralismo, como valor superior del Ordenamiento jurídico.

246.Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de

los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE.

247.Su propósito es, según la Comisión Europea, garantizar un elevado nivel de protección de la intimidad de los usuarios de servicios de comunicaciones electrónicas y condiciones equitativas de competencia para todos los agentes del mercado.

248.Se trata del derecho de toda persona al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones, reconocido por la Carta de los derechos fundamentales de la Unión Europea.

249.Supondría un cambio radical porque muchas compañías basan su modelo en otorgar un servicio gratuito, pero a cambio de publicidad e información del usuario (*freemiums*). También afectaría, considero, incluso a la manera de enfrentarse el particular a estas aplicaciones.

250.Incluye a proveedores de *software* como *Facebook, Messenger*, *WhatsApp*, *Telegram*, *Line*, *Skype.*

251.Anglicismo que hace referencia a la información enviada por un sitio web y que se almacena en el navegador del usuario con la finalidad de recordar accesos y conocer información sobre los hábitos de navegación, lo que puede ocasionar problemas de privacidad. En relación con las *cookies*, *the Guidelines 05/2020 on consent under Regulation 679/2016*, considera que vincular la aceptación de las mismas al acceso a la navegación entorpece la consideración de la libertad del consentimiento. Es interesante consultar a este respecto la *Guía sobre el uso de las cookies* publicada por la AEPD en noviembre de 2019.

252.En relación con la propiedad intelectual, *vid.* MAESTRE RODRÍGUEZ, Javier (2017). "La responsabilidad de los prestadores de servicios de la Sociedad de la información y el concepto de público nuevo". *Revista Derecho & Sociedad*, núm. 49, págs. 77 a 86. ARROYO AMAYUELAS, Esther (2020). "La responsabilidad de los intermediarios en Internet, ¿Puertos seguros a prueba de futuro?". *Cuadernos de Derecho Transnacional*. Vol. 12, núm. 1, pág. 818, entiende que los legisladores nacional y europeo deben replantearse el rol de los intermediarios de Internet, especialmente las grandes plataformas, sin cuya colaboración los terceros no podrían llevar a cabo actos ilícitos contra la propiedad intelectual de los autores.

253.*Vid.* Exposición de motivos de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico y considerando 18 de la Directiva 2000/31/CE. El Anexo de definiciones considera *servicio* todo aquél prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario; también los servicios no remunerados por sus destinatarios si constituyen una actividad económica para el prestador de servicios; y por *servicio de intermediación* aquél que facilita la prestación o utilización de otros servicios o el acceso a la información.

254.Se aplica también este concepto al prestador de servicios que sin ser residente en España presta servicios de la sociedad de la información a través de un establecimiento *permanente* en nuestro país, aplicándosele la Ley española sólo respecto de estos servicios; de igual modo, a los prestadores de servicios establecidos en otro Estado de la UE cuando el destinatario de los servicios radique en España y estos afecten a las materias señaladas en el art. 3 LO 34/2002. La STS de 4 de marzo de 2013 (RJ 144, 2013), considera que *Google* queda sometido a la LO 34/2002 pues opera en España a través de una oficina permanente. DE MIGUEL ASENSIO, Pedro (2013). "Responsabilidad de los intermediarios en Internet y Ley aplicable en la reciente jurisprudencia del Tribunal Supremo". Disponible en: http://pedrodemiguelasensio.blogspot.com/ (27 de mayo de 2013), dice que las normas sobre el ámbito de aplicación de la Ley 34/2002 no dejan sin efecto las reglas de conflicto sobre Ley aplicable a las obligaciones extracontractuales y que cabe entender que su aplicación depende en principio de que conforme a las reglas de Derecho internacional privado que deban aplicar los tribunales españoles, sea la Ley española la aplicable a la responsabilidad de que se trate.

255.LORENTE LOPEZ, María Cristina (2014). "Los derechos al honor, a la intimidad personal y familiar y a la propia imagen en la jurisprudencia más reciente". *Los derechos a la intimidad y a la privacidad en el siglo XXI*. Dykinson. Madrid, pág. 145, destaca que es precisamente la publicación y divulgación del contenido ilícito, a través de los intermediarios, lo que le confiere potencialidad lesiva de los derechos de la personalidad.

256.*Vid.* STS de 23 de noviembre de 2018 (RJ 668, 2018). En ella el TS considera que *VLex* es un proveedor de servicios de bases de datos de carácter jurídico mediante una página web, pero esta actividad no se puede considerar como servicio de intermediación pues no es un operador o proveedor de acceso a una red de telecomunicaciones; no realiza el almacenamiento automático, provisional o temporal de la información, no presta servicios de alojamiento o almacenamiento, ni facilita enlaces a contenidos. De hecho, al texto de la sentencia en el que aparece el nombre de la víctima de un delito sexual no se accede a través de un enlace que se contenga en *VLex,* sino que el texto se encuentra directamente disponible en dicha plataforma, habiéndola obtenido de otro proveedor de contenidos en la red como es el *Cendoj*. Por no

ser un servicio de intermediación no se le aplica el art. 13.2 ni la remisión que se hace al art. 16 para considerar las causas de exoneración. Ahora bien, en cuanto proveedor de servicios sí le es aplicable el párrafo primero del art. 13 que se remite a la normativa correspondiente del Ordenamiento jurídico que para este caso sería la LO 1/82, en cuanto se alega por la demandante la vulneración de su honor e intimidad. A ello habría de añadirse, considero, aunque no lo hace la sentencia, la aplicación del Reglamento 679/2016. Finalmente, aplicando estas normas, *VLex* queda exonerado de responsabilidad pues podía esperarse legítimamente que las sentencias que le suministró el *Cendoj* estuvieran correctamente tratadas y más en concreto, anonimizadas. Además, la ingente información contenida en las sentencias que el *Cendoj* suministra a las empresas que prestan estos servicios hace que no se pueda considerar exigible que estas revisen las sentencias que le son suministradas para comprobar que están correctamente anonimizadas. Junto a ello, *VLex* actuó diligentemente pues en cuanto tuvo conocimiento del problema lo solucionó e incluso lo comunicó al motor de búsqueda de Google para que no pudiera enlazarse el texto de la sentencia mal anonimizada.

257.Esta actuación se conoce como *hosting*. El art. 14 se refiere a la responsabilidad de los operadores de redes y proveedores de acceso; el art. 15, a la responsabilidad de los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios y el art. 17, a la responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda, *linking.* Son los arts. 12 (mera transmisión) 13 (memoria tampón o *caching*) y 14 (alojamiento de datos o *hosting*) de la Directiva.

258.Es importante destacar que el art. 15 de la Directiva establece la *inexistencia de una obligación general de supervisión* para los prestadores de servicios de los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas; aunque se puede establecer el *deber de colaboración*, comunicando con prontitud a las autoridades públicas competentes los datos o actividades ilícitas llevadas a cabo por los destinatarios de su servicio y la obligación de comunicar a las autoridades, a solicitud de las mismas, información que les permita identificar a los destinatarios de sus servicios, con los que hayan celebrado acuerdos de almacenamiento.

259.*Vid.* STJUE de 12 de julio de 2011 (C-324/09). Pensemos, por ejemplo, en un caso de pornografía infantil o en una difamación grave. La STS de 26 de febrero de 2013 (RJ 1441, 2013) destaca el envío de un fax que el intermediario rehusó recibir para apreciar la existencia de conocimiento efectivo. En sentido contrario, la STS de 4 de marzo de 2013 (RJ 2245, 2013) exonera a *Google* por falta de conocimiento efectivo, pues de la información publicada no se deducía de forma notoria la ilicitud, porque el periodista no había remitido ninguna resolución judicial que la declarara y porque las afirmaciones realizadas por el ofendido no se consideraron suficientes para provocar la retirada de los enlaces.

260.ARROYO AMAYUELAS, Esther (2020). “La responsabilidad de los intermediarios en Internet, ¿Puertos seguros a prueba de futuro?”. *Cuadernos de Derecho Transnacional*. Vol. 12, núm. 1, pág. 822. MAESTRE RODRÍGUEZ, Javier (2017). “La responsabilidad de los prestadores de servicios de la Sociedad de la información y el concepto de público nuevo”. *Revista Derecho & Sociedad*, núm. 49, pág. 80, explica que la idea de un conocimiento efectivo ha ido poco a poco ampliándose respecto del inicialmente previsto por el legislador pues en el caso *GS Media* se plantea incluso el establecimiento de una presunción *iuris tantum* a favor de su existencia en algunos supuestos (STJUE de 8 de septiembre de 2016. Asunto C-160/15).

261.En este sentido, la STS de 9 de diciembre de 2009 (RJ 773, 2009).

262.(RJ 805, 2013).

263.ARROYO AMAYUELAS, Esther (2020). “La responsabilidad de los intermediarios en Internet, ¿Puertos seguros a prueba de futuro?”. *Cuadernos de Derecho Transnacional*. Vol. 12, núm. 1, pág. 823, explica que el deber de diligencia no puede identificarse con un deber de vigilancia permanente, porque eso equivaldría a establecer la responsabilidad objetiva del intermediario por el mero hecho de poner a disposición del público herramientas y espacios que faciliten las actividades y además porque ello daría lugar a poder calificar al proveedor de *activo* (no neutro).

264.ARROYO AMAYUELAS, Esther (2020). “La responsabilidad de los intermediarios en Internet, ¿Puertos seguros a prueba de futuro?”. *Cuadernos de Derecho Transnacional*. Vol. 12, núm. 1, pág. 808 y 837, considera que ha llegado el momento de adaptar las exenciones de responsabilidad (puertos seguros) a los nuevos modelos de negocio en Internet, en la onda de la Directiva 2019/790, de 17 de abril sobre los derechos de autor y afines en el mercado único digital. Entiende que la nueva directiva que se promulgue sobre esta materia, en atención a las nuevas directrices políticas para la próxima Comisión Europea 2019-2024, no debe tener por finalidad preservarlos, sino más bien, prevenir que las plataformas digitales promuevan y difundan actividades ilícitas. Para ello se prevé un incremento necesario del deber de diligencia que habrá de hacerse compatible con la libertad de información, expresión y empresa evitando que el excesivo celo en la búsqueda de ilegalidades pueda incrementar el riesgo de censura.

265.En la STJUE de 11 de septiembre de 2014 (ECLI: EU:C:2014:2209), se declara que las limitaciones de responsabilidad civil formuladas en los arts. 12 a 14 de la directiva no se aplican al supuesto de una sociedad editora de prensa que dispone de una página en Internet en la que se publica la versión digital de un periódico (…) pues tiene conocimiento de la información publicada y ejerce un control sobre la misma con independencia de que el acceso a dicha página sea gratuito o de pago; y añade que pueden aplicarse en un litigio entre particulares relativo a la responsabilidad civil por difamación, siempre que concurran los requisitos mencionados. De igual modo, la reciente STS de 27 de junio de 2019 (ROJ 2105, 2019) entiende que el responsable de una web de música no puede ser considerado como un mero intermediario al que aplicar la exención de responsabilidad, porque dicha página sugiere resultados y realiza autocorrecciones para encontrar el nombre del artista, proporciona los resultados de artistas relacionados con alguna búsqueda realizada en el pasado, incorpora datos de una base propia ajena a los datos subidos por el usuario, facilita la difusión de los contenidos y pone a disposición de sus usuarios una serie de aplicaciones para conectarse en *Facebook* y dispositivos móviles. Es decir, que su actividad no es neutral.

266.Pensemos, por ejemplo, en la apología del terrorismo, la propagación de pornografía infantil, la piratería, los fraudes y estafas, los acosos, las amenazas, las injurias y calumnias, entre otros.

267.COTINO HUESO, Lorenzo (2015). “El conflicto entre las libertades de expresión e información en Internet y el derecho a la protección de datos. El derecho al olvido y sus retos: un falso derecho a juzgar por un falso tribunal”. *Derecho de la información: El ejercicio del derecho a la información y su jurisprudencia.* Centro de estudios políticos y constitucionales. Madrid, págs. 417 y 418, afirma que sin los prestadores de servicios que permiten el acceso a la información y la generación de contenidos y la interactuación de los usuarios no hay sociedad libre ni, por tanto soberanía popular y además, insiste en que se ha de valorar el efecto que puede producirse de modo global por imponer límites o condiciones severas a los intermediarios pues por ejemplo para *Google* puede ser una molestia a la cual puede hacer frente en sus niveles de costes; sin embargo, la imposición de estas cargas puede frenar las posibilidades para otros buscadores, lo cual es negativo pues puede generarse más fácilmente una censura ya que la reacción más sencilla ante la falta de medios será retirar todo contenido que se solicite por un particular.

268.Dice YANGUAS GÓMEZ, Roberto (2012). *Contratos de conexión a Internet, Hosting y búsqueda*. Civitas, Madrid, pág. 369, que el hecho de perder la inmunidad puede ser considerado un indicio a partir del cual deducir que el prestador tenía conocimiento o contribuyó de alguna manera al ilícito, que es a la vez, un indicio de que no existió la diligencia debida y por tanto, ello permitiría imputarle la responsabilidad.