DEL PRINCIPIO DE SEGURIDAD DE LOS DATOS AL DERECHO A LA SEGURIDAD DIGITAL

ANTONIO TRONCOSO REIGADA
Universidad de Cádiz

El inicio de la aplicación del 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 –RGPDUE- (1) ha supuesto un cambio importante en el principio de seguridad de los tratamientos de datos personales, tal y como éste era entendido hasta ahora en el ordenamiento jurídico español, que lo vinculaba al cumplimiento de unas concretas medidas de seguridad aprobadas en una norma administrativa, lo que supone la materialización entre nosotros del principio de responsabilidad proactiva –art. 5.2 RGPDUE-. El RGPDUE aborda la seguridad en dos ámbitos materiales: como principio del tratamiento y como obligación del responsable y del encargado.

LA SEGURIDAD EN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA: EL PRINCIPIO DE SEGURIDAD

Así, en primer lugar, el RGPDUE contiene dentro del Capítulo II dedicado a los «Principios», los llamados «Principios relativos al tratamiento» –art. 5-, entre los que se encuentra el principio de «integridad y confidencialidad», en virtud del cual «los datos personales serán 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 daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas» –art. 5.1.f)-. En esta dirección, el Considerando 39 *in fine* del RGPDUE subraya que «los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento». Además, en segundo lugar, el RGPDUE establece dentro del Capítulo IV titulado «Responsable del tratamiento y encargado del tratamiento», una Sección 1ª dedicada a las obligaciones generales de estos y una Sección 2ª dedicada a la «Seguridad de los datos personales», que contiene tres preceptos que concretan el principio de seguridad en unas obligaciones del responsable: la «Seguridad el tratamiento» –art. 32-; la «Notificación de una violación de la seguridad de los datos personales a la autoridad de control» –art. 33-; y la «Comunicación de una violación de la seguridad de los datos personales al interesado» –art. 34-.

La seguridad en el Reglamento General de Protección de Datos de la Unión Europea a la luz de la Directiva 95/46/CE, de la LOPD y de su Reglamento de desarrollo en materia de seguridad. La STJUE de 30 mayo 2013, caso Worten

La regulación de la seguridad del tratamiento que hace la Sección 2ª del Capítulo IV del RGPDUE difiere de las normas de protección de datos personales que eran de aplicación hasta ahora en nuestro país. La Directiva 95/46/CE no proclamaba formalmente la seguridad como un principio de protección de datos sino que lo regulaba en el Capítuo II como una «Condición general para la licitud del tratamiento de datos personales», dentro de la Sección 8ª titulada «Confidencialidad y seguridad del tratamiento». El art. 17.1 de la Directiva 95/46/CE –Seguridad del tratamiento- señalaba que «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 la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales». La concreción de estas medidas de seguridad no le corresponde finalmente a la Comisión, a diferencia de la Propuesta de Directiva de 1990 que sí se las atribuía como parte del ejercicio de la potestad reglamentaria o de ejecución de la Comisión, sino que esta es una cuestión que queda en el ámbito de los Estados miembros (2).

El art. 17.1 de la Directiva 95/46/CE continuaba señalando que estas medidas técnicas y de organización adecuadas «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». Una interpretación plausible de este artículo es que el listado de medidas técnicas y de organización que podrán ser obligatorias para el responsable dependerá de los conocimientos técnicos existentes y del coste de su aplicación y que la aplicación a cada caso concreto dependerá de los riesgos que presente cada tratamiento y de la naturaleza de los datos personales (3). La cuestión es a quién le corresponde determinar las medidas técnicas y organizativas para la seguridad de los tratamientos –al Estado o a cada responsable del tratamiento- ya que la aplicación de las medidas al caso concreto le corresponderá en todo caso al responsable del tratamiento.

Es muy interesante a estos efectos la STJUE de 30 mayo 2013, *caso Worten* (asunto C-342/12), donde el TJUE tuvo que resolver una cuestión prejudicial en relación con el art. 17.1 de la Directiva 95/46/CE; en concreto, si este precepto «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, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red». El TJUE resuelve la cuestión prejudicial señalando que el art. 17.1 de la Directiva 95/46/CE «no impone a los Estados miembros, salvo cuando tienen la condición de responsables del tratamiento, la adopción de estas medidas técnicas y de organización, dado que *la obligación de adoptarlas incumbe únicamente al responsable del tratamiento, que en el presente caso es el empresario*. Sin embargo, la misma disposición sí exige a los Estados miembros la adopción de una disposición de Derecho interno que establezca esta obligación» –apdo. 25-. Es decir, los Estados no están obligados a imponer las concretas medidas de seguridad a los responsables salvo para sus propios tratamientos, pero sí tenían que aprobar una legislación que transpusiera la Directiva obligando al responsable a adoptar estas medidas para garantizar un nivel de seguridad adecuado (4).

Existían discrepancias entre los Estados a la hora de transponer el art. 17 de la Directiva 95/46/CE que regulaba la seguridad de los tratamientos. La mayoría de los Estados habían optado por una formulación similar a la prevista en el art. 17 de la Directiva, imponiendo únicamente a los responsables del tratamiento la obligación de aplicar medidas técnicas y de organización adecuadas para la protección de los datos personales contra la destrucción, pérdida accidental, difusión y acceso no autorizado y señalando que estas medidas debían garantizar un nivel de seguridad adecuado en relación con los riesgos y la naturaleza del tratamiento, pero sin establecer unas concretas medidas de seguridad. En cambio, como destacaba la Comisión, España aprobó una regulación que con gran nivel de detalle establece las medidas de seguridad técnicas y organizativas que debían ser implantadas, teniendo en cuenta el nivel de riesgo. Todo ello generaba un alto nivel de divergencia en relación con la seguridad de los tratamientos en la Unión Europea (5).

Así, la LOPD no se limitó a transponer este precepto, reproduciéndolo en términos generales en el art. 9.1 sino que avanza un poco más dentro del marco de una Directiva que es una obligación de fines que deja a los Estados la decisión sobre los medios. Por una parte, la LOPD consideró la seguridad de los datos como uno de los «Principios de protección de datos» recogidos en el Título II. Por otra parte, la LOPD no se circunscribió a establecer un mandato genérico de que «el responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole 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» –art. 9.1- LOPD-, que estaría en línea con lo plasmado en la Directiva

95/46/CE. Además, la LOPD añadió que «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» –art. 9.2-, completando que «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 [Datos especialmente protegidos]» –art. 9.3-. Así, señala, por una parte, que una norma reglamentaria establecerá las condiciones relativas a la integridad y a la seguridad que deben reunir los ficheros y los centros de tratamiento, locales, equipos, sistemas y programas; y, por otra parte, que específicamente en relación con los datos especialmente protegidos del art. 7 LOPD –los datos de carácter personal que revelen la ideología, afiliación sindical, religión o creencias, origen racial, salud y vida sexual-, una norma reglamentaria establecerá los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de estos datos. De hecho, la LOPD calificaba después como una infracción grave «mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen» -art. 44.3.h)- (6).

Por tanto, en nuestro país, hasta ahora el cumplimiento del principio de seguridad no era una obligación genérica del responsable sino que éste estaba obligado a cumplir unas medidas concretas. Si la Directiva 95/46/CE señalaba que los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, la LOPD, a diferencia de la legislación de otros países, ha vinculado el principio de seguridad a la adopción por parte del responsable del fichero de medidas de seguridad concretas. El principio de seguridad no podía considerarse una obligación de resultado porque la seguridad absoluta no existe. De esta forma, el incumplimiento por parte del responsable de una concreta medida de seguridad era lo que podía justificar en nuestro país una declaración de infracción por vulneración del principio de seguridad (7). La normativa que desarrolló esta previsión legal del art. 9.2 y 3 LOPD fue, en primera instancia, el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal, aprobado por el Real Decreto 994/1999, de 11 de junio, y finalmente, el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, que regulaba en su Título VIII «las medidas de seguridad en el tratamiento de datos de carácter personal» –y derogaba el Real Decreto anterior-.

La LOPD no establecía que todos los ficheros y tratamientos tuvieran que cumplir idénticas medidas de seguridad sino esto dependía del estado de la tecnología, de la naturaleza de los datos almacenados y de los riesgos a los que estén expuestos, ya provengan de la acción humana o del medio físico o natural. Como acabamos de señalar, parece razonable que la definición del listado de medidas de seguridad dependa de los conocimientos técnicos existentes (8) y sea algo que le corresponda al regulador mientras que su exigencia a los responsables y encargados dependa de la naturaleza o clase de datos personales y de los riesgos que presente cada tratamiento, que también es consecuencia en parte –aunque no sólo- de la naturaleza de los datos. En esta dirección, el Reglamento de Medidas de Seguridad de los Ficheros Automatizados de 1999 estableció tres niveles de seguridad, dependiendo, únicamente, de la tipología de datos, haciendo una especial consideración, además, a los datos especialmente protegidos. Así, el Reglamento de 1999 señalaba que la atribución de un nivel de seguridad básico, medio y alto se establecía «atendiendo a la *naturaleza de la información* tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información» –art. 3- (9). Era la naturaleza de la información –en el fondo, la clase de dato- lo que determinaba la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información y, por tanto, la aplicación de un nivel de seguridad básico, medio y alto. Esta regulación atendía de manera específica a la preocupación que el legislador había manifestado en el art. 9.3 LOPD por la seguridad de los tratamientos de datos regulados en el art. 7 LOPD. Hay que recordar que los tratamientos de datos especialmente protegidos estaban sometidos también a unas mayores exigencias de legitimación del tratamiento, tanto en la Directiva 95/46/CE –art. 8- como en la LOPD –art. 7-, especialmente en relación con el consentimiento. De esta forma, la consideración de un dato como especialmente protegido tenía consecuencias no sólo en relación con los requisitos de licitud del tratamiento sino también con la definición de las medidas de seguridad que debían ser adoptadas. Este modelo de regulación no atendía específicamente a otros elementos recogidos en el art. 9.1 LOPD como el estado de la tecnología o los riesgos a los que están expuestos los datos almacenados, provenientes de la acción humana o del medio físico o natural. O mejor dicho, este modelo de regulación está pensado para que el responsable del tratamiento aplique las medidas de seguridad teniendo en cuenta la naturaleza de los datos, sin tener que valorar los riesgos a los que están expuestos o el estado de la tecnología. Este planteamiento traslada la idea de que estos dos últimos elementos no deben preocuparle al responsable o al encargado porque ya los ha tenido en cuenta el regulador al definir las medidas de seguridad y al concretarlas teniendo en cuenta la naturaleza de los datos sometidos a tratamiento.

En esta dirección, el Reglamento de medidas de seguridad de 1999 reguló de manera específica la aplicación de los niveles de seguridad básico, medio y alto, teniendo en cuenta la naturaleza o la categoría de datos –art. 4-. Años más tarde, el Reglamento de desarrollo de la LOPD de 2007 precisó y delimitó mejor

el tipo de datos a los que había que aplicar las medidas de seguridad -art. 81-(10). Esta normativa estableció con carácter general que todos los ficheros que contengan datos de carácter personal debían adoptar las medidas de seguridad calificadas de nivel básico –por ejemplo, los ficheros con datos personales de carácter identificativo, académicos, de empleo y carrera profesional-. Las medidas de seguridad de nivel medio —además de las de nivel básico— debían implantarse en los ficheros y tratamientos que contengan datos relativos a la comisión de infracciones penales o administrativas, en los ficheros o tratamientos cuyo funcionamiento se rija por el art. 29 de la LOPD —es decir, los de solvencia patrimonial y de crédito—, en aquellos de los que sean responsables las Administraciones Tributarias y se relacionen con el ejercicio de sus potestades tributarias, en los ficheros y tratamientos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros, en los ficheros o tratamientos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias, en aquellos de los que sean responsables las Mutuas de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social, así como en aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos. Finalmente, había que implantar medidas de seguridad de nivel alto —además de las de nivel básico y medio— a los ficheros y tratamientos con datos de ideología, afiliación sindical, religión y creencias, raza, salud y vida sexual –los llamados datos especialmente protegidos del art. 7 LOPD-, a los ficheros y tratamientos para fines policiales y a los ficheros o tratamientos que contengan datos derivados de actos de violencia de género (11). En general, eran muchos los ficheros en los que había que implementar medidas de seguridad de nivel alto (12). No obstante, hay que indicar que el Reglamento de desarrollo de la LOPD había tratado de reducir en algunos casos el nivel de seguridad exigible a algunos ficheros y tratamientos, como los relativos a recursos humanos o nóminas. Este descenso era consecuencia, «por una parte, [de] la experiencia dimanante de la aplicación del Real Decreto 994/1999 [que] permitía conocer las dificultades que habían enfrentado los responsables e identificar los puntos débiles y fuertes de la regulación. Por otra, se reclamaba la adaptación de la regulación en distintos aspectos» -Exposición de Motivos, apdo. III del Real Decreto 1720/2007, de 21 de diciembre- (13).

Las novedades del Reglamento General de Protección de Datos de la Unión Europea en relación con la seguridad

El RGPDUE establece dentro las obligaciones generales del responsable recogidas en el Capítulo IV la llamada «responsabilidad del responsable del tratamiento», una tautología que concreta uno de los nuevos principios relativos al tratamiento que es el de «responsabilidad proactiva», en virtud del cual «el responsable del tratamiento será responsable del cumplimiento de [los principios relativos al tratamiento] y capaz de demostrarlo» –art. 5.2-. Por ello, el responsable del tratamiento debe aplicar las medidas técnicas y organizativas *apropiadas* «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» para garantizar y poder demostrar que el tratamiento es conforme con el Reglamento –art. 24.1-.

El RGPDUE obliga al responsable a ser reflexivo, a llevar a cabo una valoración, por una parte, de la naturaleza del tratamiento, del ámbito, del contexto y de los fines, y por otra parte, de los riesgos para los derechos de las personas que pueden provenir del tratamiento de datos, también de la gravedad de los riesgos y de su mayor o menor probabilidad; es decir, le obliga a realizar una evaluación de los riesgos –alto, estándar o bajo-. En virtud de esta evaluación, el responsable del tratamiento debe aplicar las medidas técnicas y organizativas apropiadas no sólo para garantizar que el tratamiento de datos personales cumple el Reglamento –esto es insuficiente- sino también para poder demostrarlo. El responsable debe adoptar las medidas adecuadas a cada caso concreto, con un claro enfoque al riesgo –qué cosas pueden pasar para evitar que pasen-, obligándole incluso a valorar el riesgo en términos de probabilidades. Además, se establece un mayor dinamismo y fluidez en el análisis del cumplimiento de las medidas al señalar que «dichas medidas se revisarán y actualizarán cuando sea necesario» –art. 24.1 *in fine* RGPDUE-.

El Capítulo IV del RGPDUE establece un conjunto de obligaciones del responsable y del encargado del tratamiento, con una marcada dirección hacia la autorregulación (14). Así, dentro de las obligaciones generales se establece que las oportunas políticas de protección de datos serán medidas técnicas y organizativas para garantizar y poder demostrar el cumplimiento de la normativa, cuando sean proporcionadas con las actividades del tratamiento –art. 24.2-. También se establece expresamente la adhesión a los códigos de conducta y los mecanismos de certificación como «elementos para poder demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento» –art. 24.3-.

El RGPD contiene otras obligaciones del responsable del tratamiento que provienen del ámbito de la autorregulación como la protección de datos desde el diseño y por defecto –art. 25-, el registro de las actividades de tratamiento –art. 30-, la evaluación de impacto relativa a la protección de datos –art. 35-, el delegado de protección de datos –arts. 37 a 39-, los códigos de conducta –arts. 40 a 41-, y la certificación –arts. 42 y 43-. Todo esto configura un modelo de responsable, siguiendo la tautología presente en el título del art. 24, doblemente responsable, que actúa según el principio de responsabilidad proactiva. Por

tanto, el RGPDUE configura un modelo de responsable con iniciativa, diligente, que no se limita a cumplir una norma porque la solución ya no a venir definida en ésta. El Reglamento quiere un responsable que piense en la protección de datos en el momento del diseño del sistema de información y que la prevea por defecto, que se asesore de una persona con conocimientos especializados en protección de datos, que lleve a cabo una evaluación de impacto de las operaciones de tratamiento en la protección de datos y que se adhiera a códigos de conducta o a mecanismos de certificación. El Reglamento se aleja así del modelo de responsable definido en la LOPD, que era una figura más pasiva, diseñando un modelo de responsable como una figura más activa y propositiva, más moderno, más *cool*, inspirado en un modelo anglosajón de responsabilidad *–accountability, compliance-*, que no se limita a cumplir lo que dice una norma sino que previene posibles incumplimientos (15).

El RGPDUE dedica el Capítulo IV al responsable y al encargado del tratamiento, donde se contienen un conjunto de obligaciones que sirven para que el tratamiento de datos personales respete los derechos de las personas en este ámbito. Específicamente el RGPDUE dedica la Sección 2ª del Capítulo IV a la Seguridad de los datos personales. Esta Sección tiene tres artículos: el art. 32 dedicado a la «Seguridad del tratamiento», el art. 33 relativo a la «Notificación de una violación de la seguridad de los datos personales a la autoridad de control» y el art. 34 que regula la «Comunicación de una violación de la seguridad de los datos personales al interesado».

La seguridad del tratamiento como obligación del responsable y del encargado del tratamiento y la modificación de la Propuesta de Reglamento de la Comisión

El RGPDUE regula la seguridad del tratamiento como obligación del responsable y del encargado del tratamiento –art. 32.1-. Así establece que «teniendo en cuenta 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, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo» (16). La redacción de este precepto tiene mucho en común por no decir que reitera el art. 24.1 del RGPDUE, que recogía la «responsabilidad del responsable del tratamiento» ya analizada. De nuevo se establece: primero, que el responsable y el encargado del tratamiento «aplicarán medidas técnicas y organizativas apropiadas»; segundo, que para la aplicación de estas medidas se tendrá en cuenta dos elementos: el tratamiento –su naturaleza, alcance (el art. 24.1 utilizaba una expresión semejante como el «ámbito»), contexto y fines del tratamiento- y los riesgos para los derechos de las personas, tanto su probabilidad como su gravedad; tercero, que la finalidad de estas medidas es garantizar un nivel de seguridad adecuado al riesgo, una finalidad más concreta y coherente con el objeto del artículo que es la seguridad del tratamiento, que se separa de la finalidad más genérica del art. 24.1 de garantizar y poder demostrar el cumplimiento del Reglamento.

En todo caso, el art. 32.1 RGPDUE, después de señalar que el responsable y el encargado del tratamiento deben aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, menciona expresamente algunas medidas que han de tenerse en cuenta:

En primer lugar, el RGPDUE menciona expresamente que dentro de las medidas técnicas deben estar «la seudonimización y el cifrado de datos personales» –art. 32.1.a)-. Es decir, si bien el RGPDUE no precisa en concreto qué medidas de seguridad debe implantar el responsable y el encargado del tratamiento, hace una excepción con la seudonimización y el cifrado. De hecho, la seudonimización y el cifrado son las dos únicas medidas de seguridad técnicas que se incorporan al Reglamento lo que dice mucho de su importancia. Hay que insistir en que en todo el texto del RGPDUE se percibe una apuesta constante por la seudonimización y por el cifrado.

En segundo lugar, el RGPDUE señala que las medidas técnicas y organizativas deben tener «la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento» –art. 32.1.b)-. Por tanto, la seguridad del tratamiento requiere la garantía de la confidencialidad, integridad, disponibilidad y resiliencia. En esta misma dirección, el art. 32.2 señala que «al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de 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». Se trata de adoptar medidas adecuadas de seguridad para evitar estos riesgos. Los riesgos de comunicación o acceso no autorizados, a los que también hacía mención el art. 17.1 de la Directiva 95/46/CE -empleando también la palabra difusión- y el art. 9.1 LOPD, obligan al responsable a adoptar medidas para garantizar la confidencialidad de la información (17). Posiblemente, la seguridad como principio relativo a la protección de datos personales tradicionalmente ha estado vinculado a la confidencialidad y a evitar accesos indebidos. Los riesgos de destrucción, pérdida o alteración accidental o ilícita de datos personales, que ya se contenían en el art. 17.1 de la Directiva 95/46/CE y, de manera más incompleta, en el art. 9.1 LOPD, obligan a tomar medidas para garantizar la integridad de la información. De hecho, estos dos aspectos de la seguridad son tan importantes que el art. 5.1.f) RGPDUE, como hemos señalado antes, incluye dentro de los principios relativos al tratamiento el de «integridad y confidencialidad», en virtud del cual «los datos perso-

nales serán 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 daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas». El RGPDUE añade en relación con la Directiva 95/46/CE y la LOPD la necesidad de aplicar medidas técnicas y organizativas para garantizar la disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento –art. 32.1.b)-. Además, reitera que las medidas técnicas deben ser apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que incluya «la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico» –art. 32.1.c). Si la seguridad como disponibilidad de la información es bien conocida entre nosotros, la resiliencia es un concepto más novedoso y hace referencia a la capacidad de un responsable o encargado del tratamiento para seguir cumpliendo sus funciones en situaciones de riesgo, lo que conlleva una monitorización continua del nivel de protección y de los riesgos potenciales.

En tercer lugar, las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo deben incluir «un proceso de verificación, evaluación y valoración regulares de [su] eficacia […] para garantizar la seguridad del tratamiento» –art. 32.1.d)-. Por tanto, no es suficiente con implantar unas medidas en un momento concreto –al principio del tratamiento- sino que es necesario una evaluación y verificación continuas y regulares de la eficacia de estas medidas. Esta previsión coincide con la recogida en el art. 24.1 *in fine* del RGPDUE ya mencionada de que las medidas técnicas y organizativas apropiadas para garantizar que el tratamiento cumple con esta normativa «se revisarán y actualizarán cuando sea necesario».

En cuarto lugar, el RGPDUE señala que la adhesión a un código de conducta o a un mecanismo de certificación «podrá servir de elemento para demostrar» que se adoptan las medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado y que, por tanto, se cumplen los requisitos recogidos en el art. 32.1 –art. 32.3-, lo que acredita la apuesta por los mecanismos de autorregulación. De nuevo, aparece aquí una reiteración con la previsión contenida en el art. 24.3 RGPDUE que señalaba que la adhesión a códigos de conducta o a mecanismos de certificación pueden ser elementos para demostrar el cumplimiento de las obligaciones del responsable del tratamiento.

Finalmente, el RGPDUE establece que «el responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros» –art. 32.4-.

En lo relativo a la seguridad del tratamiento es tan relevante lo que dice el RGPDUE como lo que deja de decir. De hecho, el texto del RGPDUE se aparta deliberadamente en este aspecto de la Propuesta de Reglamento de la Comisión. Esta Propuesta, siguiendo en este punto la regulación española -y a diferencia de la Directiva 95/46/CE-, concretaba el cumplimiento del principio de seguridad por parte del responsable en la implantación de medidas concretas aprobadas previamente por la Comisión, lo que facilitaba la declaración de infracción, objetivando la actividad de la autoridad de control. De esta forma, la vulneración del principio de seguridad por parte del responsable estaba vinculado en la Propuesta de la Comisión al incumplimiento de unas medidas concretas. La propuesta de Reglamento no incluía una referencia a niveles de seguridad ni tampoco un conjunto de medidas de seguridad a implementar sino que, al igual que el art. 9 LOPD que prevé su desarrollo reglamentario, y a diferencia de la Directiva, facultaba a la Comisión para realizar los actos normativos necesarios para especificar las medidas técnicas y organizativas, lo que incluía la referencia a sectores específicos y situaciones de tratamiento de datos, teniendo en cuenta no sólo la evolución de la tecnología, sino también las soluciones de privacidad desde el diseño y la protección de datos por defecto (18).

Existía un problema de divergencia entre los Estados miembros de la Unión Europea en relación con la normativa sobre seguridad de los tratamientos que transponía la Directiva 95/46/CE, lo que perjudicaba el funcionamiento del mercado interior (19). Esta fragmentación de la legislación, como hemos señalado en otro momento, dificultaba la comercialización de productos y servicios de la sociedad de la información y la implantación de políticas de privacidad paneuropeas, obligando a las empresas a adaptarse y a adaptar sus productos a las cambiantes legislaciones nacionales, lo que representaba un límite a la competencia –empresas en países con un mayor y menor nivel de exigencia sobre seguridad de los tratamientos- e incrementaba los costes –al tener que hacer extensiones nacionales de sus productos-. La Comisión planteaba inicialmente enfrentarse a esta divergencia a través de la aprobación de una normativa común relativa a la seguridad de los tratamientos para toda la Unión Europea aprobada por la Comisión.

Finalmente, pudo más en la negociación del RGPDUE la voluntad de simplificación normativa en materia de protección de datos, que trataba de suprimir o de flexibilizar las exigencias que los mercados consideraban trabas burocráticas y el acercamiento a la posición anglosajona –en un Reglamento negociado en una situación pre-Brexit- de no sobrecargar –*not overburden*- a las empresas, ayudando al desarrollo económico del mercado digital y a la innovación También pudo más el avance hacia un modelo de autorregulación, que dejaba esas cuestiones –como otras- en manos de los responsables del tratamiento. De esta forma, suprimiendo la normativa sobre medidas de seguridad se materializó uno de los objetivos

del RGPDUE de hacer sencilla la protección de datos, reduciendo las obligaciones impuestas por las normas pero incrementando al mismo tiempo la *accountability*. En todo caso, hay que recordar, que las obligaciones de seguridad de los tratamientos subsisten para el responsable, con importantes sanciones económicas por lo que no sabemos si finalmente las empresas han ganado en flexibilidad pero han perdido en seguridad jurídica en relación con sus obligaciones relativas a la seguridad de los tratamientos (20).

El RGPDUE supone un importante cambio en lo relativo a la seguridad de los tratamientos. No se prevé que la Comisión o los Estados miembros vayan a aprobar un conjunto de medidas de seguridad sino que le corresponde ahora al responsable del tratamiento en virtud del Reglamento aplicar en cada caso las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento y los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas. Por tanto, le corresponde al responsable valorar en cada supuesto qué medidas de seguridad debe aplicar porque, como señalamos anteriormente, la respuesta no va a venir prevista en la norma. Debe llevar a cabo una evaluación de riesgos (21), lo que pone de manifiesto el principio de responsabilidad proactiva.

Como hemos señalado en otro momento (22), «las medidas de seguridad reguladas en el Real Decreto 1720/2007 de 21 de diciembre, podrán ser indicativas, incluso a nuestro juicio en un futuro próximo la mera aplicación de estas medidas acredita que el responsable del tratamiento garantiza un nivel de seguridad adecuado al riesgo –si estas medidas eran adecuadas hasta ahora, lo normal es que lo sigan siendo-. Pero lo que queremos resaltar en este momento es que en relación con la seguridad de los tratamientos, el Reglamento se aleja de un modelo de seguridad basado en que el responsable aplique unas normas predeterminadas decididas por la Administración. El Reglamento no sólo desplaza las normativas nacionales en materia de seguridad e impide que los Estados nacionales dicten una normativa en materia de seguridad, sino que tampoco permite que esa materia sea objeto de actos de delegación y aplicación por parte de la Comisión. El Reglamento no establece unas medidas específicas sino que deja en manos de los responsables del tratamiento la adopción de las medidas técnicas y organizativas apropiadas al caso concreto, si bien es posible que las autoridades de control elaboren y den publicidad a protocolos, parámetros o indicadores de seguridad».

De esta forma, «el Reglamento se aleja de un modelo jurídico de Derecho continental europeo, que proviene del Derecho romano y que se caracteriza por una amplia regulación y una predeterminación de la solución jurídica, para acercarse más a un modelo de *Common Law*, que se caracteriza por una mayor desregulación y que tiene en cuenta la valoración del caso concreto. Esto se pone de manifiesto especialmente en las medidas de seguridad de los tratamientos. Pues bien, estas medidas de seguridad no sólo han sido desplazadas y como obligación jurídica para el responsable resultaban inaplicables desde el 25 de mayo de 2018, sino que a nuestro juicio su incumplimiento *por sí solo* en ese periodo transitorio no podía haber sido fundamento para la declaración de una infracción en virtud del principio de retroactividad de las disposiciones administrativas más favorables –art. 9.3 CE-. Evidentemente, la introducción de elementos de la cultura jurídica anglosajona, como la autorregulación, la desregulación y la *accountability*, si bien aporta una mayor flexibilidad a la hora de buscar soluciones al caso concreto y de adaptarse a los futuros cambios tecnológicos, también supone, como acabamos de señalar, una mayor inseguridad jurídica para aquellos responsables acostumbrados a la detallada y extensa regulación característica del modelo jurídico continental».

Hay que mencionar, en todo caso, que el RGPDUE ha tenido en cuenta la importancia de la seguridad del tratamiento al definir las funciones del Comité Europeo de Protección de Datos –art. 70-. Así, le corresponde a este Comité supervisar y garantizar la aplicación coherente del RGPDUE y asesorar a la Comisión sobre cualquier cuestión relativa a la protección de datos personales en la Unión Europea –art. 70.1.a) y b)-, lo que también alcanza la seguridad del tratamiento. En especial, el Comité examinará «cualquier cuestión relativa a la aplicación del Reglamento, y emitirá directrices, recomendaciones y buenas prácticas a fin de promover la aplicación coherente del Reglamento» –art. 70.1.e)-. En especial, a lo que a nosotros nos interesa, le corresponde al Comité Europeo emitir *directrices, recomendaciones y buenas prácticas* «a fin de constatar las violaciones de la seguridad de los datos y determinar la dilación indebida y con respecto a las circunstancias particulares en las que el responsable o el encargado del tratamiento debe notificar la violación de la seguridad de los datos personales» –art. 70.1.g)- y «con respecto a las circunstancias en las que sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas» –art. 70.1.h). El Comité Europeo no va a aprobar normas en materia de seguridad, pero sí algún tipo de *soft law* a este respecto.

La notificación de una violación de la seguridad de los datos personales a la autoridad de control

El RGPDUE no sólo regula, dentro de la Sección 2ª dedicada a la «Seguridad de los datos personales», la seguridad de los tratamientos, sino que también aborda las violaciones de la seguridad de los datos personales que requieren una notificación a la autoridad de control y una comunicación al interesado. Esta es una de las novedades en materia de seguridad de los datos que aparecen en el RGPDUE y que adelantaba la Propuesta de la Comisión. De hecho, entre las definiciones no-

vedosas que incluye el RGPDUE –que se encontraba también en la Propuesta de la Comisión- y que no estaba ni en la Directiva 95/46/CE, ni en la LOPD ni en su Reglamento de desarrollo es la de «violación de la seguridad de los datos personales», más conocida por brechas de seguridad -las llamadas «*BCR`s*-» (23) como «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» -4.16-. Esta definición de la violación de la seguridad de los datos personales está centrada en la seguridad como garantía de la integridad y de la confidencialidad de la información, dejando de lado la disponibilidad y la resiliencia. Ahora bien, no toda violación de la seguridad de los datos personales debe ser notificada a la autoridad de control y comunicada a los interesados. El RGPDUE establece que el responsable del tratamiento notificará una violación de la seguridad de los datos personales a la autoridad de control cuando sea probable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas –art. 33.1- (24). Así, el Considerando 89 del RGPDUE aclara este punto señalando que el responsable no lo notificará a la autoridad cuando «pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas». Por tanto, el parámetro para determinar si hay que notificar la violación de la seguridad a la autoridad de control es si existe riesgo para los derechos y las libertades de las personas (25). De esta forma, se materializa de manera práctica que la seguridad de la información no es una materia únicamente tecnológica, sino que está vinculada al ejercicio de los derechos, que la protección de datos personales no es sólo un derecho autónomo sino una garantía institucional de otros derechos y que el principio de seguridad tiene una gran relevancia dentro del contenido del derecho fundamental a la protección de datos personales (26).

Esta notificación a la autoridad de control competente debe hacerse «sin dilación indebida» – dice el Considerando 85 «tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales»-, «y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella» (27). Así, se establece que «si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de la indicación de los motivos de la dilación» –art. 33.1-. En este punto, el Considerando 87 del RGPDUE aporta algo de confusión al establecer que «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», cuando estos son elementos para valorar la necesidad o no de la notificación a la autoridad de control y no para determinar el plazo para esta notificación. El Considerando 85 del RGPDUE recoge claramente la importancia de que esta notificación a la autoridad de control competente se haga sin dilación indebida, aportando ejemplos de cómo las violaciones de la seguridad constituyen un riesgo para los derechos y las libertades de las personas físicas y, por tanto, deben ser notificadas a la autoridad de control. Así, «si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona», justificaciones que muchas de ellas sirven también para razonar la comunicación de esta violación al interesado.

Así, la notificación a la autoridad de control deberá como mínimo: «describir 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», «describir las posibles consecuencias de la violación de la seguridad de los datos personales» y «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» –art. 33.3-. Además, «si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida» –art. 33.4-.

Lógicamente, la notificación de la violación de la seguridad de los datos personales a la autoridad de control no es una formalidad administrativa vacía sino que está destinada a facilitar el ejercicio por parte de la autoridad de control de los poderes de investigación y correctivos para garantizar el cumplimiento de la normativa de protección de datos personales en lo relativo a la seguridad del tratamiento, comprobando que el responsable y el encargado del tratamiento aplican todas las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, valorando, en su caso, 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 –art. 32.1 RGPDUE-. No hay que olvidar que la notificación de la violación a la autoridad de control está regulada en la Sección 2ª dedicada a la «Seguridad de los datos personales». De hecho, el Considerando 87 del RGPDUE establece que la notificación a la autoridad de control «puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el [...] Reglamento». Evidentemente esta posibilidad tiene que ser aplicada con prudencia, teniendo en cuenta el riesgo de disuadir las notificaciones de violaciones de segu-

ridad a la autoridad de control. No obstante, hay que recordar que «la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida» es un elemento que se tiene en cuenta al decidir la imposición de una multa administrativa y su cuantía en cada caso individual –art. 83.2.h) RGPDUE-.

Hay que subrayar que bajo el título de «Notificación de una violación de la seguridad de los datos personales a la autoridad de control», el RGPDUE contiene dos obligaciones importantes en materia de seguridad de los tratamientos de datos personales, que tienen una autonomía propia. La primera es la obligación del responsable del tratamiento de documentar «cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas». Esta obligación de documentación de las violaciones de seguridad permitirá a la autoridad de control, señala expresamente el RGPDUE, verificar el cumplimiento de la obligación de notificación –art. 33.5-, lo que se extiende a comprobar que se ha notificado cuando está preceptuado –cuando sea probable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas- y que esta notificación se ha hecho sin dilaciones indebidas. También a nuestro juicio esta obligación de documentación de las violaciones de la seguridad debe servir a la autoridad de control para supervisar la seguridad del tratamiento, es decir, para asegurar que el responsable y el encargado del tratamiento están aplicando todas las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo y que han valorado para ello el estado de la técnica, los costes de aplicación, y la naturaleza y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas –art. 32.1 RGPDUE-. Esta obligación de documentación de las violaciones de seguridad recuerda la obligación del responsable y del encargado que se contenía en el art. 28 de la Propuesta de Reglamento de la Comisión de documentar y de conservar la documentación de todas las operaciones de tratamiento efectuadas bajo su responsabilidad, quedando esta documentación a disposición de la autoridad de control (28). En todo caso, haya o no una ulterior obligación de notificación a la autoridad de control, la mera existencia de una violación de la seguridad de los datos personales obliga al responsable a documentarla, incluyendo los hechos, los efectos y las medidas correctoras, lo que le obliga a verificar si ha aplicado toda la protección tecnológica adecuada y si ha 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», como expresa de manera algo confusa el Considerando 87 del RGPDUE. Hay que recordar, como hemos señalado anteriormente, que la adopción de medidas técnicas y organizativas debe estar sometido a un proceso de verificación y evaluación constante para garantizar un nivel de seguridad adecuado al riesgo –art. 32.1.d)-, por lo que una violación de la seguridad por sí solo justifica este proceso de revisión de las medidas de seguridad por parte del responsable.

La segunda obligación en materia de seguridad de los tratamientos de datos personales contenida en el art. 33 es la de notificación de la violación de la seguridad de los datos personales del encargado del tratamiento al responsable, que, a diferencia de la notificación del responsable a la autoridad de control, se hará siempre y en todos los supuestos y sin dilación indebida –art. 33.2-. Esta notificación servirá al responsable para determinar si el encargado garantiza el cumplimiento de las medidas de seguridad.

La comunicación de una violación de la seguridad de los datos personales al interesado

Para finalizar la Sección 2ª del Capítulo IV dedicada a la «Seguridad de los datos personales» regula la obligación de comunicar una violación de la seguridad de los datos personales al interesado cuando sea probable que ésta «entrañe un alto riesgo» para sus derechos y libertades –art. 34.1- (29), comunicación que va a permitir al interesado «tomar las precauciones necesarias» –Considerando 86 del RGPDUE- (30).

No obstante, el RGPDUE establece algunos supuestos donde no es necesaria esta comunicación al interesado: que el responsable del tratamiento «haya adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado»; que el responsable del tratamiento «haya tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado», o que «suponga un esfuerzo desproporcionado» (31), por lo que, en este último caso, se deberá llevar a cabo una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados –art. 34.3-. Además, se establece que «cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas» en el art. 34.3 que hace innecesaria esta comunicación.

Por tanto, la comunicación de una violación de seguridad de los datos personales a un interesado no es una obligación en todos los supuestos. Además, el Considerando 73 del RGPDUE aclara un conjunto de circunstancias en que no es preceptiva esta comunicación, poniendo un límite al derecho a la protección de datos personales para garantizar otros derechos y bienes jurídicos: «El Derecho de la Unión o de los Estados miembros puede imponer restricciones a esta obligación en la medida en que sea necesario y pro-

porcionado en una sociedad democrática para salvaguardar la seguridad pública, incluida la protección de la vida humana, especialmente en respuesta a catástrofes naturales o de origen humano, la prevención, investigación y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública o de violaciones de normas deontológicas en las profesiones reguladas, y su prevención, otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un importante interés económico o financiero de la Unión o de un Estado miembro, la llevanza de registros públicos por razones de interés público general, el tratamiento ulterior de datos personales archivados para ofrecer información específica relacionada con el comportamiento político durante los regímenes de antiguos Estados totalitarios, o la protección del interesado o de los derechos y libertades de otros, incluida la protección social, la salud pública y los fines humanitarios. Dichas restricciones deben ajustarse a lo dispuesto en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales».

En todo caso, cuando sea preceptiva la comunicación de una violación de la seguridad de los datos personales al interesado, el RGPDUE regula el plazo para efectuar esta comunicación, la forma de hacerlo y su contenido –art. 34.1 y 2-. Así, el responsable del tratamiento comunicará al interesado sin dilación indebida –«tan pronto como sea razonablemente posible»- (32), utilizando un lenguaje claro y sencillo, la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Esta comunicación contendrá como mínimo 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, la descripción de las posibles consecuencias de la violación de la seguridad de los datos personales y de 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. Esta comunicación al interesado debe hacerse en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales -Considerando 86 RGPDUE-. De hecho, el Considerando 88 *in fine* del RGPDUE señala que las normas y procedimientos sobre las comunicaciones de las violaciones de seguridad de los datos personales al interesado deben «tener en cuenta los intereses legítimos de las autoridades policiales en caso de que una comunicación prematura pueda obstaculizar innecesariamente la investigación de las circunstancias de una violación de la seguridad de los datos personales».

Finalmente hay que señalar que este enfoque al riesgo y la valoración del riesgo en términos de probabilidades que predica el RGPDUE se ponen de manifiesto en estas dos medidas de seguridad contenidas en la Sección 2ª del Capítulo IV. La violación de la seguridad de los datos personales debe notificarse a la autoridad de control «a menos que sea improbable que dicha violación de seguridad constituya un riesgo para los derechos y libertades de las personas físicas» –art. 33.1-. Igualmente, la comunicación al interesado de una violación de la seguridad de los datos personales debe hacerse «cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas» –art. 34.1-.

Otras referencias a la seguridad en el Reglamento General de Protección de Datos de la Unión Europea

La seguridad de los tratamientos no se encuentra regulada únicamente en la Sección 2ª del Capítulo IV, sino que está presente en todo el RGPDUE, lo que pone en evidencia la importancia de la seguridad en la normativa de protección de datos personales y, en definitiva, en el derecho fundamental a la protección de datos personales.

El RGPDUE subraya la importancia de la seguridad en la regulación del encargado del tratamiento. Así, la obligación de seguridad del tratamiento recogida en el art. 32.1 no sólo le corresponde al responsable sino también al encargado. El art. 28.1 del RGPDUE que regula al encargado del tratamiento incide en la importancia de la seguridad de los tratamientos a la hora de elegir encargado del tratamiento por parte del responsable. Destaca que hay que elegir un encargado que ofrezca garantías suficientes para implementar las medidas apropiadas –existe una responsabilidad *in eligendo,* a la que ya hacía mención la Directiva en relación con la seguridad- (33). Así, establece que «cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado» –art. 28.1-. El Considerando 81 del RGPDUE es aún más claro al señalar que «para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento» (34). El contrato o acto jurídico que vincule al responsable con el encargado deberá estipular también que el encargado «tomará todas las medidas necesarias de conformidad con el artículo 32 [relativo a la seguridad del tratamiento]» y «ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a

36 [notificaciones de las violaciones de seguridad a la autoridad de control y al interesado» –art. 28.3.c) y f)-, exigencias que se aplican igualmente cuando el encargado recurra a otro encargado.

La seguridad del tratamiento no sólo es una obligación del responsable y del encargado del tratamiento, sino que también supone un interés legítimo del responsable que le justifica para poder llevar a cabo sus propios tratamientos de datos personales. Hay que recordar que un criterio de licitud del tratamiento de datos personales del responsable sin consentimiento del interesado es que este sea necesario «para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales» –art. 6.1.f) RGPDUE-. Pues bien, el Considerando 49 del RGPDUE afirma que «constituye un interés legítimo del responsable del tratamiento interesado el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para *garantizar la seguridad de la red* y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, *y la seguridad de los servicios conexos* ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas».

Por otro lado, también tiene una gran importancia la seguridad de los tratamientos en la regulación que el RGPDUE hace de la protección de datos desde el diseño –art. 25.1-. Hay que subrayar que el RGPDUE regula la protección de datos desde el diseño y por defecto no como un principio sino como una de las obligaciones generales del responsable y del encargado del tratamiento –Sección 1ª del Capítulo IV-. De hecho, como hemos adelantado, haber implantado la protección de datos desde el diseño es una forma de demostrar que se aplican medidas técnicas y organizativas apropiadas. El Considerando 78 establece que «la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del Reglamento», por lo que «a fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto». Por ello, el RGPDUE establece, al regular la protección de datos desde el diseño y por defecto, que el responsable del tratamiento «*aplicará,* tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, *medidas técnicas y organizativas apropiadas, como la seudonimización*, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados» –art. 25.1-. Estas medidas permitirán al responsable del tratamiento «crear y mejorar elementos de seguridad» –Considerando 78-. Lógicamente, la determinación de estas medidas técnicas y organizativas apropiadas debe tener en cuenta «el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas»–art. 25.1 RGPDUE-.

La importancia de la seguridad del tratamiento en la privacidad en el diseño no afecta sólo al responsable y encargado del tratamiento sino de manera a específica a las empresas de productos, servicios y aplicaciones que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función. Estas deben «desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos» teniendo en cuenta el derecho a la protección de datos y asegurándose «con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos» –Considerando 78 *in fine* del RGPDUE-. Esta apuesta del RGPDUE por la protección de datos desde el diseño y por defecto es coherente con la importancia que en los últimos años la Comisión Europea había dado a las «tecnologías de protección de la privacidad –PET-, considerando que era necesaria la utilización de las propias tecnologías como aliadas para favorecer el respeto a la protección de datos personales, lo que ya anticipaba el posterior paso adelante dado por el Reglamento hacia la autorregulación. Como hemos señalado en otro momento, estas iniciativas tratan de «alcanzar sinergias con la industria para que ésta proporcione equipos y software que permita el cumplimiento de la legislación de protección de datos personales». Para la Comisión, si bien «la responsabilidad jurídica del cumplimiento de las normas de protección de datos personales recae en los responsables de su tratamiento, desde el punto de vista social y ético también recae en parte, por ejemplo, en quienes elaboran las especificaciones técnicas y quienes realmente desarrollan o ejecutan programas o sistemas operativos» (35).

También hay que mencionar la referencia a la seguridad dentro de una nueva obligación del responsable

del tratamiento que es llevar a cabo un registro de las actividades de tratamiento efectuadas bajo su responsabilidad –art. 30 RGPDUE-, que sustituye a la notificación de los tratamientos. Este registro de actividades de tratamiento debe contener, los datos de contacto del responsable –y en su caso de su representante y del delegado de protección de datos-, los fines del tratamiento, una descripción de las categorías de interesados y de las categorías de datos personales, los destinatarios a quienes se comunicarán los datos personales, las eventuales transferencias de datos a terceros países, los plazos previstos para la supresión de las diferentes categorías de datos y, «cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el art. 32.1 [seguridad del tratamiento]» –art. 30.1.g) RGPDUE-. Idéntica obligación tiene el encargado del tratamiento y el representante del encargado que llevará un registro donde consten, «cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad» –art. 30.2.d) RGPDUE-. Este registro del responsable y del encargado está a disposición de la autoridad de control que lo solicite –art. 30.4-, lo que facilita la supervisión de que las medidas de seguridad técnicas y organizativas son las apropiadas. En todo caso, hay que recordar que la notificación de los ficheros que antes tenía que hacer el responsable también le obligaba a indicar «las medidas de seguridad, con indicación del nivel básico, medio y alto exigible» –art. 20.2.h) LOPD relativo a las disposiciones de carácter general de creación, modificación o supresión de ficheros de las Administraciones Públicas-.

Asimismo hay que destacar la importancia de la seguridad en la evaluación de impacto relativa a la protección de datos –art. 35-, que es una nueva obligación del responsable del tratamiento establecida en el RGPDUE que éste debe realizar antes del tratamiento cuando sea probable que un tipo de tratamiento, especialmente si utiliza la nuevas tecnologías, por su naturaleza, alcance, contexto o fines, pueda suponer un alto riesgo para los derechos y libertades de las personales, como es el caso de la evaluación sistemática y exhaustiva de aspectos personales de las personas físicas a través de un tratamiento automatizado –la elaboración de perfiles- y sobre cuya base se tomen decisiones con efectos jurídicos para las personas físicas, los tratamientos a gran escala de categorías especiales de datos o de datos relativos a condenas e infracciones penales o la observación sistemática a gran escala de zonas de acceso público. La evaluación de impacto debe incluir, además de la descripción sistemática de las operaciones de tratamiento y de los fines, la evaluación de la necesidad y proporcionalidad del tratamiento con respecto a la finalidad y la evaluación de los riesgos para los derechos y libertades de los interesados, «las medidas previstas para afrontar los riesgos, incluidas *garantías, medidas de seguridad* y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas» –art. 35.7.d) RGPDUE-. De hecho, se establece que el responsable del tratamiento, cuando proceda, podrá recabar la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, pero ello «sin perjuicio de la protección de intereses públicos o comerciales o de la *seguridad* de las operaciones de tratamiento» –art. 35.9 RGPDUE-.

Igualmente, la seguridad de los tratamientos es un elemento importante a la hora de determinar la necesidad de efectuar una consulta previa a la autoridad de control. El RGPDUE establece que «el responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos […] muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo» –art. 36.1-. El Considerando 94 del RGPDUE obliga a consultar a la autoridad de control «si una evaluación de impacto relativa a la protección de datos muestra que, *en ausencia de garantías, medidas de seguridad y mecanismos destinados a mitigar los riesgos*, el tratamiento entrañaría un alto riesgo para los derechos y libertades de las personas físicas, y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación» (36). En esta consulta a la autoridad de control, el responsable le facilitará, entre otras cuestiones, la información de las «medidas y garantías establecidas para proteger los derechos y libertades de los interesados» –art. 36.3.c)-, cobrando una especial importancia, a nuestro juicio, las medidas organizativas y técnicas propuestas por el responsable para garantizar la seguridad del tratamiento. Lógicamente, como parte del proceso de consulta se puede presentar a la autoridad de control el resultado de la evaluación de impacto relativa a la protección de datos, lo que incluye las medidas previstas para mitigar los riesgos para los derechos y libertades de las personas físicas –Considerando 94-. Así, la autoridad de control deberá asesorar por escrito al responsable y, en su caso, al encargado del tratamiento y podrá ejercer alguno de los poderes descritos en el art. 58 RGPDUE –art. 36.2-, incluso el poder de prohibir operaciones de tratamiento.

Asimismo, la seguridad de los tratamientos debe estar presente en los Códigos de Conducta. El RGPDUE incluye dentro del Capítulo IV dedicado al responsable y al encargado del tratamiento, una regulación de los Códigos de Conducta –art. 40-. El RGPDUE impulsa que los Estados miembros, las autoridades de control, el Comité y la Comisión promuevan la elaboración de códigos de conducta para contribuir a la aplicación del RGPDUE, teniendo en cuenta las características específicas de los distintos sectores de tratamiento. Estos códigos de conducta son elaborados por asociaciones y organismos representativos de categorías de responsable y encargados de tratamiento y tienen por objeto especificar la aplicación del RGPDUE en distintos aspectos, entre los que están también la seudonimización de datos personales, las medidas para garantizar la seguridad de los tratamientos y la notificación de violaciones de la seguridad de los datos

personales a las autoridades de control y la comunicación de dichas violaciones a los interesados –art. 40.2.d), h) e i)- (37).

La regulación de las transferencias de datos personales a terceros países u organizaciones internacionales basadas en una decisión de adecuación –art. 45 RGPDUE- también tiene presente la importancia de la seguridad de los tratamientos. Así, la Comisión puede decidir que un tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o una organización internacional tienen un nivel adecuado de protección de datos personales que permita una transferencia internacional sin necesidad de ninguna autorización específica teniendo en cuenta distintos elementos, entre los que se encuentran «las normas de protección de datos, las normas profesionales y las medidas de seguridad» –art. 45.2.a)- (38). También las normas corporativas vinculantes que facilitan las transferencias internacionales de datos deben cumplir unos requisitos mínimos entre los que se encuentra la obligación de especificar «la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, *las medidas encaminadas a garantizar la seguridad de los datos* y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes» –art. 47.2.d)- RGPDUE-.

El RGPDUE atribuye a la autoridad de control un conjunto de poderes, recogidos en el art. 58 para poder garantizar el cumplimiento de la normativa de protección de datos y las obligaciones de los responsables y de los encargados de tratamiento, también aquellas relativas a la seguridad de los datos personales recogidas en la Sección 2ª del Capítulo IV, como son la seguridad del tratamiento –art. 32-, la notificación de una violación de la seguridad de los datos personales a la autoridad de control –art. 33- y la comunicación de una violación de la seguridad de los datos personales al interesado –art. 34-. Así, el RGPDUE atribuye a la autoridad de control unos poderes correctivos como sancionar a todo responsable o encargado del tratamiento con una advertencia «cuando las operaciones de tratamiento previstas puedan infringir» lo dispuesto en el Reglamento –art. 58.2.a)-; sancionar a todo responsable o encargado del tratamiento con apercibimiento «cuando las operaciones de tratamiento hayan infringido» lo dispuesto en el Reglamento –art. 58.2.b)-; ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado –art. 58.2.d)-; ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales –art. 58.2.e)-; e incluso «imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular» –art. 58.2.i)-.

El RGPDUE considera como infracciones las violaciones a las obligaciones del responsable y del encargado en el ámbito de la seguridad de los datos personales, que se recogen en la Sección 2ª del Capítulo IV. Pues bien, las infracciones a la normativa de protección de datos se sancionarán con multas administrativas de 10 millones de euros como máximo o, tratándose de una empresa, con una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía -art. 83.4.a)-. El RGPDUE regula unas condiciones generales para la imposición de multas administrativas, señalando que «cada autoridad de control garantizará que la imposición de las multas administrativas […] sean en cada caso individual efectivas, proporcionadas y disuasorias» –art. 83.1-. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j) –art. 83.2-. De hecho, el art. 58.2.i) señala que la imposición de una multa administrativa con arreglo al artículo 83 se hará «además o en lugar» de otras medidas señaladas en ese artículo, según las circunstancias de cada caso particular. Estas otras medidas son, como acabamos de mencionar, los poderes correctivos de la autoridad de control. Además, al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta: la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido; la intencionalidad o negligencia en la infracción; cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados; el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las *medidas técnicas u organizativas que hayan aplicado* en virtud de los artículos 25 y 32 del RGPDUE; toda infracción anterior cometida por el responsable o el encargado del tratamiento; el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción; las categorías de los datos de carácter personal afectados por la infracción; la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida; cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas; la adhesión a códigos de conducta o a mecanismos de certificación; cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción –art. 83.2-.

LA SEGURIDAD EN EL PROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES. EL DERECHO A LA SEGURIDAD DIGITAL Y LA CONCRECIÓN DEL PRINCIPIO DE SEGURIDAD

El RGPDUE, a pesar de ser una norma obligatoria en todos sus elementos y directamente aplicable, ha dejado margen de maniobra a los Estados miembros, a los que llama expresamente a concretar éste a través de la Ley. Además, el RGPDUE desplaza la normativa interna que esté en contradicción por lo que le corresponde a la Ley nacional, por razones de seguridad jurídica, derogar los preceptos de la LOPD que sean incompatibles con el RGPDUE. Por estos dos motivos, el Consejo de Ministros aprobó el 10 noviembre de 2017 el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal –PLOPD-. Este PLOPD fue remitido al Congreso de los Diputados, siendo objeto de importantes enmiendas. En especial hay que mencionar las enmiendas del Grupo Parlamentario Socialista relativas a los llamados derechos digitales. El retraso en la tramitación parlamentaria y en la consiguiente aprobación de la LOPD hizo que comenzara el inicio de la aplicación del RGPDUE el 25 de mayo de 2018, sin haberse aprobado antes la nueva LOPD. Por esta razón, el Consejo de Ministros aprobó el 27 de julio de 2018 un Real Decreto Ley con medidas urgentes para adaptar el Derecho español al Reglamento General de Protección de Datos. Este Real Decreto Ley señala que éste permanecerá vigente hasta la entrada en vigor de la nueva legislación orgánica de protección de datos, cuyo objeto será adaptar el ordenamiento jurídico español al Reglamento General de Protección de Datos -Disposición Final Única-.

Parece razonable afirmar que el PLOPD será aprobado, aunque no ha sido fácil establecer hasta ahora un calendario concreto. Por una parte, el procedimiento legislativo en el Congreso no está sujeto a plazos por lo que siempre podía haberse continuado ampliando el trámite de enmiendas. Por otra, siempre ha existido el riesgo de una disolución anticipada de las cámaras, lo que supone la caducidad de los trabajos parlamentarios. A finales de septiembre de 2018 se elaboró el Informe definitivo de la Ponencia sobre el Proyecto de Ley Orgánica, que pasó a denominarse de Protección de Datos Personales y Garantía de los Derechos Digitales –PLOPDyGDD-. El dictamen de la Comisión fue el 9 de octubre y después pasó al Pleno del Congreso. El 18 de octubre se aprobó por unanimidad en el Pleno del Congreso de los Diputados el Dictamen de la Comisión sobre el Proyecto de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (39). El 23 de octubre de 2018 el texto aprobado por el Pleno del Congreso tuvo entrada en el Senado y se remitió a la Comisión de Justicia, abriéndose el plazo para presentar enmiendas y propuestas de veto hasta el 5 de noviembre (40). La aprobación por unanimidad del texto en el Congreso anticipa una tramitación rápida en el Senado sin modificaciones, por lo que es prudente afirmar que la LOPDyGDD será finalmente aprobada aunque más tarde de lo inicialmente previsto.

El derecho a la seguridad digital en el PLOPDyGDD

Una de las principales novedades que aparece en el PLOPDyGDD, que lo diferencia no sólo de la actual LOPD y del Proyecto de LOPD inicialmente aprobado por el Gobierno en noviembre de 2017 sino también del RGPDUE, es la inclusión en el Título X de la «Garantía de los derechos digitales», que proviene de las enmiendas del Grupo Parlamentario Socialista al PLOPD, que, como acabamos de señalar, se incorporaron finalmente al Informe definitivo de la Ponencia acordado en la Comisión de Justicia del Congreso de los Diputados. La Exposición de Motivos del PLOPDyGDD recoge que «finalmente, el Título X de esta Ley acomete la tarea de reconocer y garantizar un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución. En particular, son objeto de regulación los derechos y libertades predicables al entorno de Internet como la neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital así como los derechos al olvido, a la portabilidad y al testamento digital. Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en Internet. Finalmente, resulta destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales». La Exposición de Motivos no contribuye mucho a acercarnos o a clasificar los preceptos incluidos en el Título X. No nos corresponde entrar a valorar aquí en profundidad la oportunidad y la técnica normativa empleada en el Título X. En todo caso, el Título X, titulado «*Garantía* de los derechos digitales», regula materias distintas:

En primer lugar, se encontrarían dentro de este Título X unos derechos y libertades de carácter general en relación con Internet, donde podríamos establecer dos categorías. La primera categoría sería la relativa a que los derechos y libertades de la Constitución son predicables y vigentes en Internet; es decir, que Internet no es un territorio de excepción para el ejercicio de los derechos. En esta categoría estarían: los «derechos de la Era digital», donde se establece que «los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet», obligando a los prestadores de servicios de la sociedad de la información y a los proveedores de servicios de Internet a contribuir a garantizar su aplicación» –art. 79-. También dentro de esta categoría estaría la «protección de los menores en Internet», que obliga a los padres a procurar que los menores hagan un uso equilibrado de los dispositivos digitales para garantizar el desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales y obliga al Ministerio Fiscal a intervenir cuando la difusión de información personal de menores en las redes sociales suponga una intromisión en sus derechos –art. 84-. La segunda categoría haría referencia a que el acceso a internet es en sí mismo un derecho. Dentro de esta categoría

estaría el reconocimiento de que los usuarios tienen un «derecho a la neutralidad de Internet», por lo que «los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos» –art. 80-, y, sobre todo, el «derecho de acceso universal a Internet», por el que «todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica» –art. 81.1- (41). Finalmente se reconoce el derecho a la educación digital –art. 83-. En virtud del reconocimiento de este derecho, «el sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales». En relación con la seguridad de la información, es importante subrayar la previsión de que «los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y *seguridad de los medios digitales* y en la garantía de los derechos fundamentales en Internet» (42).

En segundo lugar, el Título X del PLOPDyGDD recogería una concreción de los derechos de protección de datos regulados en el RGPDUE para el ámbito de Internet. Así, se regula el «derecho de rectificación en Internet», que reconoce que «todos tienen derecho a la libertad de expresión en Internet» pero obliga a los responsables de redes sociales y servicios de la sociedad de la información a adoptar protocolos «para garantizar el ejercicio del derecho de rectificación, en particular en relación con los contenidos que atenten contra el derecho al honor, la intimidad personal y familiar y personal en Internet y el derecho a comunicar o recibir libremente información veraz» –art. 85-. También se incluye el «derecho a la actualización de informaciones en medios de comunicación digitales», por el que «toda persona tiene derecho a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual», en especial cuando «las informaciones originales se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado por decisiones judiciales posteriores» –art. 86-. Lógicamente, estos derechos de rectificación y de actualización de informaciones en medios de comunicación digitales también se encuentran vinculados al tradicional derecho de rectificación regulado en la Ley Orgánica 2/1984, aunque este se configure más como una vía de protección del honor que de la veracidad de la información. Asimismo se regula el «derecho al olvido en búsquedas de Internet» que establece que «toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo» –art. 93-. También se encontraría en este ámbito el «derecho al olvido en servicios de redes sociales y servicios equivalentes», por el que «toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado él mismo o terceras personas para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes» –art. 94-. También hay que mencionar el «derecho de portabilidad en servicios de redes sociales y servicios equivalentes» por el que «los usuarios de servicios de redes sociales y servicios de la sociedad de la información equivalentes tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible» –art. 95-. También dentro de esta concreción de los derechos de protección de datos en el ámbito de Internet se encontraría la regulación de la «protección de datos de los menores en Internet», por el que los centros educativos garantizarán la protección del interés superior del menor y su derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información –art. 92-. Finalmente, hay que mencionar en este ámbito el «derecho al testamento digital», a través del cual se regula los accesos y las decisiones sobre contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas –art. 96-.

En tercer lugar, el Título X del PLOPDyGDD regula un conjunto de derechos a la intimidad y a la protección de datos personales relativos a los trabajadores. Dentro de este grupo estaría el derecho a la intimidad en el uso de dispositivos digitales puestos a su disposición por el empleador –art. 87-; el «derecho a la desconexión digital en el ámbito laboral», que permite garantizar, fuera del tiempo de trabajo, el respeto de su tiempo de descanso y de su intimidad personal y familiar –art. 88-; el «derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo», que obliga a los empleadores a informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores de esta medida –art. 89-; el «derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral», que obliga a los empleadores, con carácter previo, a informar de forma expresa, clara e inequívoca acerca de la existencia y características de estos dispositivos; y los «derechos digitales en la negociación colectiva», que permite a los convenios colectivos establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral –art. 90-.

Es en este contexto de inflación de los derechos digitales en el que debe comprenderse la regulación que

hace el PLOPDyGDD de la seguridad del tratamiento de datos personales. Así, en línea con el tener general de un proyecto de Ley, que se denomina de «Garantía de los derechos digitales» y que establece en el Título X nuevos derechos digitales, hay que entender el reconocimiento que hace el art. 82 de «derecho a la seguridad digital». Así, se establece que «los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos». Llama la atención que el principio de seguridad de los tratamientos recogido en el art. 9 LOPD y en el RGPDUE se convierta en un derecho a la seguridad únicamente en relación con las comunicaciones que los usuarios transmitan y reciban a través de Internet y no sea un derecho a la seguridad en los tratamientos de datos personales en general. Hay que recordar que también la Directiva 95/46/CE hizo especial hincapié en la seguridad en la transmisión de datos dentro de una red –art. 17.1-. Por último, hay que señalar que el PLOPDyGDD también establece que «los proveedores de servicios de Internet informarán a los usuarios de sus derechos», sin precisar bien si informarán de todos sus derechos de protección de datos personales o de su derecho a la seguridad digital –art. 82-.

Hay que recordar que otros textos legislativos ya habían puesto de manifiesto que la seguridad de la información no es sólo un principio de protección de datos que debe respetar el responsable del tratamiento, sino que también es un derecho de las personas. La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, reconoció como un derecho de los ciudadanos «la garantía de la seguridad y la confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas» -art. 6.2.i)-, hoy ya derogada por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que también reconoce entre los derechos de las personas en sus relaciones con las Administraciones Públicas «la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas» –art. 13.h)-. Igualmente, la Ley 41/2002, de 14 de noviembre básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, señala que el paciente «tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad» -art. 19-.

El principio de seguridad de los tratamientos en el PLOPDyGDD

El PLOPDyGDD no desarrolla el principio de seguridad y confidencialidad regulado en el art. 5.1.f) del RGPDUE ni tampoco la seguridad de los datos personales como obligación del responsable y del encargado recogida en los arts. 32-34 del RGPDUE. Esto es así porque, como hemos señalado antes, el RGPDUE no permite ni a la Comisión ni a los Estados miembros aprobar un listado de medidas de seguridad sino que ésta es una cuestión que le corresponde ahora al responsable del tratamiento que debe aplicar en cada caso las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento y los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas –art. 32.1-.

Esto no impide que el legislador pueda establecer exigencias en materia de seguridad de la información personal destinadas a los poderes públicos. En esta dirección hay que mencionar específicamente la Disposición adicional primera del PLOPDyGDD que recoge «Medidas de seguridad en el ámbito del sector público». Hay que recordar que al aprobarse el RGPDUE, inicialmente se pensaba que el Esquema Nacional de Seguridad podría servir de guion para las Administraciones públicas, pero su contenido debería conciliarse plenamente con el nuevo Reglamento Europeo. Pues bien, la Disposición adicional primera del PLOPDyGDD en su apartado 1 establece expresamente que «el Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales, para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679». Además, su apartado 2 señala que determinadas categorías de responsables o encargados del tratamiento «deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad». Estas categorías de responsables o encargados son las recogidas en el art. 77.1 PLOPDyGDD: los órganos constitucionales o con relevancia constitucional y las instituciones de las Comunidades Autónomas análogas a los mismos, los órganos jurisdiccionales, la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las entidades que integran la Administración Local, los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas, las autoridades administrativas independientes, el Banco de España, las Corporaciones de Derecho Público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público, las fundaciones del sector público, las Universidades Públicas, los consorcios y los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales (43).

El PLOPDyGDD no se limita a obligar aplicar el Esquema Nacional de Seguridad a los órganos constitucionales y estatutarios, al Poder Judicial, al Poder Ejecutivo –a la

Administración General e Institucional de los diferentes niveles territoriales, a la Administración Corporativa, a las Administraciones Independientes- y al Poder Legislativo, sino que pretende que este Esquema Nacional de Seguridad sea también aplicable a las empresas y fundaciones vinculadas a las Administraciones Públicas sujetas al Derecho privado, e incluso a empresas privadas que presten servicio para las Administraciones Públicas. Así, anima a estas categorías de responsables o encargados a «impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado. En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad» -Disposición adicional primera. Apartado 2-.

El RGPDUE impide a los Estados miembros desarrollar reglamentariamente el principio de seguridad, aprobando medidas de seguridad, si bien es posible, como antes hemos indicado, que las autoridades de control elaboren y den publicidad a protocolos, parámetros o indicadores de seguridad. El PLOPDyGDD quiere facilitar que los responsables de tratamiento, especialmente aquellos que puedan disponer de menos medios, puedan tener unas orientaciones y guías sobre el cumplimiento de las Disposiciones aplicables a tratamientos concretos –Título IV-, también en lo relativo a la seguridad de los tratamientos. Por ello, la Disposición adicional decimoctava, denominada «Criterios de seguridad» establece que «la Agencia Española de Protección de Datos desarrollará, con la colaboración, cuando sea precisa, de todos los actores implicados, las herramientas, guías, directrices y orientaciones que resulten precisas para dotar a los profesionales, microempresas y pequeñas y medianas empresas de pautas adecuadas para el cumplimiento de las obligaciones de responsabilidad activa establecidas en el Título IV del RGPDUE» [se trata de un error ya que se refiere al Capítulo IV del RGPDUE, que está dedicado a las obligaciones de responsable y del encargado del tratamiento, entre las que se encuentra de manera específica la seguridad del tratamiento] y el Título V de esta ley orgánica», dedicado a las obligaciones del responsable y del encargado del tratamiento. Lógicamente, esto debe hacerse en coordinación con el Comité Europeo de Protección de Datos a través de los mecanismos establecidos en el RGPDUE.

El RGPDUE, al regular la licitud de tratamiento –art. 6-, deja a los Estados un cierto margen de maniobra, permitiéndoles establecer disposiciones específicas en materia de seguridad en dos supuestos: en el tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento –art. 6.1.c)- y en el tratamiento para el cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos conferidos al responsable del tratamiento –art. 6.1.f)-. Así, el art. 6.2 establece expresamente que «los Estados miembros «podrán *mantener o introducir disposiciones más específicas* a fin de adaptar la aplicación de las normas del presente Reglamento» con respecto al tratamiento en cumplimiento de una obligación legal aplicable al responsable del tratamiento o para el cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos conferidos al responsable del tratamiento, «*fijando de manera más precisa requisitos específicos de tratamiento y otras medidas* que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento». En la misma dirección, el art. 6.3 señala que la base jurídica del tratamiento tanto en el supuesto del cumplimiento de una obligación legal aplicable al responsable del tratamiento como en el supuesto del cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos conferidos al responsable del tratamiento «deberá ser establecida por el Derecho de la Unión o el Derecho de los Estados miembros que se aplique al responsable del tratamiento». Esta base jurídica, por tanto, también el Derecho de los Estados miembros deberá determinar la finalidad del tratamiento y «podrá contener disposiciones específicas para adaptar la aplicación de normas del […] Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido».

Este margen de maniobra a los Estados que recoge el RGPDUE es aprovechado por el PLOPDyGDD. Así, la Exposición de Motivos –apdo. V- señala que «se regulan asimismo las posibles habilitaciones legales para el tratamiento fundadas en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una ley, *que podrá determinar las condiciones generales del tratamiento* y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal». […] Se podrán igualmente *imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras, cuando ello derive del ejercicio de potestades públicas* o del cumplimiento de una obligación legal y sólo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el reglamento europeo, cuando derive de una competencia atribuida por la ley». Por ello, el art. 8.1 PLOPDyGDD -*Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos-,* después de afirmar que el tratamiento

de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del RGPDUE cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, establece que ésta Ley «podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679» (44).

El RGPDUE también reconoce abiertamente un cierto margen de maniobra a los Estados en el ámbito de la seguridad en relación con el tratamiento de categorías especiales de datos personales, al afirmar que los «Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud» –art. 9.4-. De hecho, se prevé en los tratamientos por razones de un interés público esencial que el Derecho de los Estados miembros pueda establecer «medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado –art. 9.2.g)-. Igualmente en los tratamientos en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, se prevé que el Derecho de los Estados miembros pueda establecer «medidas adecuadas y específicas para proteger los derechos y libertades del interesado» –art. 9.2.i)-; también se establece que en el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, el Derecho de los Estados miembros «podrá establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado» -art. 9.2.j). Aprovechando este margen de maniobra, el art. 9.2 PLOPDyGDD establece que los tratamientos de categorías especiales de datos por razones de interés público esencial –g)-, para fines de medicina preventiva o laboral, diagnóstico médico, prestación de asistencia o gestión de los sistemas y servicios de asistencia sanitaria y social –h)- y en el ámbito de la salud pública o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios –i)- deberán estar amparados en una norma con rango de ley, «*que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad*».

El PLOPDyGDD también concreta a través del Título IX dedicado al «Régimen sancionador» la imposición de multas administrativas recogida en el art. 83 RGPDUE en el ámbito de la seguridad. En relación con el régimen de infracciones, hay que señalar en términos generales que la violación de la seguridad de los tratamientos sigue siendo considerada infracción grave en el art. 73 PLOPDyGDD, existiendo una continuidad entre este precepto y el art. 44.3.h) de la LOPD que calificaba como infracción grave «mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen». Así, las diferentes violaciones a la seguridad de los tratamientos, que se recogían en el art. 83.4 del RGPDUE en relación con las vulneraciones de las obligaciones del responsable y del encargado previstas en los arts. 32-34 son calificadas infracciones graves por el art. 73 del PLOPDyGDD y prescribirán a los dos años. El PLOPDyGDD no se limita a señalar que son infracciones graves las que «supongan una vulneración sustancial de los artículos mencionados» en el art. 83, sino que describe de manera más precisa las infracciones, también aquellas relativas a la seguridad de los tratamientos. Así, en relación con la obligación de seguridad del tratamiento prevista en el art. 32 del RGPDUE, se considera infracción grave: «la falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 RGPDUE» –art. 73.f) PLOPDyGDD-; el «quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del RGPDUE» –art. 73.g) PLOPDyGDD-. Igualmente, en relación con la obligación de notificación de una violación de la seguridad de los datos personales a la autoridad de control prevista en el art. 33 del RGPDUE, se considera infracción grave «el incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 RGPDUE» –art. 73.r PLOPDyGDD-. También se considera una infracción grave «el incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento» -art. 73.q PLOPDyGDD-, una obligación que se encontraba escondida en el art. 33.2 del RGPDUE. Finalmente, en relación con la obligación de comunicación de una violación de la seguridad de los datos personales al interesado recogida en el art. 34 del RGPDUE, se considera infracción grave «el incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 34 del RGPDUE, únicamente si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación» –art. 73.s PLOPDyGDD- (45).

Otra manifestación de la importancia que el PLOPDyGDD da a la seguridad de los tratamientos es la previsión de que el Consejo Consultivo de la Agencia Española de Protección de Datos cuente con un «representante de los profesionales de la seguridad de la información, propuesto por la asociación de ámbito estatal con mayor número de asociados» –art. 49.1.m)-, que es distinto del «representante de los profesionales de la protección de datos y de la privaci-

dad, propuesto por la asociación de ámbito estatal con mayor número de asociados» –art. 49.1.i)-. Esta representación parece razonable dado el incremento del número de miembros del Consejo Consultivo de la Agencia Española de Protección de Datos, que pasa de estar compuesto por ocho miembros –art. 38 LOPD- a disponer ahora de dieciséis miembros –art. 49.1 PLOPDyGDD-, a los que hay que sumar, en ambos casos, a los representantes de cada Comunidad Autónoma que haya creado una Agencia de Protección de Datos.

El PLOPDyGDD regula en la Disposición adicional novena «Tratamiento de datos personales en relación con la notificación de incidentes de seguridad», considerándolo un supuesto de licitud del tratamiento. Así, se establece que «cuando, de conformidad con lo dispuesto en la legislación nacional que resulte de aplicación, deban notificarse incidentes de seguridad, las autoridades públicas competentes, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad, podrán tratar los datos personales contenidos en tales notificaciones, exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta ante incidentes y adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado».

Hemos señalado antes que el RGPDUE considera la seudonimización una importante medida de seguridad en el tratamiento –art. 32.1.a)-. Es importante subrayar el recurso a la seudonimizacion que se encuentra en el PLOPDyGDD, especialmente en la Disposición adicional decimoséptima del PLOPDyGDD «Tratamientos de datos de salud», donde se afirma expresamente que «se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica» -2.d)-. Ahora bien, este uso está sometido a unas condiciones concretas: 1º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación. 2º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando: i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación. ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados». No obstante, «podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria». De hecho, cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo 89.2 del Reglamento (UE) 2016/679, podrán excepcionarse los derechos de acceso, rectificación, limitación del tratamiento y oposición de los afectados cuando estos derechos «se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados –apartado 2.e)-. En todo caso, «el uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial» –apartado 2.g)-.

NOTAS

[1] Sobre el RGPDUE, cfr. J. L. Piñar Mañas (Dir.), *Reglamento general de protección de datos*, Reus, Madrid, 2016; J. López Calvo (Coord.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, Wolters Kluwer, Madrid, 2018; E. Delgado Carravilla y J. Puyol Montero, *La implantación del nuevo Reglamento General de Protección de Datos de la Unión Europea*, Tirant lo Blanch, Valencia, 2018; J. Puyol Montero, *Guía divulgativa del Reglamento General de Protección de Datos de la Unión Europea*, Tirant lo Blanch, Valencia, 2018; *Protección de datos. Aplicación del RGPD*, Francis Lefebvre, Madrid, 2018. Cfr. A. Rallo Lombarte: «*Hacia un sistema europeo de protección de datos:* las claves de la reforma», RDP, núm. 85, 2012, pp. 15-56; A. Rallo Lombarte y R. García Mahamut (ed.), Hacia un derecho europeo de protección de datos, Tirant lo Blanch, Valencia, 2015; A. Troncoso Reigada, «Hacia un nuevo marco jurídico europeo de protección de datos personales», *REDE*, núm. 43, 2012, pp. 25-184.

[2] Hederero Higueras considera que este artículo sufrió una evolución sustancial en el curso de la negociación de la Directiva en relación con la Propuesta de la Comisión de 1990, que seguía de cerca el art. 7 del Convenio 108 del Consejo de Europa, haciendo un especial hincapié en los aspectos de compatibilidad e interoperabilidad de las redes. Lo más relevante es que la Propuesta de Directiva de la Comisión exigía que el responsable del fichero observara las normas técnicas cuya elaboración el art. 29 atribuía a la Comisión. Finalmente, el texto aprobado limitaba la potestad reglamentaria de la Comisión a los problemas de transferencia de datos a terceros países. Cfr. M. Hederero Higueras, *La Directiva Comunitaria de Protección de los Datos de Carácter Personal*, Aranzadi, Pamplona, págs. 162-163.

[3] También analiza Hederero Higueras la evolución en la negociación de los criterios para determinar las medidas de seguridad. La Propuesta modificada de la Comisión de 1992, sobre la base de las enmiendas del Parlamento Europeo, había suprimido el criterio del coste de aplicación que se encontraba en la Propuesta de la Comisión de 1990, junto con progresos técnicos y la naturaleza de los datos. Alemania, Dinamarca, Irlanda y Reino Unido propusieron que se recuperara de nuevo el criterio del coste. De esta forma, quedan restablecidos en el texto definitivo los que para este autor son los tres parámetros del nivel de seguridad: los conocimien-

tos técnicos, el coste de su aplicación y la naturaleza de los datos –*ibidem*-.

[4] La cuestión prejudicial planteaba si un Estado miembro que no haya aprobado medidas de seguridad podía sancionar a una empresa que, como responsable del tratamiento, había adoptado un sistema de acceso restringido a tales datos que no permita el acceso inmediato de la autoridad nacional competente para la supervisión de las condiciones de trabajo. Worten alegaba, además, que la obligación de tener accesible el registro del tiempo de trabajo para permitir su consulta inmediata por las autoridades laborales prevista en la legislación portuguesa, resultaba incompatible en la práctica con la obligación de establecer un sistema de protección adecuado de los datos personales contenidos en dicho registro pues equivalía a admitir que cualquier empleado de la empresa pudiera acceder a tales datos, en contra de lo establecido en la Directiva 95/46/CE. Como acertadamente señala el TJUE –apdo. 28-, la obligación de un empleador, como responsable del tratamiento de datos personales, de dar acceso inmediato al registro del tiempo de trabajo a la autoridad nacional competente para la supervisión de las condiciones de trabajo no implicaba en absoluto que los datos personales que figuraran en dicho registro debían necesariamente, por este simple motivo, hacerse accesibles a quienes no estuvieran autorizados para ello porque, como establece el art. 17.1 de la Directiva 95/46/CE, corresponde a los responsables del tratamiento de datos personales adoptar las medidas técnicas y de organización necesarias para garantizar que sólo las personas debidamente autorizadas para acceder a los datos personales puedan responder a una solicitud de acceso procedente de un tercero. Además, este acceso de la autoridad administrativa portuguesa es un tratamiento lícito porque «es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento» y «es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos».

[5] Holanda también había aprobado unas medidas de seguridad que no eran vinculantes para los responsables de ficheros aunque eran usadas como un importante elemento de autorregulación. Cfr. *Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE)*, Bruselas, 15.5.2003 COM (2003) 265 —http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm—; *Analysis and impact study on the implementation of Directive EC 95/46 in Member States*, http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm

[6] Incluso la LOPD, en la regulación de las disposiciones de carácter general de creación o modificación de ficheros, señalaba que éstas debían indicar «las medidas de seguridad con indicación del nivel básico, medio o alto exigible» –art. 20.2.h)-.

[7] Esto fue lo que ocurrió en 2008 con la Resolución de infracción que la APDCM dictó a la Consejería de Sanidad de la Comunidad de Madrid por vulneración del principio de seguridad, en relación con la filtración de las historias clínicas del Hospital Severo Ochoa de Leganés a medios de comunicación y a asociaciones de pacientes, lo que se fundamentó en el incumplimiento de dos concretas medidas de seguridad previstas en la normativa: que no estaba en funcionamiento el registro de accesos, que facilita la trazabilidad de las personas que accedían a las historias clínicas, y la omisión de la auditoría bienal.

[8] La LOPD suprimió la referencia al coste de aplicación en línea con las enmiendas del Parlamento Europeo y con la Propuesta de la Comisión de 1992.

[9] El Tribunal Constitucional se ha pronunciado en una única ocasión sobre la importancia de la seguridad de los datos como garantía de la confidencialidad de la información: la Sentencia 17/2013, de 31 de enero, que resolvió el recurso de inconstitucionalidad contra de la Ley Orgánica 14/2003, de 20 de noviembre, que modificaba la LBRL en relación con el acceso a los datos del padrón por parte de la Policía, fijando que «para la exclusiva finalidad del ejercicio de las competencias establecidas en la Ley Orgánica de Derechos y Libertades de los Extranjeros en España y su Integración Social, sobre control y permanencia de extranjeros en España, la Dirección General de la Policía accederá a los datos de inscripción padronal de los extranjeros existentes en los Padrones Municipales, preferentemente por vía telemática. A fin de asegurar el estricto cumplimiento de la legislación de protección de datos de carácter personal, *los accesos se realizarán con las máximas medidas de seguridad*. A estos efectos, quedará constancia en la Dirección General de la Policía de cada acceso, la identificación de usuario, fecha y hora en que se realizó, así como de los datos consultados». El recurso entendía que esta reforma legal vulneraba el art. 18.4 CE en cuanto que la misma permitiría la utilización de los datos contenidos en el padrón para finalidades distintas de aquella para las que se recogieron, habilitando la posibilidad de que se produzcan, además, transferencias masivas de datos

La Sentencia señala que esta previsión legal «prevé una posibilidad diferenciada de acceso al padrón, que viene delimitada por la naturaleza del cesionario (la Dirección General de la Policía), la finalidad que justifica el acceso (el ejercicio por la misma de las competencias específicamente atribuidas por la legislación sobre extranjería) y el alcance de los datos que podrán ser objeto de cesión (exclusivamente los referidos a la inscripción de los extranjeros existentes en los padrones municipales), adoptando como cautela que los accesos se realicen *con las máximas medidas de seguridad*, para lo cual quedará constancia de cada acceso, la identificación del usuario, fecha y hora en que se realizó así como de los datos consultados». De esta forma, este acceso «ha de ser entendido de forma acorde con las exigencias de proporcionalidad que nuestra doctrina exige en la limitación de un derecho fundamental como es el aquí concernido, relativo la protección de datos de carácter personal. Eso significa que la cesión de datos que el acceso regulado por el precepto supone ha de venir rodeado de una serie de garantías específicas, garantías que, cumplimentadas por el órgano administrativo al que el precepto hace

referencia, son, evidentemente, susceptibles de control. Entre ellas se encuentra *la necesidad de motivar y justificar expresamente tanto la concreta atribución de la condición de usuario* para el acceso telemático a los datos del padrón que el precepto prevé, como los concretos accesos de que se trate, evitando –en cuanto que la exigible motivación de tales decisiones facilita su correspondiente control mediante los mecanismos previstos en el ordenamiento jurídico, en especial, a través del control jurisdiccional contencioso-administrativo– que se produzca tanto un uso torticero de dicha facultad como accesos indiscriminados o masivos. Límites al contenido del acceso que también resultan de determinadas previsiones de la legalidad ordinaria [art. 22.2 LOPD]. Resulta de ello que el acceso solamente será posible, en las condiciones antes dichas, cuando el concreto dato en cuestión resulte pertinente y necesario en relación con la finalidad que ha justificado el acceso, quedando garantizada la posibilidad de analizar si, en cada caso concreto, el acceso tenía amparo en lo establecido en la ley pues, en caso contrario, no resultará posible su uso. Con tales garantías el acceso regulado en la disposición cuestionada resulta ser proporcionado en relación con la finalidad perseguida, ya que, en tanto que el dato resultante solo puede ser utilizado para la finalidad establecida en el precepto, ha de realizarse de forma puntual por quien se encuentre expresamente habilitado para ello y en relación a datos concretos cuya necesidad ha de ser también justificada de forma expresa y, por tanto, sometida a control, en los términos que acabamos de exponer» –F. J. 9º-.

El voto particular del Magistrado Pérez Tremps –F. J. 3º- centra su discrepancia sobre un aspecto que se considera nuclear del sistema de garantías diseñado por la Constitución en la protección de los derechos y libertades públicas, «la calidad de la ley como exigencia material impuesta al legislador de los derechos fundamentales con el fin de respetar el principio de reserva de ley y el contenido esencial del derecho fundamental concernido». Estas exigencias de la calidad de la ley obligan a ésta no sólo a respetar el principio de proporcionalidad sino a «la necesidad de que se regulen las instituciones o medidas limitativas de derechos fundamentales con un grado de determinación y certeza suficiente para evitar que se genere grave inseguridad o incertidumbre sobre su modo de aplicación efectiva». Así, este voto particular, en relación con la regulación del acceso al padrón de habitantes, considera que «existen profundas indeterminaciones en relación con el sujeto habilitado para el acceso, así como con la forma, objeto y garantías del acceso. Por ejemplo, se habilita de forma general a la Dirección General de la Policía para acceder a los datos, sin que la norma, ni la interpretación conforme, aclaren si el acceso se permite al titular de ese órgano (el Director General de la Policía) o a cualquier órgano o unidad integrados en dicha dirección, aunque la lectura completa de la norma permite deducir que podrá acceder cualquier miembro de la Dirección General de la Policía, en la medida en que se establece en la propia disposición impugnada que «quedará constancia en la Dirección General de la Policía de cada acceso, la identificación de usuario, fecha y hora en que se realizó, así como de los datos consultados». Esto supone un amplio universo de sujetos habilitados, lo que va en detrimento de la proporcionalidad de la medida y del mandato de predeterminación de las medidas limitativas de derechos fundamentales». Por último, «aunque la norma prevé que el acceso se realizará con las «*máximas medidas de seguridad*», éstas no se concretan, más allá de que quedará constancia de cada acceso, de la identidad del accedente, de la fecha y hora del acceso y de los datos consultados. La posición de la mayoría afirma que el acceso, y la motivación que lo inspira, estará sujeta a control mediante los mecanismos previstos en el ordenamiento jurídico, en especial, a través del control jurisdiccional contencioso-administrativo, y entiende que habrá de evitarse que se produzca un uso torticero de la facultad de acceso, así como un acceso indiscriminado o masivo. Todas estas previsiones, no obstante, resultan excesivamente indeterminadas e insuficientes. Por dar sólo un ejemplo, no se contempla que el propio afectado pueda conocer que se ha producido el acceso y, en consecuencia, queda indefenso respecto de una medida limitativa de un derecho fundamental ante la que no puede protegerse plenamente en caso de un eventual acceso indebido en su información padronal».

Con anterioridad a esta Sentencia, habíamos manifestado la necesidad en este caso de dejar registro del acceso, lo que obligaba a implantar en el fichero del padrón municipal medidas de seguridad de nivel alto. Cfr. A. Troncoso Reigada, La protección de datos personales, En busca del equilibrio, Tirant lo Blanch, Valencia, 2010, págs. 1074-1076. La aplicación del principio de proporcionalidad a las interconexiones en la Administración electrónica también ha sido analizado *ibídem* págs. 645-672.

[10] La Exposición de Motivos del Real Decreto 1720/2007, de 21 de diciembre, establece que el Reglamento «trata de ser particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que corresponda adoptar en cada caso» –III-.

[11] También se establecía, además de las medidas de seguridad de nivel básico y medio, una medida de seguridad de nivel alto referida al registro de accesos a los «ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización» -art. 81.4 del Reglamento-.

[12] Los de historias clínicas, investigación sanitaria, historias sociales, atención psicopedagógica en los centros educativos, los ficheros policiales, etc.

[13] Así, señalaba que se podían mantener las medidas de seguridad de nivel básico a los ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual cuando «los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros» -art. 82.5.a)-, lo que se aplicaba al tratamiento del dato del pago de la cuota sindical en el fichero de nóminas.

También establecía que se podían implantarse medidas de seguridad de nivel básico en los «ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos» -art. 82.6-, lo que parecía referirse al tratamiento del dato de salud en el fichero de nóminas —aunque no hacía ninguna exclusión en relación al número de días de baja, que seguía siendo un dato de salud—. También se señalaba que no era necesario aplicar las medidas de seguridad de nivel alto cuando «se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad» -art. 81.5.b)-. En cambio, no se decía nada de la falta de sentido de exigir medidas de seguridad de nivel alto a los ficheros donde se contienen la pertenencia a un grupo político o a una central sindical de un representante —un Diputado, un Concejal, un liberado sindical—, puesto que el tratamiento se refería a datos que el interesado había hecho manifiestamente públicos -art. 8.2.e) de la Directiva 95/46/CE- e, incluso, en muchas ocasiones, se encontraban en fuentes accesibles al público.

Como señalamos en su momento, estas previsiones no eran acertadas porque podía no ser razonable o posible ser mucho más exigente en el establecimiento de medidas de seguridad, pero lo que no debía hacerse a nuestro entender era ir hacia atrás, disminuyendo el nivel de seguridad y reduciendo las medidas ya establecidas. Hay que tener en cuenta que muchas Entidades públicas y privadas ya habían hecho el esfuerzo —también económico—, que resultaba de esta forma baldío, de adecuarse a las exigencias fijadas en el Real Decreto 994/1999, de 11 de junio, por lo que esta decisión respaldaba a aquellas entidades que no habían implantado las medidas de seguridad adecuadas a los ficheros de nóminas, a pesar de que ya estaban en vigor a partir de junio de 2002. Si las medidas de seguridad de nivel alto parecían demasiado exigentes para las pequeñas empresas, hubiera sido mejor establecer una solución adecuada para este tipo de responsable de los ficheros —con las necesarias disposiciones transitorias—, pero no disminuir de manera general las medidas de seguridad que ya estaban en vigor y habían sido implantadas. Esta cuestión la hemos analizado ya en «Introducción», Seguridad y protección de datos personales, Civitas-APDCM, Madrid, 2009, pág. 28.

[14] Esta tendencia hacia la autorregulación ya aparecía claramente en la Propuesta de Reglamento de la Comisión. Cfr. A. Troncoso Reigada, «Hacia un nuevo marco jurídico europeo de la protección de datos personales», REDE, núm. 43, 2012, págs. 48-53.

[15] Este planteamiento lo habíamos adelantado en el apartado «Una aproximación al modelo anglosajón: autorregulación, desregulación, accountability y un estándar más cool de protección de datos. El Reglamento como reflejo del diálogo entre ordenamientos jurídicos» dentro del Capítulo XXVI Autoridades de control independientes, en J. L. Piñar Mañas (Dir.), Reglamento general de protección de datos, cit. págs. 461-471.

[16] Cfr. I. González Ubierna, «Seguridad del tratamiento», en J. López Calvo (Coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos, cit. págs. 453-459; J. Puyol Montero, Guía divulgativa del Reglamento General de Protección de Datos de la Unión Europea, cit. págs. 148-149. E. Delgado Carravilla y J. Puyol Montero, La implantación del nuevo Reglamento General de Protección de Datos de la Unión Europea, cit. págs. 169-223 y 515-536; M. Carpio Cámara, «Seguridad del tratamiento de los datos personales y notificaciones de violaciones de seguridad», en J. L. Piñar Mañas (Dir.), Reglamento general de protección de datos, cit. págs. 335-348.

[17] Hay que recordar que la referencia a la garantía de la confidencialidad se encontraba también en el art. 16 de la Directiva 95/46/CE, aunque no en relación con las medidas de seguridad.

[18] La Propuesta del Reglamento delegaba en la Comisión el poder de adoptar actos no legislativos de alcance general que completen o modifiquen determinados elementos no esenciales del Reglamento (actos cuasi legislativos), de conformidad con el artículo 290 del TFUE, en muchas materias como las condiciones de licitud para tratamientos específicos o la especificación de las medidas de seguridad técnicas y organizativas. El art. 86 de la Propuesta señalaba las condiciones a las que estaban sujetas los poderes de la Comisión para adoptar actos delegados. Igualmente, la propuesta de Reglamento confería a la Comisión competencias de ejecución con la finalidad de garantizar unas condiciones uniformes para la aplicación del Reglamento. El artículo 87 recogía la disposición relativa al procedimiento del comité necesario para la atribución de competencias de ejecución a la Comisión.

[19] También se ha señalado la responsabilidad en este punto del Grupo de Trabajo del Artículo 29 -que era, como se había dicho reiteradamente, «a key element in ensuring better and more coherent implementation»-, que podía haber tratado de reducir la repercusión negativa de las divergencias legislativas de los Estados miembros en materia de seguridad, aportando alternativas más sencillas que la aprobación de un nuevo marco normativo europeo. Era importante que el Grupo de Trabajo hubiera sido capaz de encontrar una respuesta armonizada a cuestiones de interés público como la seguridad de los tratamientos, lo que hubiera facilitado a las empresas multinacionales el cumplimiento de sus obligaciones. No olvidemos que el Grupo de Trabajo debía informar a la Comisión de la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieran afectar a la equivalencia de la protección de datos personales. De hecho, este grupo tenía la función de «estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea» –art. 30.1.a) y 2 de la Directiva-. La Comisión Europea había reprochado al Grupo de Trabajo que debía mejorar su contribución a la armonización entre los Estados miembros, llegando a afirmar que «estaba dispuesta a formular propuestas si el Grupo de Trabajo no podía hacerlo en un plazo razonable (12 meses)». Cfr. Communication

from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, Bruselas, 7.3.2007, COM (2007) 87 -http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm-.

[20] Cfr. A. Troncoso Reigada, «Hacia un nuevo marco jurídico europeo», cit. págs. 172-184.

[21] En relación con esta evaluación de riesgos, el Considerando 83 del RGPDUE establece que «a fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos […]. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales».

[22] Cfr. A. Troncoso Reigada, «Autoridades de control independientes», cit. págs. 468-469.

[23] La Directiva 2009/136/CE, por la que se modifica la Directiva 2002/58/CE relativa al tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas, incorpora a ésta un art. 2.h) sobre el concepto de violación de datos personales y añade un apartado 4.3, estableciendo la obligación del proveedor de servicios de comunicaciones electrónicas de notificar la violación de datos personales sin dilaciones indebidas tanto a la autoridad de control como a los abonados o particulares, una cuestión que la Comisión Europea había pretendido extender a otras áreas como los servicios financieros.

[24] Cfr. F. Pérez Bes, «La obligación de notificar una violación de seguridad de datos personales», en J. López Calvo (Coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos, cit. págs. 461-470; J. Puyol Montero, Guía divulgativa del Reglamento General de Protección de Datos de la Unión Europea, cit. págs. 149-151.

[25] Además, a la hora de notificar a la autoridad de control la violación de seguridad parece relevante la probabilidad de usurpación de identidad. Así, el Considerando 88 del RGPDUE señala que «al establecer disposiciones de aplicación sobre el formato y los procedimientos aplicables a la notificación de las violaciones de la seguridad de los datos personales, hay que tener debidamente en cuenta las circunstancias de tal violación, inclusive si los datos personales habían sido protegidos mediante las medidas técnicas de protección adecuadas, limitando eficazmente la probabilidad de usurpación de identidad u otras formas de uso indebido».

[26] Esta reflexión la hemos realizado en La protección de datos personales. En busca del equilibrio, cit. págs. 64-78.

[27] La regulación definitiva es más flexible que la propuesta de la Comisión que establecía que la violación de datos personales debía notificarse a la autoridad de control sin demora injustificada y, de ser posible, a más tardar veinticuatro horas después de que se haya tenido constancia de ella –art. 32-.

[28] Esta obligación de documentación de los tratamientos sustituía la obligación de notificación de los tratamientos a la autoridad de control, en aras de la simplificación de cargas administrativas. Finalmente el RGPDUE establece como una obligación del responsable y del encargado del tratamiento el registro de las actividades del tratamiento –art. 30 RGPDUE-, con las excepciones recogidas en el apartado 5.

[29] La propuesta de la Comisión señalaba la obligación de comunicación de la violación de datos personales al interesado cuando sea probable que ésta afecte negativamente a la protección de sus datos personales o a la privacidad del interesado –art. 33-, sin hacer mención a otros derechos y libertades.

[30] Cfr. J. Puyol Montero, Guía divulgativa del Reglamento General de Protección de Datos de la Unión Europea, cit. págs. 152-153.

[31] Con anterioridad, la STJUE de 7 mayo 2009, Caso Rijkeboer, -asunto C-553/07- señalaba que la Directiva 95/46/CE ya apuntaba el carácter desproporcionado de ciertas medidas: «En relación con la obligación de informar al interesado, el cuadragésimo considerando de la Directiva señala que el número de interesados y la antigüedad de los datos pueden ser tomados en consideración a este respecto» –apdo. 62- citando, además, el art. 17 de la Directiva relativo a la seguridad del tratamiento, donde se establece que los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización pertinentes para asegurar un nivel de seguridad adecuado, teniendo en cuenta el estado de la técnica y el coste de su aplicación en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

[32] El Considerando 86 RGPDUE señala que la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

[33] La figura del encargado del tratamiento no estaba bien resuelta en la Directiva –que únicamente definía al encargado en el art. 2.e) y lo regulaba en el art. 17 en relación con la seguridad de los tratamientos-, pero sí en la LOPD –art. 12- y especialmente, en su Reglamento de desarrollo, que establecía un auténtico estatuto del encargado del tratamiento –arts. 20-22-, por lo que la regulación prevista en el RGPDUE supone un avance a nivel europeo pero no aporta grandes novedades en nuestro país.

[34] Esta previsión del RGPDUE proviene del art. 17.2 de la Directiva 95/46/CE que señalaba que «los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguri-

dad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas».

[35] Las PET son «un sistema coherente de medidas de TIC que protege el derecho a la intimidad suprimiendo o reduciendo los datos personales o evitando el tratamiento innecesario o indeseado de datos personales, sin menoscabo de la funcionalidad del sistema de información». De esta forma, «gracias a dichas tecnologías, las infracciones de las normas de protección de datos y la vulneración de los derechos del ciudadano, además de estar prohibidas y sujetas a sanciones, resultarían más difíciles desde el punto de vista técnico». Cfr. la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET) —COM (2007) 228 final—, de 2.5.2007, en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:ES:PDF y que era consecuencia del Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE), cit. También la Comunicación de la Comisión «Una estrategia para una sociedad de la información segura» [COM (2006) 251, de 31 de mayo de 2006], invitaba al sector privado a «estimular el despliegue de productos, procesos y servicios que favorezcan la seguridad a fin de evitar y combatir la sustracción de la identidad y otros ataques contra la privacidad». Con esta comunicación, la Comisión trataba de fomentar la utilización de las PET por parte de los responsables del tratamiento de datos y los consumidores. Con anterioridad, la Directiva 2002/58/CE establecía que «cuando proceda, se podrán adoptar medidas para garantizar que los equipos terminales estén fabricados de manera compatible con el derecho de los usuarios de proteger y controlar el uso de sus datos personales» –art. 14.3-. Esta cuestión la hemos analizado en «Hacia un nuevo marco jurídico europeo», loc. cit. págs. 48-49.

[36] Además de la seguridad del tratamiento, el Considerando 94 RGPDUE señala que existe la probabilidad de que ese alto riesgo se deba a determinados tipos de tratamiento y al alcance y frecuencia de este, lo que también puede ocasionar daños y perjuicios o una injerencia en los derechos y libertades de la persona física.

[37] Los códigos de conducta abordan otros aspectos como el tratamiento leal y transparente; los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos; la recogida de datos personales; la información proporcionada al público y a los interesados; el ejercicio de los derechos de los interesados; la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño; la transferencia de datos personales a terceros países u organizaciones internacionales, o los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento.

[38] La Comisión evaluará la adecuación del nivel de protección teniendo en cuenta distintos elementos como el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación relativa a la seguridad pública, la defensa y la seguridad nacional, la legislación penal, el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, incluidas las normas sobre transferencias internacionales de datos personales, la jurisprudencia y el reconocimiento a los interesados de derechos efectivos y exigibles, y de recursos administrativos y acciones judiciales que sean efectivos.

[39] Cfr. el debate y votación en el Diario de Sesiones de ese día. http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu12&DOCS=1-1&QUERY=%28DSCD-12-PL-157.CODI.%29#(P%C3%A1gina38).

[40] Cfr. el texto aprobado por el Pleno del Congreso de los Diputados, relativo al Proyecto de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, que se encuentra publicado en el BOCG, Senado, Núm. 289, 23 de octubre de 2018.

[41] Así, en relación con este último derecho, el art. 81.2 establece que «se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población», sin precisar a quien le corresponde esta función. Además, el art. 81.3 señala que «el acceso a Internet de hombres y mujeres procurará la superación de la brecha de género tanto en el ámbito personal como laboral» y el art. 81.4 recoge que «el acceso a Internet procurará la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores». Parece razonable pensar que esta obligación de superar la brecha género y la brecha generacional le corresponda a las Administraciones Públicas o a la regulación que lleven a cabo estas. Sin embargo, no parece posible que esta función le corresponda a un nuevo sujeto, «el acceso a Internet», y que este nuevo sujeto vaya a llevar a cabo «acciones dirigidas a la formación y el acceso a las personas mayores». Algo semejante puede decirse del art. 81.6 que señala que «el acceso a Internet deberá garantizar condiciones de igualdad para las personas que cuenten con necesidades especiales». Hay que leer este precepto a la luz del art. 97, que regula las «políticas de impulso de los derechos digitales», que establece que el Gobierno, en colaboración con las CC.AA. elaborará un Plan de Acceso a Internet para «superar las brechas digitales y garantizar el acceso a Internet de colectivos vulnerables», «impulsar la existencia de espacios de conexión de acceso público»; y «fomentar medidas educativas que promuevan la formación en competencias y habilidades digitales básicas a personas y colectivos en riesgo de exclusión digital y la capacidad de todas las personas para realizar un uso autónomo y responsable de Internet y de las tecnologías digitales».

[42] Sin embargo, sí parece un poco desmedida la Disposición final octava, que modifica el art. 46.2 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades para añadir un nuevo apartado l). Este artículo regula los derechos y deberes de los estudiantes así como la igualdad de oportunidades y no discriminación en el acceso a la universidad, el asesoramiento y asistencia por parte de profesores, la representación

de los alumnos en los órganos de gobierno, la libertad de expresión, de reunión y de asociación en el ámbito universitario, la garantía de sus derechos a través de la actuación del defensor universitario, a lo que ahora se añade la «formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet».

[43] La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, señala en relación con el archivo de documentos que «los medios o soportes en que se almacenen documentos deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados» -art. 17.3-. También en lo relativo a la validez y eficacia de las copias realizadas por las Administraciones Públicas se establece que para garantizar la identidad y contenido de las copias electrónicas o en papel, y por tanto su carácter de copias auténticas, las Administraciones Públicas deberán ajustarse a lo previsto en el Esquema Nacional de Interoperabilidad, el Esquema Nacional de Seguridad y sus normas técnicas de desarrollo –art. 27-. Por último, la Disposición adicional segunda señala que las plataformas y registros de las Comunidades Autónomas y Entidades Locales deben garantizar que cumplen los requisitos del Esquema Nacional de Interoperabilidad, el Esquema Nacional de Seguridad, y sus normas técnicas de desarrollo.

[44] El art. 8.2 PLOPDyGDD reitera que «el tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley».

[45] También hay otras infracciones consideradas graves en el art. 73 PLOPDyGDD que tienen también una relación indirecta con la seguridad de los tratamientos. Así, se considera infracción grave «la falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del RGPDUE» –art. 73.d) PLOPDyGDD-, teniendo en cuenta que dentro de estas medidas técnicas y organizativas está la seudonimización. En esta misma dirección también se considera infracción grave «la falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, sólo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento, conforme a lo exigido por el artículo 25.2 del RGPDUE» –art. 73.e) PLOPDyGDD-. Igualmente se considera infracción grave «la contratación por el responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas conforme a lo establecido en el Capítulo IV del RGPDUE» - art. 73.j) PLOPDyGDD-.