*La seguridad como elemento clave en el tratamiento de datos personales en Europa: especial referencia al régimen de responsabilidad civil derivado de las brechas de seguridad**

Security as a Key Element in the Processing of Personal Data in Europe: Especial Reference to the Civil Liability Regime derived from Security Breaches

Alejandro Platero Alcón** https://orcid.org/0000-0002-3318-6441

http://dx.doi.org/10.21503/lex.v17i23.1670

* Este trabajo se ha desarrollado en el marco del Programa Nacional de Formación del Profesorado Universitario del Ministerio de Educación, Cultura y Deporte del Gobierno de España.

** Investigador y docente (FPU) del área de Derecho Civil de la Universidad de Extremadura (ESPAÑA). Miembro del grupo de investigación de Estudios en España, Portugal y América Latina, grupo oficial de investigación de la Universidad de Extremadura.
Correo electrónico institucional: platero@unex.es

La pesca milagrosa. Óleo.
Agustín Aquino Mejías (pintor peruano).

RESUMEN

Las nuevas tecnologías han permitido enormes ventajas para los ciudadanos del siglo XXI, pero a su vez han puesto de manifiesto graves intrusiones en la privacidad de los mismos. En concreto, se expondrán las posibles consecuencias jurídicas civiles derivadas de las conocidas como brechas de seguridad, figura regulada recientemente en el Reglamento de Protección de DatosEuropeo, instrumento que impone al responsable del tratamiento de datos personales una serie de obligaciones cuando acontece la misma.

Palabras clave: *datos personales, brechas de seguridad, responsable del tratamiento, responsabilidad civil.*

ABSTRACT

The new technologies provided enormous advantages for the 21st century citizens, but at the same time revealed serious intrusions in their privacy. Specifically, the possible civil legal consequences derived from the security breaches will be exposed, a figure recently regulated in the European Data Protection Bylaw imposing a series of obligations on the person responsible for the processing of personal data when a security breach occurs.

Key words: *personal data, security breaches, responsible for treatment, civil liability.*

I. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

La protección de datos personales, al contrario de lo que podría imaginarse, no es una preocupación reciente en Europa, sino que el reconocimiento de la conocida figura como un derecho fundamental ha sido una consecuencia del acaecimiento de una serie de hechos con enorme transcendencia. Se narrarán, a continuación, algunos de esos hechos, para comprender la importancia del citado derecho fundamental.

Los verdaderos orígenes del derecho a la protección de datos personales, con independencia de lo establecido con anterioridad en la Declaración Universal de Derechos Humanos[1] o en el Pacto Internacional de Derechos Civiles y Políticos,[2] se deben situar a partir de la década de los sesenta del siglo pasado, destacando, en primer lugar, el año 1967, cuando se estableció una Comisión Consultiva dentro del Consejo de Europa, de la cual emanó la Resolución 509 sobre los Derechos Humanos y los nuevos logros científicos y técnicos.

El Tribunal de Justicia de las Comunidades Europeas resolvió ya en el año 1969 un caso sobre protección de datos personales, aunque realmente, no nombra todavía este derecho en su resolución, ya que no se encontraba previsto todavía en ningún texto legal. Se trata del conocido caso *Stauder*, basado en la reclamación de un ciudadano alemán que para obtener mantequilla a precio reducido debía entregar un cupón en los supermercados con su nombre, número de documento de identidad y condiciones económicas. El Tribunal consideró que era contrario a los principios generales del derecho comunitario dichas revelaciones personales.[3]

[1] Art. 12 de la Declaración Universal de Derechos Humanos de 10 de diciembre de 1948: Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

[2] Art. 17 del Pacto Internacional de Derechos Civiles y Políticos de 16 de diciembre de 1966: 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

[3] STJCE de 12 de noviembre de 1969, caso *Stauder*.

Posteriormente en la década de los setenta comenzó el desarrollo legislativo del derecho a la privacidad del individuo. Así, destacan especialmente cuatro países. El primer país en legislarlo fue Suecia en el año 1973 con la denominada *Data Leg*, seguida de Estados Unidos con la conocida como *Privacy Act* de 1974; en tercer lugar está Alemania con la aprobación de su ley federal para la protección de datos en el año 1977, y, Francia en el año 1978 con la Ley *Relative á l´informatique, auxfichiers et auxlibertés*. Resulta paradigmático el caso de Portugal que fue pionero en la incorporación de este derecho al texto constitucional en el año 1976, pero no tenía ley sobre la materia.[4]

Posteriormente, en el año 1981, se promulga el Convenio número 108 para la protección de la personas con respecto al tratamiento automatizado de los datos de carácter personal emanado por parte del Consejo de Europa,[5] donde se encuentran ya enumerados una serie de principios básicos en la protección de datos personales, que, como después se expondrá, todavía se encuentran en la legislación europea y española, como son el de calidad de datos personales, o el de garantía y seguridad de los datos personales.

En el año 1983 el Tribunal Constitucional Federal alemán dictó una conocida sentencia sobre la Ley del Censo Alemana, que perfiló el alcance y contenido del derecho a la autodeterminación informativa,[6] origen del conocido actualmente como derecho a la protección de datos personales. En palabras del Tribunal:

> (…) la libertad de decisión, de control, supone además que el individuo tenga la posibilidad de acceder a sus datos personales, que pueda, no solo tener conocimiento de que otros procesan informaciones relativas a su persona, sino también someter el uso de estas a un control, ya que, de lo contrario, se limitará su libertad de decidir por autodeterminación.[7]

Posteriormente, en la década de los noventa, surgirá la normativa europea de protección de datos que ha estado vigente más de 20 años, la cual ha dado sustento tanto a la normativa española, como al resto de países europeos. Se trata de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección

[4] A. Cerda Silva, "El nivel adecuado de protección para las transferencias internacionales de datos personales desde la Unión Europea", *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, 36(2011): 328.

[5] Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981,*BOE* núm. 274, de 15 de noviembre de 1985.

[6] Un concepto de autodeterminación informativa puede encontrarse en la obra de L. Murillo de la Cueva, *El derecho a la autodeterminación informativa*(Madrid: Tecnos, 1990), 173: "pretende satisfacer la necesidad, sentida por las personas en las condiciones actuales de la vida social, de preservar su identidad controlando la revelación y el uso de los datos que les conciernen y protegiéndose frente a la ilimitada capacidad de archivarlos, relacionarlos y transmitirlos propia de la informática, y de los peligros que esto supone".

[7] M. Heredero Higueras, "La sentencia del Tribunal Constitucional de la República Federal Alemana relativa al censo de población", *Documentación Administrativa,*198 (1983).

de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos.[8]

Otro importante avance se encontraría con la promulgación de la Carta de los Derechos Fundamentales de la Unión Europea de 18 de diciembre del año 2000, que establecía en su Art.8 el siguiente dogma, "toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan". Estos postulados incluso fueron recogidos en la fallida Constitución para Europa,[9] donde se hacía mención en dos ocasiones al derecho fundamental a la protección de datos personales.[10]

Ahora bien, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, por el que se deroga la Directiva 95/46/CE, (en acrónimo RGPD),[11] reformó todo el sistema de privacidad existente en Europa, sirviendo su articulado de base para el análisis de la exigencia de seguridad en el tratamiento de datos personales que se realizará en el presente trabajo.

II. LA RECOPILACIÓN DE DATOS DE LAS NUEVAS TECNOLOGÍAS

La importancia del derecho fundamental a la protección de datos en actual escenario de desarrollo tecnológico del siglo XXI es innegable, así:

> (…) la universalización de la informática, unida a la masiva, imparable y vertiginosa propagación del uso de Internet, con sus inagotables recursos, pero también con los más variados instrumentos que permiten, casi al alcance de cualquiera, la invasión de la privacidad de los ciudadanos, ha derivado en una preocupación general por este fenómeno y puesto de manifiesto la necesidad de su regulación jurídica.[12]

Resulta evidente que las nuevas tecnologías han cambiado la forma de vida de los seres humanos. La mayor parte de la comunicación con el resto de personas ya no se realiza ver-

[8] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, "DOCE" núm. 281, de 23 de noviembre de 1995.

[9] Dos menciones al derecho fundamental a la protección de datos se encuentran en la fallida Constitución: La primera mención se encuentra en el Art. I.51: "Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernen". La segunda se encuentra en el Art. II.68 donde se establece el mismo texto que el expresado con anterioridad y se añaden cuestiones básicas como el deber de tratar los datos de forma leal.

[10] R. Martínez Martínez, "El derecho fundamental a la protección de datos: Perspectivas", *Revista de Internet, Derecho y Política*, 5(2007):50.

[11] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, "DOUE" núm. 119, de 4 de mayo de 2016.

[12] A. Acedo Penco, "El derecho al olvido en internet como componente esencial del derecho al honor en el siglo XX", en-*DirieitosFundamentais Da Pessoa Humana*, ed. por J. A., Sabaris (Curitiba: Alteridade, 2012), 191-221.

balmente, sino que se lleva a cabo fundamentalmente a través de servicios de mensajería instantánea como *WhatsApp*, el contacto con los amigos lejanos se realiza mediante el visionado de fotos o videos que suben en redes sociales como *Facebook*, muchos de los ciudadanos han sustituido los taxis por *Uber*, y ya no se contrata el hotel para las vacaciones a través de una agencia de viajes, e incluso, en muchos casos, no se acude ni a *Booking* para encontrar alojamiento, sino que se accede a *Airbnb* para buscar un piso donde alojarse.

Todos los productos nombrados con anterioridad tienen una característica común, ya que se encuentran disponibles en formas de aplicaciones que se instalan en el *smartphone*, siendo capaces de "captar información del usuario o de su equipo terminal, en algunas ocasiones de forma más que discutible, al no ser consciente de ello el usuario".[13]

La doctrina así, muestra de manera casi unánime su preocupación por la privacidad del individuo ante las nuevas tecnologías citadas con anterioridad,[14] así:

> (…) en etapas anteriores, el respeto a la vida privada podía realizarse mediante el uso de los sentidos, permanecía dentro de los límites de las relaciones naturales. Los muros de una casa, la soledad de un lugar desierto eran suficientes para asegurar la protección de la intimidad (…) hoy es posible observar y escuchar a distancia, sin límites de tiempo, de espacio o de modo; estas circunstancias, en especial la utilización masiva de la informática, han determinado que para la opinión pública y el debate político de nuestro tiempo constituya un problema nodal el establecimiento de unas garantías que tutelen a los ciudadanos de la agresión a su intimidad.[15]

Resulta evidente, que el Derecho debe articular mayores medidas de protección ya no solo frente al uso de los datos personales que se ceden por parte de los usuarios a determinados sitios web o *apps*, sino también, reforzando las medidas de protección que deben articular los responsables del tratamiento de los datos, frente a los ataques de terceros, que quieren acceder de manera ilícita a los citados datos personales, es decir, mediante ataques cibernéticos. De hecho, el ciberespacio donde se almacenan normalmente los datos personales "es un espacio vulnerable, ya que todas las tecnologías, ya estén formadas por software, hardware o una combinación de ambas, pueden contener errores en su diseño o incluirlos en el proceso de su desarrollo. Estas vulnerabilidades, una vez que han sido descubiertas, pueden ser explotadas

[13] A. Paniza Fullana, "Una nueva era en la privacidad y las comunicaciones electrónicas: La 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", *Revista Aranzadi Civil-Mercantil*, 4(2017): 106.

[14] Se ha utilizado la expresión casi unánime, porque existen lógicamente excepciones. Así, por ejemplo puede observarse la obra de, J.L.Dader, "La privacidad como excusa para restringir la información de interés público", *Revista General de Derecho Constitucional*, 15 (2012): 2: El citado autor considera que la privacidad se encuentra "hiperprotegida", limitando de ese modo la libertad de expresión y de información.

[15] A. E. Pérez Luño, *Derechos humanos, Estado de Derecho y Constitución*, (Madrid: Tecnos, 2010), 365.

para la realización de acciones no autorizadas, como pueden ser entre otros el robo de información o la disrupción del sistema".[16]

Es por eso que el presente trabajo se centra en la exposición de las exigencias comunitarias de la seguridad en la protección de datos personales por parte del responsable del establecimiento, y presta mayor importancia a las consecuencias jurídicas de las conocidas como brechas de seguridad. Su importancia en la sociedad actual es capital, así a modo de ejemplo, recientemente la han sufrido compañías de transporte aéreo como *Airbus*, donde se ha accedido a datos personales de trabajadores de la compañía.[17] La industria de los videojuegos también se ha mostrado vulnerable a estas brechas, así el conocido juego *Fortnite* también ha sufrido una brecha de seguridad, dejando al descubierto datos económicos de sus usuarios,[18]incluso universidades públicas como la de Valladolid, que comunicó haber sufrido una brecha de seguridad, donde se ha accedido a datos personales de los alumnos matriculados.[19]

III. LA REGULACIÓN CLÁSICA DE LA SEGURIDAD EN EL TRATAMIENTO DE DATOS

La regulación jurídica principal de las brechas de seguridad de datos personales, se encuentra en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, por el que se deroga la Directiva 95/46/CE.[20] Sin embargo, cabe decir que con anterioridad a la entrada en vigor del RGPD, tanto a nivel comunitario como en el ámbito interno español, ya había normas que regulaban esta cuestión, aunque como se observará, las mismas no albergaban el mismo nivel de desarrollo que el existente en la actualidad.

En efecto, ya en la década de los noventa surgió la normativa europea de protección de datos que ha estado vigente durante más de 20 años,[21] la cual ha dado sustento tanto a la normativa española que después se expondrá, como al resto de países europeos. Se trata de la

[16] A. Hernández Moreno, "Ciberseguridad y confianza en el ámbito digital", *Información Comercial Española, ICE: Revista de economía*, 897 (2017): 57.

[17] Comunicado de 30 de enero de 2019, reconociendo los hechos: https://www.airbus.com/newsroom/press-releases/en/2019/01/airbus-statement-on-cyber-incident.html, (consultado el 1 de febrero de 2019).

[18] Descubierta por una empresa experta en ciberseguridad. Véase: https://blog.checkpoint.com/2019/01/16/fortnite-vulnerability-where-only-the-secure-survive/, consultado el 1 de febrero de 2019.

[19] Véase, https://www.elnortedecastilla.es/valladolid/hacker-roba-datos-20190114100856-nt.html, (consultado el 1 de febrero de 2019).

[20] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, "DOUE" núm. 119, de 4 de mayo de 2016.

[21] Para profundizar en la misma, obsérvese M. Heredero,*La Directiva comunitaria de protección de datos de carácter personal*(Pamplona: Aranzadi, 1997).

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, (en acrónimo Directiva 95/46), cuya importancia residía en los fundamentos de la propia, "construcción europea, que requiere ineludiblemente la constitución del mercado interior, exige que se garantice la libre circulación de los datos personales, dado el valor económico que los mismos tienen en las transacciones comerciales, sobre todo en el marco de una económica cada vez más globalizada y transfronteriza".[22]

La seguridad en la Directiva comunitaria venía configurada como una *condición general para la licitud del tratamiento de datos personales*, estableciendo el Art. 17 lo siguiente:

> Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya latransmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

El citado precepto relaciona la seguridad de los datos con los conocimientos técnicos existentes en cada momento, pero no determina cuáles son los métodos que deben seguirse para proteger los datos en cuestión, sino que dejaba dicha materialización en manos de los Estados miembros. Así, se pronunció el Tribunal de Justicia de la Unión Europea, (en acrónimo TJUE), en su sentencia 30 de mayo de 2013, en el conocido como caso *Worten*, considerando que el Art. 17.1 de la Directiva debe interpretarse en el sentido de que: "Los Estados miembros están obligados a prever medidas técnicas y de organización adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados".[23]

La trasposición española de la Directiva comunitaria llegaría en el año 1999, regulando como norma la necesidad de la seguridad en el tratamiento de datos personales. En efecto, en el citado año se produce un hecho importante en la configuración del derecho fundamental a la protección de datos en España, como fue la promulgación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos[24] (en acrónimo LOPD). La citada disposición ha

[22] J. L. Piñar Mañas, "El derecho a la protección de datos de carácter personal en la jurisprudenciadel Tribunal de Justicia de las Comunidades Europeas", *Cuadernos de Derecho Público*,20 (2003):48.

[23] STJUE (Sala Tercera) de 30 de mayo de 2013, asunto C-342/12, (caso Worten), apartado 19.

[24] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, "BOE" núm. 298, de 14/12/1999.

constituido la norma básica de interpretación del citado derecho[25] hasta el año 2016,cuando la Unión Europea modificó por completo la Directiva del año 1995.

La LOPD configuró la seguridad de los datos, ya como un principio, a diferencia de lo que hacía la directiva comunitaria, aumentando además las salvaguardias y exigencias comunitarias. Así, su artículo noveno, establecía lo siguiente:

> 1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas deíndole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
> 2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
> 3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

El precepto citado con anterioridad,[26] refuerza las exigencias de seguridad en el tratamiento de datos personales, mediante la mención a una serie de estándares que deben reunir todos los ficheros de datos personales, y en especial, imponiendo un mayor nivelde seguridad en el tratamiento de datos personales especialmente protegidos, aunque todo ello se determinaría reglamentariamente. Así, dichas concreciones se encontrarían en el Reglamento de desarrollo aprobado por el Real Decreto 1720/2007, de 21 de diciembre[27] (en acrónimo RLOPD).

En el RLOPD se establecían tres niveles de seguridad: el básico, el medio y el alto.[28] *El nivel de seguridad básico* debía ser instaurado por cualquier fichero que tratara datos de carácter personal, mientras que el *nivel de seguridad medio*se establecía en los siguientes supuestos: a) los relativos a la comisión de infracciones administrativas o penales, b) los relativos a solvencia patrimonial y de crédito, c) aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias, d) aquellos de los que

[25] Para profundizar sobre la misma, obsérvese la obra de J. Aparicio Salom, *Estudio sobre la Ley Orgánica de protección de datos de carácter personal* (Pamplona: Aranzadi, 2000).

[26] Para profundizar, obsérvese Y. Navalpotro Navalpotro, "El deber de secreto", en *Estudio práctico sobre la protección de datos de carácter personal*, ed. por. C. Almuzara Almaida (Madrid: Lex Nova, 2005), 515 - 533.

[27] Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, "BOE" núm. 17, de 19/01/2008.

[28] F. Falcón y Tella, "El principio de seguridad y el derecho fundamental a la protección de datos personales", *Anuario de Derechos Humanos*, 10 (2009).

sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros, e) aquellos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y f) aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.*El nivel de seguridad alto* se aplicaba en relación a los siguientes datos: a) de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual; b) que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas; c) datos derivados de actos de violencia de género.

IV. LAS BRECHAS DE SEGURIDAD EN EL RGPD

El régimen descrito sobre la seguridad en el tratamiento de datos personales, cambia radicalmente con la promulgación del Reglamento General de Protección de Datos europeo en el año 2016, instrumento en forma de reglamento que presenta aspectos muy positivos, "como es el hecho de implantar, por vez primera, una regulación jurídica homogénea y uniforme en materia de protección de datos para todos los Estados miembros de la Unión Europea, lo que beneficia tanto a los consumidores como a las propias empresas, que disponen de una norma única que implantar en todos los países miembros, con la consiguiente seguridad jurídica y transparencia".[29]

El Reglamento reforma todo el sistema de protección de datos existente hasta el momento, centrándose para ello, en un aumento de la seguridad en el tratamiento de datos personales. Una muestra de lo anterior, es la inclusión del principio de responsabilidad activa, o *accountability*, el cual obliga al responsable del tratamiento de datos de estar en condiciones de demostrar, en cualquier momento, de que cumple con la norma de protección de datos, como se infiere del Art. 24.1RGPD,[30] cuestión que, demuestra que con el nuevo régimen, "no incumplir ya no será insuficiente".[31]

El RGPD regula la seguridad desde dos puntos de vista. En primer lugar, como principio del tratamiento, como se desprende del Art. 5.1.f) al establecer que los datos deben ser "tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o

[29] V. Puldain Salvador, "El futuro marco legal para la protección del acceso a los datos", *Revista Ibero-Latinoamericana de Seguros*26,47 (2017):128

[30] Art. 24.1 RGPD: "Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario".

[31] F. J. Biurrum Abad, "*Accountability* o responsabilidad activa en el Reglamento General de Protección de Datos", *Actualidad Jurídica Aranzadi*, 927 (2017):1.

daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas". En segundo lugar, la seguridad aparece regulada como una obligación del responsable o encargado del tratamiento, en los Arts. 32 a 34, donde se recoge la regulación actual de las conocidas como brechas de seguridad.[32]

El Art. 32 RGPD establece que el responsable y el encargado del tratamiento deben aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta para su adopción el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, incluyendo dentro de esas medidas, la técnica de seudonimización y el cifrado de datos personales.

Dichas medidas también deben garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico, e incluir entre las mismas un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

En último lugar, este Art. 32, establece que la adhesión a un código de conducta[33]o a un mecanismo de certificación podrá servir de elemento probatorio por parte del responsable del tratamiento de datos personales, de intención de cumplimiento con las exigencias necesarias para la protección de los datos personales de sus usuarios.

Resulta interesante destacar que el RGPD, a diferencia de lo que ocurría en la Directiva del año 1996, no deja en manos de los Estados miembros la concreción de las medidas de seguridad a adoptar para proteger el acceso de terceros a los datos de sus usuarios, sino que esta cuestión corresponde a los responsables o encargados del tratamiento, que la deberán realizar de acuerdo con el desarrollo o avances de la técnica, ya que el RGPD solo cita dos medidas de protección específicas: la seudonimización y el cifrado de datos personales.[34]

Pero la gran novedad que introduce el RGPD, respecto a las brechas de seguridad, es su obligación de notificación en dos vertientes: en primer lugar, a las agencias independientes

[32] El RGPD no define exactamente el término brechas de seguridad, pero sí el término genérico de "violación de la seguridad de los datos personales", considerando en su Art. 4 que el mismo hace referencia a:"toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".

[33] Sobre los mismos, obsérvese A. O. Ortega Giménezy J. J. Gonzalo Domenech, "Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea", *Revista de la Facultad de Derecho*44, (2018).

[34] A. Troncoso Reigada, "La seguridad en el Reglamento General de Protección de Datos de la Unión Europea", *Diario la Ley*, 15647 (2018): 8 y ss.

de protección de datos personales implicadas y, en segundo lugar, al interesado cuyos datos personales han sido expuestos, obligación que ya en el considerando 87 de la norma se puede apreciar con claridad.[35]

En efecto, el Art.33 impone al responsable del tratamiento de datos la obligación de notificar a las agencias independientes de control, en un plazo de 72 horas desde que se produzca[36] la brecha de seguridad, y si la comunicación se produce en un momento posterior, indicar los motivos de la dilación. Como excepción a la obligación de notificación anterior, se permite no notificar cuando resultara improbable que como consecuencia de dicha brecha se hubiera producido un riesgo para los derechos y libertades de las persona físicas, o en lengua inglesa, que refleja todavía más la importancia de la citada obligación, *"unlikely to result in a risk to the rights and freedoms of natural persons"*.[37]

La notificación deberá contener los siguientes extremos: a) la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados; b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información; c) describir las posibles consecuencias de la violación de la seguridad de los datos personales; d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

La Agencia Española de Protección de Datos ha elaborado una guía sobre el proceso a seguir en la comunicación de las brechas de seguridad, donde, aparte de suministrar un formulario al alcance del responsable del tratamiento de datos que se encuentre en la obligación de notificar la misma, distingue tres tipos de brechas:

a) *Brecha de confidencialidad*: tiene lugar cuando partes que no están autorizadas, o no tienen un propósito legítimo para acceder a la información, acceden a ella. La severidad de la pérdida de confidencialidad varía según el alcance de la divulgación, es decir, el

[35] Considerando 87 RGPD: "Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento".

[36] Plazo del que se queja parte de la doctrina. Obsérvese, M.L.González Tapia, "Violaciones de seguridad en el Reglamento de Protección de datos", *Diario La Ley,* 14344 (2017): 1 y ss.

[37] A. Daly, "The introduction of data breach notification legislation in Australia: A comparative view", *Computer Law and Security Review*, 34 (2018):484.

número potencial y el tipo de partes que pueden haber accedido ilegalmente a la información.

b) *Brecha de integridad*: se produce cuando se altera la información original y la sustitución de datos puede ser perjudicial para el individuo. La situación más grave ocurre cuando existen serias posibilidades de que los datos alterados se hayan utilizado de una manera que pueda dañar al individuo.

c) *Brecha de disponibilidad*: su consecuencia es que no se puede acceder a los datos originales cuando es necesario. Puede ser temporal (los datos son recuperables, pero tomará un periodo de tiempo y esto puede ser perjudicial para el individuo), o permanente (los datos no pueden recuperarse).[38]

Además, el Art.34 RGPD impone también la obligación de que dicha comunicación se realice al interesado mediante el uso de un lenguaje claro y sencillo, donde como mínimo se deberá indicar lo siguiente: a) la naturaleza de la violación de la seguridad, b) notificar el nombre y datos de contacto del delegado de protección de datos o la persona encargada, c) realizar una descripción de las consecuencias de la violación de seguridad en los datos personales del usuarios, d) describir las medidas realizadas para reprimir dicha situación. No hará falta realizar dicha comunicación al interesado, cuando el responsable del tratamiento hubiera adoptado medidas técnicas que permitan proteger los datos personales ante dichas brechas de seguridad,[39] o fuera desproporcionado comunicarse uno a uno con todos los usuarios, por lo que entonces bastará realizar una comunicación de carácter pública.

V. LA RESPONSABILIDAD CIVIL DE LAS BRECHAS DE SEGURIDAD

Una vez expuesto el régimen jurídico principal de las conocidas como brechas de seguridad, toca hacer referencia a las consecuencias jurídicas que deben soportar los responsables del tratamiento que las sufren, desde una óptica civilista. Si como consecuencia de la brecha de seguridad, se acceden a datos personales que pueden identificar a los usuarios, ya que no se encontraban sujetos a un programa de cifrado adecuado al nivel de desarrollo de la tecnología, se puede generar un daño al usuario, daño que debe ser resarcible económicamente, es decir, se genera una responsabilidad civil por parte del responsable del tratamiento de los datos personales.

Es el Art. 82 RGPD el que establece: "Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una

[38] Véase: https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf (consultado el 2 de febrero de 2019).

[39] El cifrado de los datos personales puede ser motivo de ausencia de obligatoriedad de notificar la brecha de seguridad a los usuarios. Al respecto, véase, P. Fernández Burgueño, "La obligación de cifrado de la información en el Reglamento Europeo de Protección de Datos", *Diario La Ley*, 1091 (2017): 29 y ss.

indemnización por los daños y perjuicios sufridos". En virtud del mismo, si la filtración consistiera en la revelación de datos económicos que permitieran a terceros realizar, por ejemplo, compras por internet, esos daños materiales deberán ser indemnizados. Sin embargo, la filtración puede suponer la creación de un daño moral,[40] piénsese por ejemplo, en los casos en que se divulgan mensajes íntimos de personas casadas, mantenidos con hombres o mujeres que no son precisamente sus esposos. Pues bien, esos daños, también deben ser indemnizados, ya que el Art. 82 RGPD, alude claramente tanto a los daños materiales como inmateriales.

Además, se debe destacar que la tutela judicial civil de los perjudicados por violaciones en su derecho fundamental a la protección de datos, también se ha visto mejorada conforme al Art. 79.2 RGPD que permite demandar a los perjudicados en el fuero de su propio domicilio habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.[41]

Con anterioridad a la promulgación de este artículo, para considerar que un ciudadano podía demandar al responsable del tratamiento, incluso situado fuera de la Unión Europea, en el foro de su propio domicilio, había que acudir al reglamento 1215/2012 del parlamento europeo y del consejo de 12 de diciembre de 2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil. Este establece en sus Arts.17 a 19 un sistema de competencia especial en el caso de contratos celebrados con consumidores.[42]Concretamente, el Art.18 establece que el consumidor podrá interponer su acción judicial ante los órganos jurisdiccionales del Estado miembro en que esté domiciliada dicha parte o, con independencia del domicilio de la otra parte, ante el órgano jurisdiccional del lugar en que esté domiciliado el consumidor.

Además, tanto el actual régimen competencial como el resultante de la aplicación del foro del consumidor en reglamento de Derecho Internacional mencionado con anterioridad resultaban de aplicación preferente, dejando sin aplicación la sumisión a determinados tribunales que se encuentran articulados en determinados contratos de términos y servicios con algunos responsables del tratamiento, que indican que se les debe demandar ante sus propios tribunales, ya que"estas cláusulas no podrán ser invocadas válidamente por el prestador de servicios

[40] Cuestiones como la inclusión indebida en registros de morosos pueden generar un daño moral, como establece C. Lasarte Álvarez, *Principios de Derecho Civil.* Tomo II: Derecho de Obligaciones(Madrid: Marcial Pons, 2018), 240 y ss.

[41] A. Durán Arroyo, "El nuevo Reglamento de Protección de Datos Personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito", *Revista Jurídica de la Universidad Autónoma de Madrid*, 37 (2018): 429 y ss.

[42] Véase, la sentencia del TJUE (Gran Sala) de 7 de diciembre de 2010, en el asunto *Pammer*, donde se estableció los requisitos que una empresa que presta servicios en Internet, debe reunir para considerar el contrato con sus usuarios como de consumo.

online para desplazar la competencia reconocida por el sistema Bruselas a los tribunales de un Estado miembro a favor de un tercer Estado".[43]

En el supuesto objeto de análisis, es decir, que como consecuencia de una brecha de seguridad se genere un daño que debe ser indemnizado a un particular, resulta interesante catalogar esta responsabilidad civil, bien como contractual, o extracontractual, ya que, entre otras cuestiones, el plazo de prescripción para exigir la reparación económica varía en cada institución. En efecto, al no indicar el Reglamento europeo plazo de prescripción de la acción para reclamar daños y perjuicios, se debe acudir al ordenamiento interno de cada país para determinar el mismo.

Piénsese por ejemplo, que la fuga de datos personales, tiene su origen en una relación entre un usuario de una red social con domicilio en España, que, para participar en la red social, tiene que aceptar una serie de condiciones preestablecidas, lo que se conoce como un contrato de términos y servicios. En ese supuesto, si los datos personales filtrados le producen ese daño, el presente autor defiende que ese derecho a indemnización debe ser considerado como contractual, ya que existe una relación contractual previamente establecida entre ambos, y el deber de seguridad de los datos del usuario forma parte intrínseca de esa relación.

Sobre esta responsabilidad contractual en España, el Art.1101 del Código Civil[44] (en adelante CC) establece lo siguiente:

> (…) quedan sujetos a la indemnización de los daños y perjuicios causados los que en el cumplimiento de sus obligaciones incurrieren en dolo, negligencia o morosidad, y los que de cualquier modo contravinieren al tenor de aquellas.

Parece evidente que la violación de la obligación de seguridad en el tratamiento, mediante la creación de una brecha de seguridad que produce un daño al usuario de esa red social, por seguir con el ejemplo utilizado, puede encajarse dentro de la categoría de negligencia, ya que podría demostrarse que el responsable del tratamiento no adoptó las medidas técnicas necesarias, como el cifrado de datos personales, para garantizar la seguridad de los mismos.

Además, sobre el ámbito de aplicación del Art. 1101 CC se ha escrito que lo que en realidad describe es la responsabilidad obligacional y no únicamente la contractual, así, "el artículo 1.101 determina las consecuencias indemnizatorias que surgen del incumplimiento de cualquier obligación, no importa cuál sea su fuente. No es, por tanto, la norma que disciplina la responsabilidad contractual, sino la genérica responsabilidad obligacional, cuando la obligación que se infringe estaba previamente constituida, por contrato, ley o cuasi contrato.

[43] C. Cordero Álvarez, *Litigios Internacionales sobre difamación y derechos de la personalidad* (Madrid: Dykinson, 2015), 127.
[44] Art.1101 del Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil, "BOE" núm. 206, de 25/07/1889.

Es de aplicación, en consecuencia, a los contratos, pero también a las obligaciones que surgen directamente de la ley".[45]

Debe destacarse también el plazo de prescripción existente en el caso de que la brecha de seguridad tuviera su origen en una responsabilidad de carácter contractual. Así, en España, hasta fechas no muy recientes, su plazo era muy generoso, en concreto de 15 años. Pero con la reforma del Código Civil producida en el año 2015,[46] el citado plazo es actualmente de cinco años como establece el Art. 1964.2 del CC, comenzando a contar dicho plazo, desde que el interesado tenga conocimiento de la brecha de seguridad producida.

VI. CONCLUSIONES

El Reglamento General de Protección de Datos personales ha introducido una mayor preocupación por la seguridad en el tratamiento de los datos por parte del encargado o responsable del tratamiento. Así, dicha preocupación se observa al configurar a la seguridad tanto como principio relativo al tratamiento de datos personales, y como obligación dirigida al responsable del tratamiento. La obligatoriedad en la comunicación de las brechas de seguridad, tanto a las agencias de control como al interesado, es otra de esas manifestaciones de un mayor nivel de preocupación en la seguridad por parte de la Unión Europea.

El RGPD recomienda el cifrado de datos personales y, además, lo configura como una posible excepción de notificación de la brecha de seguridad hacia el interesado, aunque lógicamente, este último tiene un derecho reconocido a obtener una reparación económica por los daños, tanto materiales como inmateriales, que se le hubieran podido ocasionar como consecuencia de la citada filtración.

En la actualidad, teniendo en cuenta la normativa española, el interesado podrá reclamar esta responsabilidad en el plazo de 5 años, siempre que el daño sea considerado como contractual, hecho que se antoja bastante probable, como consecuencia de la relación que tiene que unirle al responsable del tratamiento, pudiendo además, como se ha expresado, demandar en el fuero de su propio domicilio, hecho que va a facilitar las demandas de responsabilidad civil frente a violaciones del derecho fundamental a la protección de datos personales.

Quizás el plazo de 72 horas concedido para notificar dicha brecha de seguridad sea demasiado corto, aunque el RGPD parte de la necesidad de que los responsables del tratamiento deben estar en condiciones de cumplir con el mismo en cualquier momento, en virtud del principio de responsabilidad activa, principio que influye notablemente en la regulación y articulado de las conocidas como brechas o incidentes de seguridad.

[45] A. Carrasco Perera, "Comentario al artículo 1101 CC", en *Comentarios al Código Civil y Compilaciones Forales,* ed. por M., Albaladejo García (Madrid: Edersa, 2004), 1.

[46] Ley 42/2015, de 5 de octubre, de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, "BOE" núm. 239, de 6 de octubre de 2015.

REFERENCIAS

- Acedo Penco, A. "El derecho al olvido en internet como componente esencial del derecho al honor en el siglo XX". En *Dirieitos Fundamentais Da Pessoa Humana*, ed. por J. A. Sabaris, 191-221. Curitiba: Alteridade, 2012.
- Aparicio Salom, J. *Estudio sobre la Ley Orgánica de protección de datos de carácter personal.* Pamplona: Aranzadi, 2000.
- Biurrum Abad, F.J. "Accountability o responsabilidad activa en el Reglamento General de Protección de Datos". *Actualidad Jurídica Aranzadi*, 927 (2017):1-7.
- Carrasco Perera, A. "Comentario al artículo 1101 CC".En *Comentarios al Código Civil y Compilaciones Forales,* ed. por M. Albaladejo García. Madrid: Edersa, 2004.
- Cerda Silva, A. "El nivel adecuado de protección para las transferencias internacionales de datos personales desde la Unión Europea". *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso.* 36 (2011): 327-356. https://doi.org/10.4067/S0718-68512011000100009
- Cordero Álvarez, C. *Litigios Internacionales sobre difamación y derechos de la personalidad.* Madrid: Dykinson, 2015. PMid:25299499
- Dader, J. L. "La privacidad como excusa para restringir la información de interés público". *Revista General de Derecho Constitucional,* 15 (2012): 1-42.
- Daly, A. "Theintroduction of data breach notification legislation in Australia: A comparativeview". *Computer Law and Security Review*, 34 (2018):484-504. https://doi.org/10.1016/j.clsr.2018.01.005
- Durán Arroyo, A. "El nuevo Reglamento de Protección de Datos Personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito". *Revista Jurídica de la Universidad Autónoma de Madrid*, 37 (2018): 415-440.
- F. Falcón y Tella."El principio de seguridad y el derecho fundamental a la protección de datos personales". *Anuario de Derechos Humanos*, 10 (2009): 131-169.
- Fernández Burgueño, P. "La obligación de cifrado de la información en el Reglamento Europeo de Protección de Datos". *Diario La Ley*, 1091 (2017): 1-32.
- González Tapia, M.L. "Violaciones de seguridad en el Reglamento de Protección de datos". *Diario La Ley*,14344 (2017): 1-8.
- Heredero Higueras, M., "La sentencia del Tribunal Constitucional de la República Federal

Alemana relativa al censo de población". *Documentación Administrativa*, 198 (1983): 139-158.

- Heredero, M. *La Directiva comunitaria de protección de datos de carácter personal*. Pamplona: Aranzadi, 1997.
- Hernández Moreno, A. "Ciberseguridad y confianza en el ámbito digital". *Información Comercial Española, ICE: Revista de economía,* 897 (2017): 55-66.
- Lasarte Álvarez, C. *Principios de Derecho Civil*. Tomo II: Derecho de Obligaciones. Madrid: Marcial Pons, 2018. PMid: 28789915

  Martínez Martínez, R. "El derecho fundamental a la protección de datos: Perspectivas". *Revista de Internet, Derecho y Política*, 5 (2007): 47-61.
- Murillo de la Cueva, L. *El derecho a la autodeterminación informativa*. Madrid: Tecnos, 1990.
- Navalpotro Navalpotro, Y. "El deber de secreto". En *Estudio práctico sobre la protección de datos de carácter personal,* ed. por C. Almuzara Almaida, 515 - 533. Madrid: Lex Nova, 2005. PMid: 16125456
- Ortega Giménez, A. O. y J. J. Gonzalo Domenech."Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea". *Revista de la Facultad de Derecho*, 44 (2018): 63-97.
  https://doi.org/10.22187/rfd2018n44a2
- Paniza Fullana, A. "Una nueva era en la privacidad y las comunicaciones electrónicas: La 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". *Revista Aranzadi Civil-Mercantil,* 4 (2017):105-122.
- Pérez Luño, A. E. *Derechos humanos, Estado de Derecho y Constitución*. Madrid: Tecnos, 2010.
- Piñar Mañas, J. L. "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas". *Cuadernos de Derecho Público*, 20 (2003): 45-90.
- Puldain Salvador, V. "El futuro marco legal para la protección del acceso a los datos".*Revista Ibero-Latinoamericana de Seguros,* 26, 47 (2017): 119-135.
  https://doi.org/10.11144/Javeriana.ris47.fmlp
- Troncoso Reigada, A. "La seguridad en el Reglamento General de Protección de Datos de la Unión Europea". *Diario La Ley*, 15647 (2018): 1-33.

RECIBIDO: 12/02/2019
APROBADO: 20/05/2019

Metamorfosis. Óleo. 90 x 100 cm.
Agustín Aquino Mejías (pintor peruano).