HACIA UN NUEVO SISTEMA EUROPEO DE PROTECCIÓN DE DATOS: LAS CLAVES DE LA REFORMA

ARTEMI RALLO LOMBARTE

SUMARIO

Fecha recepción: 14.03.2012
Fecha aceptación: 25.06.2012

HACIA UN NUEVO SISTEMA EUROPEO DE PROTECCIÓN DE DATOS: LAS CLAVES DE LA REFORMA

ARTEMI RALLO LOMBARTE[1]

Catedrático de Derecho Constitucional
Universidad Jaume I de Castellón

1. INTRODUCCIÓN: 25 DE ENERO DE 2012, EL ANUNCIO DE LA REFORMA[2]

El pasado 25 de enero de 2012 la Comisión Europea presentó sendas iniciativas legislativas dirigidas a reformar el sistema europeo de protección de datos.

En el acto de presentación de esta ambiciosa reforma, Viviane Reding, Comisaria de Justicia y Vicepresidenta de la Comisión Europea, sintetizaba así la necesidad de la reforma: «Hace 17 años, menos de un 1 % de los europeos usaba Internet. Hoy en día se transfieren e intercambian enormes cantidades de datos personales entre continentes y de una punta a otra del mundo en fracciones de segundos. La protección de los datos personales es un derecho fundamental de todos los europeos, quienes, no obstante, a veces sienten que pierden el control so-

[1] Director de la Agencia Española de Protección de Datos (2007-2011), Vicepresidente del Grupo de Trabajo creado por el art. 29 de la Directiva 95/46 formado por todas las Autoridades Europeas de Protección de Datos (2010-2011) y Presidente de la Red Iberoamericana de Protección de Datos (2007-2009).

[2] Un primer saludo a la valentía y ambición de la Comisión Europea y a la trascendencia del cambio normativo en RALLO, A.: «Que aguante el paso del tiempo», *El País*, 24 de enero de 2012.

bre sus datos personales. Mis propuestas contribuirán a infundir confianza en los servicios en línea dado que los ciudadanos estarán mejor informados de sus derechos y tendrán un mayor control sobre la información que les atañe. La reforma conseguirá todos estos objetivos al tiempo que facilitará el funcionamiento de las empresas y les permitirá ahorrar costes. La existencia de un marco legal sólido, claro y uniforme a escala de la UE permitirá liberar el potencial del Mercado Único Digital»[3].

Dicha reforma del marco legal supone dos proyectos normativos: a) por un lado, la Comisión ha presentado un *Proyecto de Reglamento del Parlamento Europeo y del Consejo para la protección de los ciudadanos en relación con el tratamiento de los datos personales y la libre circulación de dichos datos* (esto es, un **Reglamento General de Protección de Datos** —en adelante, RGPD—)[4]; b) y, por otro lado, la Comisión ha presentado un *Proyecto de Directiva del Parlamento Europeo y del Consejo sobre protección de los ciudadanos en relación al tratamiento de los datos personales por las autoridades competentes con la finalidad de prevenir, investigar, detectar y perseguir delitos o ejecutar penas, y sobre el libre movimiento de dichos datos* (**Directiva para la protección de datos en el ámbito de la Policía y la Justicia Penal** —en adelante, DPJP—)[5].

Como puede observarse, las iniciativas de la Comisión Europea comportan una *revisión global* del sistema europeo de protección de datos tanto en el ámbito formal como sustantivo. Por un lado, el nuevo marco normativo europeo se sustentará sobre la base de un *diferente instrumento normativo* (RGPD frente a la anterior Directiva 95/46) y, por otro lado, resulta evidente que este nuevo RGPD abordará nuevas problemáticas hasta la fecha no satisfactoriamente resueltas por la normativa vigente (especialmente, en cuanto al impacto de las nuevas tecnologías y de Internet en el tratamiento de los datos personales y en su incidencia en la privacidad de los ciudadanos). Todo ello, cuando resulten finalmente aprobadas ambas propuestas normativas (de lo que no existe apenas duda dado el altísimo consenso existente sobre su necesidad y del imparable impulso político-institucional que las instituciones europeas le están proporcionando), *revolucionará* el marco global europeo de la protección de datos y, además, tendrá un *extraor-*

[3] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm, págs. 1 a 134.

[4] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, págs. 1 a 59.

[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0010:en:NOT. Como es sabido, la legislación vigente de la UE en materia de protección de datos, se sustenta sobre la Directiva 95/46. Sin embargo, esta norma se complementó mediante la Decisión Marco 2008/977/JAI, en su calidad de instrumento general a escala de la Unión para la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (a la que viene a suceder la actual propuesta nueva Directiva sobre protección de datos en el ámbito de la Policía y Ja Justicia Penal.

dinario impacto en el sistema español de protección de datos por cuanto: a) por un lado, la parte principal de esta nueva legislación europea va a resultar de *directa e inmediata aplicación* por gozar de naturaleza de reglamento europeo; b) y, por otro lado, este futuro marco jurídico proporcionará *nuevos derechos* a los ciudadanos a la vista de los objetivos perseguidos por esta nueva normativa: 1) reforzar los derechos de las personas (garantizar a las personas una protección adecuada en cualesquiera circunstancias, aumentar la transparencia para los interesados, reforzar el control sobre los propios datos, garantizar un consentimiento informado y libre, proteger los datos sensibles); 2) y fortalecer el marco institucional de garantía (reforzar la independencia de las Autoridades de Protección de Datos y la eficacia de las vías de recurso y las sanciones, aumentar la seguridad jurídica y garantizar condiciones iguales a los responsables del tratamiento, reducir la carga administrativa, clarificar las normas relativas a la legislación aplicable, reforzar la responsabilidad de los responsables del tratamiento).

2. ANTECEDENTES. LA COMUNICACIÓN DE LA COMISIÓN EUROPEA DE 2009 SOBRE *«UN ENFOQUE GLOBAL DE LA PROTECCIÓN DE LOS DATOS PERSONALES EN LA UNIÓN EUROPEA»:* DE LA DIRECTIVA 95/46 AL ART. 8 CDFUE

La *Directiva relativa a la protección de datos de 1995* (95/46)[6] estableció un hito en la historia de la protección de los datos personales en la Unión Europea[7].

[6] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281, 23.11.1995).

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:HTML

[7] Entre nosotros, la Directiva 95/46 de protección de datos todavía vigente ha sido objeto de análisis jurídico durante los últimos años como lo ilustran las siguientes obras: HEREDERO HIGUERAS, M.(1997): *La directiva comunitaria de protección de los datos de carácter personal: comentario a la directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, Editorial Aranzadi, Pamplona; ANGEL DAVARA, M. (1998): *La protección de datos en Europa: principios, derechos y procedimiento*, Grupo Asnef-Equifax, Madrid; SÁNCHEZ BRAVO, A. (1998): *La protección del derecho a la libertad informática en la Unión Europea.* Universidad de Sevilla, Sevilla; ARENAS RAMIRO, M. (2006): *El derecho fundamental a la protección de datos personales en Europa,* Tirant lo Blanch-Agencia Española de Protección de Datos, Valencia; REBOLLO DELGADO, L. (2008): *Vida privada y protección de datos en la Unión Europea*, Madrid. Dykinson. Más allá de nuestras fronteras, resulta imprescindible KUNER, C. (2007): *European Data Protection Law. Corporate Compliance and Regulation*, Oxford University Press, Oxford. Y una reflexión más general sobre el alcance del recho a la protección de datos, en MARTTINEZ, R. (2004): *Una aproximación crítica a la autodeterminación informativa*, Civitas, Pamplona.

Diecisiete años más tarde, los principios consagrados en la Directiva siguen siendo válidos pero *la rapidez de la evolución tecnológica y la globalización* ofrecen *nuevos retos* en materia de protección de los datos personales[8]. La tecnología permite a los ciudadanos intercambiar fácilmente información con respecto a sus comportamientos y sus preferencias, y hacerla pública a nivel mundial a una escala sin precedentes. Las redes sociales, con centenares de millones de miembros en todo el mundo, constituyen seguramente el ejemplo más evidente de este fenómeno, sin ser el único. La computación en nube, esto es, informática basada en internet en la que los programas, los recursos compartidos y la información se encuentran en servidores remotos, también plantean retos para la protección de datos, dado que puede implicar la pérdida del control por parte de los individuos de su información potencialmente sensible cuando almacenan sus datos utilizando programas alojados en servidores ajenos.

Las autoridades responsables de la protección de datos, las organizaciones profesionales y las asociaciones de consumidores coinciden en que los riesgos para la protección de la intimidad y los datos personales están aumentando con las actividades *on line*. Paralelamente, los métodos de recogida de los datos personales son cada vez más complicados y se detectan con más dificultad. El mayor recurso a procedimientos que permiten la recogida automática de datos, como el pago electrónico de billetes, el cobro de peajes en carreteras, o instrumentos de geolocalización[9], facilitan la determinación de la ubicación de un individuo por el mero uso por su parte de un dispositivo móvil. Las autoridades públicas también utilizan cada vez más datos personales con distintos fines: para buscar personas cuando se declara una enfermedad transmisible, para prevenir y luchar más eficazmente contra el terrorismo y la delincuencia, para gestionar su régimen de seguridad social o a efectos fiscales, en el marco de sus aplicaciones de administración en línea, etc.

Las consideraciones anteriores —plenamente vigentes en la actualidad pero ya en su plenitud durante los últimos años— han venido suscitando inevitablemente la cuestión de si la legislación de la Unión Europea en materia de protección de datos era/es capaz de hacer frente plena y eficazmente a estos retos. Para responder a esta cuestión, la Comisión Europea inició un examen del marco jurídico europeo en vigor, con una conferencia de alto nivel en mayo de 2009, seguida de una consulta pública hasta finales de 2009, y de diversos es-

[8] Un recorrido por esta problemática puede encontrarse en el libro de quien fuera Presidente de la CNIL y del Grupo de Trabajo del Artículo 29, TURK, A. (2011): *La vie privée en peril*, Odile Jacob, Paris.

[9] Sobre su reciente impacto en la privacidad, véase el Dictamen 13/2011 del Grupo de Trabajo del Artículo 29 (WP 185) el 16 de mayo de 2011 sobre servicios de geolocalización en los dispositivos móviles inteligentes (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_es.pdf).

tudios. Los resultados obtenidos confirmaron que los principios fundamentales de la Directiva siguen siendo válidos y que conviene preservar su neutralidad desde el punto de vista tecnológico. No obstante, se identificaron varios problemas y *retos específicos*:

1º) *El impacto de las nuevas tecnologías*. Existe una improrrogable necesidad de clarificar y precisar la aplicación de los principios de la protección de datos a las nuevas tecnologías, con el fin de garantizar una protección real y efectiva de los datos personales, cualquiera que sea la tecnología utilizada para tratar estos datos, y que los responsables del tratamiento de los datos tengan plena conciencia de las implicaciones de las nuevas tecnologías en la protección de datos.

2º) El reforzamiento del *mercado interior de la protección de datos.* Resulta insuficiente la armonización de las legislaciones de los Estados miembros en materia de protección de datos, a pesar de la existencia de un marco jurídico común de la UE. Las empresas plantean la necesidad de aumentar la seguridad jurídica, de reducir las cargas administrativas y de garantizar la igualdad de condiciones a los agentes económicos y a otros responsables del tratamiento.

3º) La *globalización y la mejora de las transferencias internacionales de datos*. El incremento en la subcontratación del tratamiento, muy a menudo fuera de la UE, plantea varios problemas vinculados a la legislación aplicable al tratamiento y a la atribución de la responsabilidad correspondiente. Por lo que respecta a las transferencias internacionales de datos, los regímenes actuales no son plenamente satisfactorios y deben revisarse y racionalizarse.

4º) La *aplicación efectiva de las normas sobre protección de datos*. Existe un amplio consenso respecto a la conveniencia de reforzar el papel de las autoridades encargadas de la protección de datos con el fin de mejorar la aplicación de las normas en este ámbito y garantizar una mayor transparencia de los trabajos del Grupo de Trabajo del Artículo 29 y la clarificación de su misión y poderes.

5º) *Mejorar la coherencia del marco jurídico que regula la protección de datos*. Resulta necesario un instrumento global, aplicable a las operaciones de tratamiento de datos en todos los sectores y políticas de la Unión, que garantice un enfoque integrado y una protección global, coherente y eficaz.

En consecuencia, los retos previamente mencionados invitaban UE a elaborar un enfoque global y coherente que garantice el pleno respeto del derecho fundamental a la protección de los datos personales tanto en la UE como fuera de ésta.

Pero, en paralelo a la evolución de las circunstancias sociales, económicas o tecnológicas que han acompañado el proceso de globalización y su impacto en el derecho de protección de datos desde que se adoptó la Directiva 95/46, las *novedades jurídico-constitucionales* operadas desde entonces en la Unión Europea también se han proyectado singularmente en ese ámbito. Como es sabido, el 7 de diciembre de 2000 se proclamó en Niza la CDFUE que, en su art. 8, reconocía el derecho a *la protección de datos personales*: «1. *Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal,*

para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente». Posteriormente, el 12 de diciembre de 2007 esta redacción quedó confirmada en Estrasburgo y, finalmente, el artículo 6 del Tratado de la Unión Europea (TUE) —en la redacción consolidada por el Tratado de Lisboa— le ha otorgado el *mismo valor jurídico* que los Tratados.

La mejor demostración de esta historia de éxito protagonizada por la Directiva 95/46 reside en su capacidad de, en poco más de una década, consolidar constitucionalmente en los Tratados constitutivos (ex art. 6 TUE, art. 8 CDFUE y art. 16 TFUE) un derecho emergente a la protección de datos personales cuyos orígenes más remotos apenas alcanzan a la adopción del Convenio del Consejo de Europa para la protección de datos personales frente a su tratamiento automatizado en 1981[10].

Por lo tanto, el Tratado de Lisboa otorgó fuerza jurídica vinculante a la CDFUE y, en concreto, al derecho autónomo a la protección de datos de carácter personal que consagra en su art. 8. Y —lo que resulta más relevante a los efectos del presente estudio— los arts. 6 TUE, 8 CDFUE y 16 TFUE han creado una *nueva base jurídica* que permite la elaboración de una normativa global de la Unión Europea relativa al tratamiento de los datos personales y a la libre circulación de estos datos y, además, con esta nueva base jurídica se autoriza a la Unión a regular específicamente la protección de datos, por medio de una Directiva, en los ámbitos de la cooperación policial y judicial en materia penal.

Al amparo de estas nuevas posibilidades jurídicas, la Comisión Europea ha concedido la más alta prioridad al derecho fundamental a la protección de datos

[10] El art. 6 TUE proclama que los derechos, libertades y principios enunciados en la CDFUE se interpretarán con arreglo a las disposiciones generales del título VII de la Carta por las que se rige su interpretación y aplicación y teniendo debidamente en cuenta las explicaciones a que se hace referencia en la Carta, que indican las fuentes de dichas disposiciones. Y, en concreto, la Explicación relativa al artículo 8 (*Protección de datos de carácter personal*) aclara, sin margen de error, la relación causal entre la Directiva 95/46 y el art. 8 CDFUE: «Este artículo se ha basado en el artículo 286 del Tratado constitutivo de la Comunidad Europea y en la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31), así como en el artículo 8 del CEDH y en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, ratificado por todos los Estados miembros. El artículo 286 del Tratado CE ha sido sustituido por el artículo 16 del Tratado de Funcionamiento de la Unión Europea y el artículo 39 del Tratado de la Unión Europea. Conviene señalar asimismo el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (*Diario Oficial*, L 8 de 12.1.2001, p. 1)».

en el conjunto de la Unión y en todas sus políticas, reforzando al mismo tiempo la dimensión de mercado interior de esta protección y facilitando la libre circulación de datos personales. Y, para ilustrar tal interés institucional, la Comisión europea presentó en Bruselas el 4 de noviembre de 2010 la *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social europeo y al Comité de las Regiones sobre «Un enfoque global de la protección de los datos personales en la Unión Europea»*[11] con el objeto definir la estrategia que permitiría a la Comisión modernizar el régimen jurídico de la UE para la protección de los datos personales en todos los ámbitos de actuación de la Unión, teniendo en cuenta, en particular, los retos derivados de la globalización y las nuevas tecnologías, de modo que siguiera garantizando un elevado nivel de protección de los ciudadanos respecto al tratamiento de estos datos en todos estos ámbitos.

Esta *Comunicación* concluía que, al igual que la tecnología, la forma en que los datos personales se utilizan y comparten en la sociedad está en evolución constante lo que plantea a los legisladores el reto de establecer un marco legislativo que resista al tiempo y, en particular, que las normas europeas de protección de datos sigan asegurando un elevado nivel de protección y seguridad jurídica a las personas, a las Administraciones públicas y a las empresas en el mercado interior, durante varias generaciones. La Comunicación de la Comisión estimaba esencial que las normas que debían aplicar las autoridades nacionales y que debían cumplir las empresas y los responsables del desarrollo de tecnologías, estuvieran claramente definidas; y, del mismo modo, las personas deberían tener claros sus derechos. Por ello, a fin de abordar los problemas y alcanzar los objetivos esenciales puestos de relieve en dicha Comunicación, se anunció que la Comisión Europea presentaría *propuestas legislativas* destinadas a revisar el marco jurídico de la protección de datos, con el objetivo de reforzar la situación de la UE en materia de protección de los datos personales en el contexto de todas las políticas de la UE, incluso en los ámbitos de la prevención de la delincuencia y la aplicación de la ley. Además, se anunció la adopción de medidas no legislativas, como la promoción de la autorregulación y el examen de la viabilidad de los distintivos europeos de protección de la intimidad.

3. LAS CLAVES DE LA REFORMA: PRINCIPALES IDEAS-FUERZA

A) Las debilidades *de* viejo *marco jurídico*

La Directiva 95/46 fue adoptada con un doble objetivo: defender el derecho fundamental a la protección de datos y garantizar la libre circulación de estos da-

[11] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012DC0009:en:NOT

tos entre los Estados miembros. Este marco general de protección de datos se vio complementado, ya en fecha más reciente, mediante la Decisión Marco 2008/977/JAI, en su calidad de instrumento general a escala de la Unión para la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

El nacimiento de la normativa europea de protección de datos es deudor del singular proceso comunitario de construcción del sistema europeo de protección de los derechos fundamentales. A falta de un directo fundamento jurídico sobre el que derivar su garantía, sus bases originarias se edifican sobre los principios básicos de articulación comunitaria sustentados en las libertades inherentes al mercado interior. Y, así, desde esta perspectiva *mercantilista/economicista,* se observa la paradoja de que la protección de datos nace como un *problema/obstáculo* a la construcción del mercado interior y no como la autónoma definición de un nuevo status de libertad para los ciudadanos europeos. El Considerando (7) de la Directiva 95/46 lo ilustraba sin matices: «Considerando que las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, pueden impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro; que, por lo tanto, estas diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario…»[12]. La subordinación de las

[12] Y, a mayor abundamiento, enfatizan este enfoque tradicional algunos de los restantes Considerandos de la Directiva 95/46: «(3) Considerando que el establecimiento y funcionamiento del mercado interior, dentro del cual está garantizada, con arreglo al artículo 7 A del Tratado, la libre circulación de mercancías, personas, servicios y capitales, hacen necesaria no sólo la libre circulación de datos personales de un Estado miembro a otro, sino también la protección de los derechos fundamentales de las personas; (4) Considerando que se recurre cada vez más en la Comunidad al tratamiento de datos personales en los diferentes sectores de actividad económica y social; que el avance de las tecnologías de la información facilita considerablemente el tratamiento y el intercambio de dichos datos; (5) Considerando que la integración económica y social resultante del establecimiento y funcionamiento del mercado interior, definido en el artículo 7 A del Tratado, va a implicar necesariamente un aumento notable de los flujos transfronterizos de datos personales entre todos los agentes de la vida económica y social de los Estados miembros, ya se trate de agentes públicos o privados; que el intercambio de datos personales entre empresas establecidas en los diferentes Estados miembros experimentará un desarrollo; que las administraciones nacionales de los diferentes Estados miembros, en aplicación del Derecho comunitario, están destinadas a colaborar y a intercambiar datos personales a fin de cumplir su cometido o ejercer funciones por cuenta de las administraciones de otros Estados miembros, en el marco del espacio sin fronteras que constituye el mercado interior; (6) Considerando, por lo demás, que el fortalecimiento de la cooperación científica y técnica, así como el establecimiento coordinado de nuevas redes de telecomunicaciones en la Comunidad exigen y facilitan la circulación transfronteriza de datos personales».

estrategias comunitarias de garantía de determinados derechos individuales al necesario anclaje en las bases jurídicas proporcionadas por los Tratados explica, además, que años más tarde tuviera que optarse por el sistema de cooperación intergubernamental para proyectar la garantía de la protección de datos también al ámbito policial y penal a través de la Decisión Marco 2008/977. Esta singular estrategia normativa no impide constatar que, con el tiempo, la protección de datos garantizada por la Directiva 95/46 le ha otorgado un carácter sustantivo que obliga hoy a perfeccionar el instrumento jurídico elegido a la vista de las debilidades observadas en la Directiva 95/46 y de las nuevas bases jurídico-constitucionales que permiten reconocer, regular y garantizar la protección de datos personales como un derecho autónomo de los europeos.

Porque, si bien, como decíamos, la historia de la Directiva 95/46 puede ser calificada como una singular historia de éxito no son pocas las *dificultades* que ha encontrado su aplicación y las *limitaciones* que su propia naturaleza acarrea. La Directiva 95/46, a pesar de su vocación armonizadora, otorgaba a los Estados miembros un relevante margen de maniobra y les permitía mantener regulaciones específicas. En ocasiones, los Estados miembros han aplicado incorrectamente la Directiva y, todo ello, ha comportado notables divergencias entre las legislaciones nacionales de transposición, contradiciéndose precisamente el objetivo primario de la garantía de la libre circulación de datos en el mercado interior. La falta de armonización ha sido especialmente denunciada por los representantes de los sectores económicos (que en un mundo empresarial y económico globalizado dicen ver multiplicados los costes y los requisitos burocrático-administrativos nacionales) y se ha traducido en un cierto grado de inseguridad jurídica lejos del objetivo originario perseguido por la Directiva tendente a lograr un nivel equivalente de protección en todo el territorio de la Unión Europea.

De hecho, la Comisión Europea, el 15 de mayo de 2003, en su *Primer informe sobre la aplicación de la Directiva sobre protección de datos 95/46*[13] ya apuntaba buena parte de los *argumentos críticos* que han conducido al alumbramiento de las actuales propuestas de reforma: 1) la necesidad de una interpretación razonable y flexible de la normativa de protección de datos (por ejemplo, sobre el concepto de datos sensibles, el derecho de acceso de los interesados a sus datos personales o las condiciones de licitud de los tratamientos de datos personales); 2) la necesitad de una estrategia preventiva basada en la promoción y fomento de las tecnologías de protección de la intimidad que reduzcan al mínimo la recogida y empleo de datos personales y dificulte las posibilidades de tratamiento ilícito; 3) necesidad de clarificar el Derecho aplicable a las organizaciones multinacionales para operar con una única normativa en toda la UE; 4) necesidad de aclarar el concepto de

[13] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:ES:DOC, págs. 1 a 23.

«consentimiento inequívoco» frente al concepto de «consentimiento explícito» para garantizar el alcance del consentimiento válido en las actividades *on line*; 5) mejorar la información a los ciudadanos; 6) necesidad de simplificar y aproximar los requisitos de los Estados respecto a la notificación de las operaciones de tratamiento de datos; 7) revisar el impacto exterior del tratamiento de datos frente a la laxitud de legislaciones nacionales que ejercen un control muy limitado de los flujos internacionales de datos y la incoherencia de otros Estados al someter todas las transferencias a terceros países a una autorización administrativa generando una carga administrativa excesiva tanto a los exportadores de datos como para las autoridades de control.

A pesar de todo ello, este *Primer informe* de la Comisión Europea apostó por *mantener íntegra la Directiva 95/46* y reforzar la exigencia de su aplicabilidad. La Comisión consideró que los resultados de la revisión rebatían la propuesta de modificaciones a la Directiva (por las que abogaron, por ejemplo, Austria, Suecia, Finlandia y el Reino Unido) teniendo en cuenta la limitada experiencia de aplicación de la Directiva, que muy pocos Estados miembros habían aplicado puntualmente la Directiva —«los graves retrasos producidos en la aplicación en la mayoría de los Estados miembros constituye la primera y principal deficiencia que la Comisión tiene el deber de registrar en relación con la aplicación de la Directiva, por lo que los condena de manera inequívoca»[14]—, que buena parte de las críticas lo eran a la aplicación incorrecta por la legislación nacional, que la cooperación entre las autoridades de control debería permitir la convergencia necesaria superadora de las prácticas excesivamente divergentes entre los distintos Estados y que buena parte de las modificaciones propuestas pretendían la reducción de las obligaciones de los responsables del tratamiento de datos —lo que, en definitiva, suponía la reducción del nivel de protección de los datos personales—.

Y, ya en fecha más reciente, la Comisión Europea reiteró su criterio sobre la no necesidad de modificación de la Directiva 95/46 —lo que, a la vista de las propuestas de reforma legislativa presentadas el 25 de enero de 2012, resulta extraordinariamente llamativo y chocante (cuando no enigmático)—. En la *Comunicación de la Comisión Europea al Parlamento Europeo y al Consejo, de 7 de marzo de 2007, sobre «Seguimiento del Programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos»*[15] se concluyó que la aplicación de la Directiva 95/46 había mejorado pues todos los Estados miembros habían transpuesto la Directiva por lo que no se requería la modificación de la Directiva. Para la Co-

[14] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:ES:DOC, pág. 8.

[15] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0087:FIN:ES:DOC, págs. 1 a 10.

misión la Directiva sobre la protección de datos constituía un marco jurídico general que cumplía con sus objetivos originales constituyendo una garantía suficiente para el funcionamiento del mercado interior, asegurando al mismo tiempo un alto nivel de protección del derecho fundamental a la protección de los datos personales, garantizando la confianza de los individuos en la utilización de su información personal necesarial para el desarrollo de la economía que utiliza los medios electrónicos, estableciendo una referencia para las iniciativas en numerosas áreas políticas desde un enfoque tecnológicamente neutral y, en fin, proporcionando respuestas sólidas y apropiadas a todos estos asuntos. Por todo ello, concluía, «la Comisión no tiene previsto presentar ninguna propuesta legislativa para modificar la Directiva»[16].

¿Qué había ocurrido en apenas dos años (2007-2009 —el 9 de julio de 2009 la Comisión Europea lanzó la consulta pública sobre la revisión del marco legal europeo de protección de datos—) para que la Comisión Europea variara de forma tan sorprendente un criterio tan reciente e iniciara el proceso de revisión legislativa que ha culminado con la presentación de los proyectos de RGPD y DPJP?

Aparentemente, ningún hecho o factor singular se ha manifestado como individualmente causante del cambio legislativo. Más bien al contrario, cabe afirmar que fueron un conjunto amplio de motivos —unos con mayor intensidad que otros— los que operaron este asombroso cambio en la posición de la Comisión Europea. Y, de entre ellos, podemos resaltar los siguientes factores: a) La deficiente transposición de la Directiva y, en consecuencia, una débil armonización europea; b) las limitaciones de las Autoridades nacionales de protección de datos en la garantía efectiva y similar del derecho a la protección de datos en el conjunto del territorio europeo; c) la incesante presión de las empresas multinacionales europeas y, particularmente, norteamericanas quejosas ante los obstáculos burocráticos a las transferencias internacionales y la heterogeneidad de reglas nacionales; d) el extraordinario impacto tecnológico de servicios *on line* (como las redes sociales) de titularidad estadounidense y ajenos a las exigencias europeas); e) el enorme alcance mediático de la protección de la privacidad y el singular incremento en la sensibilización social; f) el dificultoso diálogo trasatlántico EU-USA sobre las transferencias de dato con fines de seguridad (Casos Swift y PNR); g) la propia agenda europea en seguridad que intensificaba las exigencias de intercambios de datos personales; h) el impulso político de la Comisión personificado en el Comisario de Justicia saliente Barrot y, singularmente, en su sucesora Reding; i) y, como veremos a continuación, de forma principal, la entrada en vigor del Tratado de Lisboa que alentaba las expectativas de nuevas ambicio-

[16] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0087:FIN:ES:DOC, pág. 8.

nes en la garantía efectiva del derecho a la protección de datos personales. Sin lugar a dudas, la confluencia, acumulación e intensificación de todos estos factores crearon el ambiente necesario para que en apenas dos años la Comisión Europea diera un golpe de timón de ciento ochenta grados y propugnara una revisión general del marco jurídico europeo de protección de datos

B) Una nueva base jurídica: *art. 16 TFUE, art. 6 TUE y el art. 8 CDFUE*

Como ya hemos señalado, la proclamación en 2000 de la Carta de Derechos Fundamentales de la Unión Europea constituyó, desde el primer momento, una referencia inexcusable en los pasos dados por la Comisión Europea en la evaluación de la aplicación efectiva de la Directiva 95/46 y en su latente pretensión de operar un giro copernicano en el enfoque de garantía de la protección de datos superando las limitadas bases jurídicas que ofrecían los Tratados hasta ese momento. No en vano, en el ya referido Informe de la Comisión Europea sobre la aplicación de la Directiva de 2003 ya anunciaba ésta el *intuible cambio de base jurídica*. La Comisión Europea reconocía explícitamente que la Directiva 95/46 consagraba dos de las ambiciones más antiguas del proyecto de integración europea —la realización del mercado interior a través de la libre circulación de datos personales y la protección de los derechos y libertades fundamentales de las personas— pero, sin embargo, advertía que, desde el punto de vista jurídico, la base jurídica de la Directiva residía en la garantía del mercado interior. El mercado interior era, en definitiva, la *verdadera excusa jurídica* para la realización de un derecho pues permitía legislar a nivel comunitario debido a que las diferencias entre los Estados miembros obstaculizaban la libre circulación de datos personales. Y así la base jurídica de la Directiva 95/46 fue el artículo 100 A del Tratado. No obstante, la Comisión reconocía en 2003 que la proclamación de la Carta de los Derechos Fundamentales de la Unión Europea por el Parlamento Europeo, el Consejo y la Comisión en diciembre de 2000 —y en particular su artículo 8, que incorpora el derecho a la protección de datos— «recalcó la dimensión que tiene la Directiva en relación con los derechos fundamentales»[17].

Las expectativas latentes en este Primer Informe de la Comisión adquirirían ya plena carta de naturaleza y serían palmariamente evidentes en 2007 cuando, todavía viva la llama en el proceso de ratificación del Tratado Constitucional Europeo, la Comisión presentó su Comunicación de 7 de marzo sobre «Seguimiento del Programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos» advirtiendo del inminente cambio que supondría la plena

[17] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:ES:DOC, pág. 3.

vigencia jurídica del art. 8 CDFUE e ilustrando sobre el *camino por recorrer en el futuro* afirmaba: «La ratificación del Tratado constitucional puede abrir nuevas perspectivas. El Tratado constitucional tendría un enorme efecto en este ámbito. Recogería en el artículo II-68 el derecho a la protección de los datos personales que figura en el artículo 8 de la Carta de los Derechos Fundamentales. También crearía un fundamento jurídico específico e independiente para que la Unión legisle en este asunto en el artículo I-51, preparando el camino para adoptar instrumentos aplicables en todos los sectores. La actual división en "pilares" y las limitaciones del artículo 3 de la Directiva no serán materia de debate»[18].

El frustrada ratificación del Tratado Constitucional no desalentó a la Comisión Europea que, con la firma del Tratado de Lisboa el 13 de diciembre de 2007 y su posterior entrada en vigor el 1 de diciembre de 2009, vio satisfecha su pretensión de búsqueda de una *nueva base jurídica para la reforma del sistema europeo de protección de datos* en los arts. 6.1 (en relación el art. 8 CDFUE) y 39 TUE y en el art. 16 TFUE (Tratado por el que se regula el Funcionamiento de la Unión Europea).

Así, el art. 16 TFUE proclama: «1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes»[19].

Obviamente, aunque resulte escasamente necesario, la delimitación del alcance del derecho reconocido en el anterior precepto obliga a recordar que el art. 6 TUE otorga a la Carta de los Derechos Fundamentales de la Unión Europea «el mismo valor jurídico que los Tratados» y que el art. 8 CDFUE reconoce y garantiza el *derecho a la protección de datos personales* en los siguientes términos: «1.

[18] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0087:FIN:ES:DOC, págs. 8 y 9.

[19] El art. 16.3 TFUE añade: «Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el art. 39 TUE». Este último precepto, ubicado en el Capítulo relativo a la Política Exterior y la Seguridad Común, afirma: «De conformidad con el artículo 16 del Tratado de Funcionamiento de la Unión Europea, y no obstante lo dispuesto en su apartado 2, el Consejo adoptará una decisión que fije las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del presente capítulo y sobre la libre circulación de dichos datos. El respeto de dichas normas estará sometido al control de autoridades independientes».

Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente».

Tras la entrada en vigor del Tratado de Lisboa resultaba evidente que, amén del *impacto general* que proyectaba el nuevo valor jurídico del art. 8 CDFUE, el artículo 16.2 TFUE introducía una *base jurídica específica* para la adopción de normas relativas a la protección de datos de carácter personal. Pero ya no se trataba sólo de una nueva *oportunidad* para la Comisión de utilizar este nuevo marco jurídico para rediseñar el enfoque de la normativa de protección de datos.

Más bien al contrario, la Comisión se veía *obligada*, a invitación de Consejo Europeo, a evaluar el funcionamiento de los instrumentos de la UE en materia de protección de datos y a presentar, en caso necesario, nuevas iniciativas legislativas y no legislativas (como preveía el *Programa de Estocolmo* en 2010). En idéntica dirección, la previa Resolución del Parlamento Europeo de 2009 sobre el mismo propugnaba un régimen general de protección de datos en la Unión Europea y la revisión de la Decisión Marco.

Tampoco hicieron oídos sordos las Autoridades Europeas de Protección de Datos (Article 29 Working Party) a los nuevos tiempos y, en su Dictamen de 1 de diciembre de 2009 (wp168) —*The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*[20]—, estimaron oportuna la consulta pública de la Comisión a la vista de los nuevos retos planteados por las nuevas tecnologías, la globalización y el Tratado de Lisboa. Si bien entendían vigentes los principales principios de la protección de datos, no desdeñaron la posibilidad de introducir reformas legislativas que permitieran: clarificar la aplicación de normas y principios claves como el del consentimiento y la transparencia; innovar el marco legal introduciendo nuevos principios como ("privacy by design" y "accountability"); fortalecer la efectividad del sistema modernizándolo y reduciendo la barreras burocráticas; e introducir los principios fundamentales de protección de datos en un marco global y coherente aplicable, también, a la cooperación policial y judicial en materia penal. Para el Article 29 Working Party, «the situation is not satisfactory, in particular for the third pillar ... The shortcomings of the present system require a reflection on "a comprehensive and consistent data protection framework covering all areas of EU competence". The Lisbon Treaty foresees a new horizontal approach to data protection and privacy and provides

[20] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf, págs. 1 a 28.

© UNED. *Revista de Derecho Político*
N.º 85, septiembre-diciembre 2012, págs. 13-56

for the necessary legal basis (Art. 16 TFEU) to get rid of the existing differences and divergences which prejudice a seamless, consistent and effective protection of all individuals. The main safeguards and principles should apply to data processing in all sectors, ensuring an integrated approach as well as a seamless, consistent and effective protection»[21].

Sin embargo, en este Dictamen se apostó por un modelo de revisión normativa que no sería totalmente secundado por la Comisión: se propugnó la *arquitectura de un marco global* no exento de flexibilidad acompañado de legislaciones especiales complementarias y reforzadoras de la protección en determinados sectores y materias como salud, empleo, brechas de seguridad, cooperación policial y judicial o seguridad nacional. El Dictamen admitía, incluso, la posibilidad de regulaciones nacionales adicionales que dieran respuesta a las diferencias culturales y de organización interna de los Estados sin que ello pusiera en cuestión la armonización buscada por un nuevo marco legal global e inequívoco.

Así las cosas, la nueva base jurídica del art. 16 TFUE posibilitaba la adopción de normas relativas a la protección de las personas físicas con respecto al tratamiento de datos de carácter personal por parte de los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión; y, al tiempo, permitía la adopción de normas relativas a la libre circulación de datos de carácter personal tratados bien por los Estados miembros bien por los operadores privados. Y la Comisión Europea, sorpresivamente y sin que hubiese sido postulado ni aventurado por ninguna de las instancias públicas o privadas convocadas en las consultas previas, sirviéndose de este anclaje jurídico-constitucional, apostó por la *opción reformadora más ambiciosa*, esto es, por el instrumento jurídico general que mayores dosis de armonización podía procurar al sistema europeo de protección de datos: un nuevo reglamento sustituiría a la Directiva 95/46 y una Directiva dejaría atrás a la Decisión Marco 2008/977.

C) Los nuevos *instrumentos jurídicos: Reglamento* versus *directiva y directiva* versus *decisión marco*

A) El proyecto de Reglamento General de Protección de Datos busca dar respuesta a las insistentes críticas que soportó la Directiva 95/46 y el conjunto del incipiente sistema europeo de protección de datos por parte, de forma muy especial, del mundo empresarial: una *fragmentación* de la protección de datos personales que urgía mayor *seguridad jurídica* mediante la *armonización* de las normas de protección de los datos. En particular, se advertía que la *complejidad* de esta

[21] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf, pág. 7.

normativa en materia de transferencias internacionales de datos personales constituía un impedimento sustancial en una economía planetariamente globalizada.

La Comisión Europea contempló *otros escenarios de revisión* que permitieran mejorar el mercado interior de la protección de datos, garantizar de forma más efectiva los derechos de protección de datos por los ciudadanos y, para ello, crear un marco general y coherente que alcanzara a todos los ámbitos de competencia de la Unión:

1º) La introducción de mínimas enmiendas legislativas y el recurso a comunicaciones interpretativas[22] y medidas financieras y promocionales de apoyo estratégico no parecía que fuera respuesta suficiente a la vista de los extraordinarios retos y riesgos que envuelven la protección de la privacidad en el mundo contemporáneo[23].

2º) En el extremo opuesto, la plena centralización de la protección de datos en la Unión Europea mediante normas precisas y detalladas para todos los sectores y la creación de una agencia de la Unión destinada a la supervisión y ejecución de las disposiciones hubiera encontrado amplia contestación en los Estados y difícilmente hubiera superado el test de subsidiariedad y proporcionalidad.

3º) Por último, cabía afrontar una revisión global del marco normativo que diera respuesta a los diferentes interrogantes planteados en la fase exploratoria.

Sin lugar a dudas, la elección del Reglamento como instrumento normativo para reformar el marco general de protección de datos viene a satisfacer de forma muy especial las pretensiones de la segunda estrategia expuesta si bien, al no agotar toda su potencialidad armonizadora, se ubica en una posición intermedia que, en todo caso, busca dar respuesta a la necesidad de seguridad jurídica mediante la global y coherente aplicación de la protección de datos en todo el territorio de la Unión, el efectivo ejercicio de los derechos individuales de protección de los datos y la mejora en su supervisión.

La Comisión consideró el *Reglamento* como el instrumento jurídico idóneo para regular el derecho a la protección de datos personales. Sin duda, la *aplicabi-*

---

[22] Recuérdese que la *Comunicación de la Comisión Europea al Parlamento Europeo y al Consejo, de 7 de marzo de 2007, sobre «Seguimiento del Programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos» excluía* la posibilidad de revisión de la Directiva y concluía precisamente apostando por el recurso a una *Comunicación interpretativa*: «La Comisión presentará una comunicación interpretativa sobre algunas disposiciones. Los problemas identificados al aplicar disposiciones concretas de la Directiva que puedan conducir a procedimientos formales de infracción corresponden a una comprensión de la Comisión del significado de las disposiciones de la Directiva y sobre la manera correcta de aplicarlas, teniendo en cuenta la jurisprudencia y el trabajo de interpretación llevado a cabo por el grupo de trabajo. Estas ideas se expondrán claramente en una comunicación interpretativa» (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0087:FIN:ES:DOC, pág. 9).

[23] Sobre la globalidad de estos inmensos retos, BENNETT, C.J. y RAAB, Ch. (2006): *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge.

lidad directa de un Reglamento europeo —alcance general, obligatoriedad en todos sus elementos y directamente aplicable en cada Estado miembro (art. 288 del TFUE)— lo convierte en el instrumento óptimo para *evitar la fragmentación jurídica* y garantizar mayor seguridad jurídica al definir un marco armonizado de normas básicas de protección de datos.

Ahora bien, cabe preguntarse si la elección por la Comisión Europea del Reglamento como instrumento jurídico para perfeccionar la armonización del derecho europeo de protección de datos respeta o no el *principio de subsidiariedad* que, consagrado en los Tratados, implica que, en los ámbitos en que no sean de su competencia exclusiva, la Unión intervendrá sólo en caso y en la medida en que, los objetivos de la acción pretendida no puedan ser alcanzados de manera suficiente por los Estados miembros, ni a nivel central ni a nivel regional y local, sino que puedan alcanzarse mejor, debido a la dimensión o a los efectos de la acción pretendida, a escala de la Unión. Y todo parece indicar, a la luz de los informes comunitarios a los que venimos haciendo referencia y a las reacciones a las sucesivas consultas públicas planteadas, que la respuesta debe ser necesariamente positiva ante la necesidad de adoptar iniciativas a escala de toda la Unión Europea para otorgar un mismo nivel de protección en todo su territorio al derecho a la protección de datos de carácter personal consagrado en el art. 8 CDFUE.

La experiencia aplicativa de la Directiva vigente ha venido demostrando que la ausencia de normas comunes aplicables directamente en toda la UE genera inevitablemente el riesgo de la existencia de distintos niveles de protección en todos los Estados miembros traduciéndose en: 1) diferentes derechos para los ciudadanos europeos en función de su nacionalidad; 2) restricciones en los flujos de datos personales entre los Estados miembros con distintas normas y en los flujos internacionales externos a la Unión Europea; 3) dificultades para garantizar la unidad de aplicación del Derecho europeo de protección de datos a pesar de los esfuerzos que puedan realizar —dentro de las escasas facultades previstas en la normativa— los Estados miembros y sus autoridades para organizarse a escala europea mediante los mecanismos de cooperación existentes.

Si ningún género de duda, la Unión Europea está en mejores condiciones que los Estados para garantizar de forma efectiva y coherente el mismo nivel de protección de los ciudadanos europeos cuando sus datos personales se transfieren a terceros países. Los Estados miembros no pueden ni resolver ni aliviar los obstáculos actualmente existentes derivados de la fragmentación de las legislaciones nacionales. Existe, en consecuencia, una necesidad real de establecer un marco armonizado y coherente que habilite la correcta transferencia interior y exterior de datos personales y preserve la igual garantía efectiva de un mismo derecho individual para todos y cada uno de los ciudadanos europeos.

Y conviene no perder de vista las *disfunciones previas* que han aupado la opción del RGPD: a) una deficiente y lenta trasposición de la Directiva en la mayor parte de los Estados: b) la heterogeneidad de normativa especial proyectada sobre el

régimen de la protección de datos; e) unos mecanismos de articulación de las transferencias internacionales de datos a terceros países que adolecen de burocracia, lentitud y diversidad de respuestas nacionales; f) una diversidad de modelos nacionales de Autoridades de Protección de Datos con enfoques aplicativos de la normativa bastante diferentes y con facultades de aplicación efectiva de la normativa bien distintas; e) existencia de modelos nacionales bien distintos (casi opuestos) de represión/sanción de las infracciones de la normativa de protección de datos); f) ausencia de mecanismos cooperativos de carácter operativo a nivel europeo que superen el rol meramente consultivo de las autoridades de protección de datos.

B) Y no pocos de los argumentos anteriores resultan de plena utilidad para explicar y justificar al sustitución de la Decisión Marco 2008/977 por una nueva Directiva para la protección de datos en el ámbito de la Policía y la Justicia Penal. Es evidente, de entrada, que la naturaleza de una Decisión Marco otorga a los Estados una amplia capacidad de incorporación al orden interno. Esta Decisión Marco gozaba, además, de una ámbito de aplicación muy limitado y restringido al intercambio transfronterizo de datos pero no al tratamiento de los mismos que pudieran realizar las autoridades policiales y judiciales nacionales —no que no resulta siempre tan sencillo de diferenciar.

Pero esta situación de evidente débil protección de los datos personales en el entonces llamado *tercer pilar* ha cambiado radicalmente con el Tratado de Lisboa y con la nueva base jurídica que otorga el art. 16 TFUE —al no diferenciar el ámbito policial y judicial de los restantes y, más bien al contrario, al obligar a la adopción de normas de protección de los datos también en la cooperación policial y judicial penal para preservar no sólo el intercambio transfronterizo de datos sino, también, el tratamiento de los mismos a escala nacional—. No es menos cierto, sin embargo, que el ámbito policial y judicial penal la necesidad de conciliar el inexcusable objetivo social de lucha contra la criminalidad con la protección de datos de singular *sensibilidad* aconseja la fijación de una normativa específica que atienda las peculiares circunstancias concurrentes y al tiempo de satisfacción a los omnipresentes recelos de los Estados que, aun abogando por la necesaria cooperación transfronteriza, temen perder su vocacional autonomía estatal en el ámbito policial y judicial penal. Por todo ello, en la *Declaración núm. 21* —aneja al Tratado de Lisboa— *relativa a la protección de datos de carácter personal en el ámbito de la cooperación judicial en materia penal y de la cooperación policial* se reconoce que «podrían requerirse normas específicas en razón de la naturaleza específica de dichos ámbitos». Y, en definitiva, esto explica la dualidad REPD-DPJP[24].

[24] Unas tempranas críticas a esta dualidad pueden encontrarse en el Dictamen del SEPD sobre este nuevo marco normativo: «The EDPS welcomes the proposed Regulation as it constitutes a huge step forward for data protection in Europe. The proposed rules will strengthen the rights of individuals and make controllers more accountable for how they handle personal data. Further-

© UNED. *Revista de Derecho Político*
N.º 85, septiembre-diciembre 2012, págs. 13-56

El proyecto de DPJP persigue garantizar un nivel uniforme y elevado de protección de datos en el ámbito policial y judicial penal y, con ello, incrementar la necesaria confianza mutua entre las autoridades nacionales policiales y judiciales y fomentar la libre circulación de datos y la cooperación entre las autoridades policiales y judiciales. No puede decirse que la experiencia aplicativa de la Decisión Marco de 2008 aconsejara inevitablemente su sustitución por la DPJP si atendemos exclusivamente a la casi paralela adopción de la Decisión Marco en 2008 y al inicio de la gestación de la nueva DPJP en 2009. No obstante, el vicio de origen que aconsejaba su sustitución para alcanzar una unión algo más perfecta en lo penal y judicial radicaba en la diferente naturaleza y alcance jurídico de esta tipología de normas y en el ambicioso reto que alentaba la nueva base jurídica proporcionada por el Tratado de Lisboa.

La postulación de este proyecto de DPJP de impacto a escala europea en los ámbitos policial y penal se sustenta en diversas *razones adicionales*: a) la intensificación de las necesidades de intercambio transfronterizo de datos para prevenir y luchar contra el terrorismo y la delincuencia transfronteriza; b) la necesidad adicional de incrementar la confianza entre las autoridades policiales y judiciales de los Estados miembros y superar, en consecuencia, la tradicional desconfianza y recelo presentes en este ámbito de actividad; c) el incremento de la confianza debería traducirse en una multiplicación de los intercambios transfronterizos de datos y, en consecuencia, en una mayor efectividad en la persecución del delito; d) la necesidad de cooperación entre los Estados miembros y sus autoridades policiales y judiciales resulta singularmente relevant4e ante determinadas formas delictivas que alcanzan al terrorismo o al crimen organizado y que adquieren un alcance no sólo nacional, y ni siquiera europeo, sino más bien mundial); e) la existencia de un marco uniforme y coherente para toda la Unión casi constituye *conditio sine qua non* para el mantenimiento y eficacia del diálogo trasatlántico que se inició a partir de los conflictivos *Casos PNR y Swift*[25] y que requerirá mayores desarrollos en el fu-

more, the role and powers of national supervisory authorities (alone and together) are effectively reinforced. The EDPS is particularly pleased to see that the instrument of a *regulation* is proposed for the general rules on data protection. The proposed Regulation would be directly applicable in the Member States and would do away with many complexities and inconsistencies stemming from the different implementing laws of the Member States currently in place. The EDPS is, however, seriously disappointed with the proposed Directive for data protection in the law enforcement area. The EDPS regrets that the Commission has chosen to regulate this matter in a self-standing legal instrument which provides for an inadequate level of protection, which is greatly inferior to the proposed Regulation» (*Opinion of the European Data Protection Supervisor on the data protection reform package*, 7 March 2012, pág. iv).

[25] Para ilustrar la larga historia de desencuentros USA-UE sobre el tema, sirva la lectura del Dictamen 10/2006 del Grupo de Trabajo del Artículo 29 (WP 128), 22 de noviembre de 2006, sobre el tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT) (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_es.pdf)

turo; f) las constantes iniciativas a escala europea de lucha contra la criminalidad o de vigilancia fronteriza se sustentan habitualmente en un procesamiento de datos personales (por ejemplo, el PNR europeo) que sería mejor articulado con un marco europeo consolidado. En fin, parece evidente que la UE estará en mejores condiciones para garantizar de forma efectiva y coherente el mismo nivel de protección de los ciudadanos cuando sus datos personales se transfieren a terceros países frente a la fragmentación actual de legislaciones nacionales.

D) La tendencia a la centralización europeizadora:

1. El reforzamiento de poderes de la comisión europea: actos delegados y de ejecución

El alcance general y aplicabilidad directa del RGPD no agota la intención de las autoridades europeas de alcanzar una *intensa armonización europea* limitando al máximo el margen de los Estados miembros para adaptar el RGPD a sus propias tradiciones culturales, normativas o institucionales. Junto a la existencia un marco normativo común y coherente representado por el RGPD, éste prevé la existencia de *dos mecanismos previstos* en los Tratados dirigidos a posibilitar que la Comisión pueda desarrollar normativamente numerosos aspectos del Reglamento y, al tiempo, que ejerza variadas competencias de ejecución —todas estas facultades resultarían necesarias, se entiende, para preservar la coherencia del sistema europeo y para evitar la anterior fragmentación normativa y diversidad aplicativa que redundó en inseguridad jurídica—: los *actos delegados y de ejecución*.

Así, al amparo del art. 290 TFUE, el proyecto de RGPD delega en la Comisión Europea poderes para adoptar actos delegados no legislativos de alcance general que completarían o modificarían determinados elementos no esenciales del RGPD. Esta habilitación normativa exige una delimitación expresa de los objetivos, el contenido, el alcance y la duración de esta delegación de poderes —pero reservándose el RGPD la regulación de los elementos esenciales que no podrá ser objeto de delegación alguna— y de las garantías de control adicionales atribuidas al Consejo y Parlamento Europeos[26]. Y, al amparo del art. 291 TFUE, a pesar de que los Estados miembros tienen la obligación de adoptar todas las

y del Dictamen 2/2007 del mimos Grupo de Trabajo (WP 151) de 15 de febrero de 2007 y revisado el 24 de junio de 2008, sobre información a los pasajeros sobre la transferencia de datos PNR a las Autoridades de Estados Unidos (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp151_es.pdf).

[26] Así, el art. 86 del Proyecto de RGPD, aunque inicialmente proclama que la delegación de poderes se atribuye a la Comisión por un periodo de tiempo indeterminado a partir de la fecha de entrada en vigor del Reglamento, permite la revocación en todo momento por el Parlamento Europeo o por el Consejo, de forma que la decisión de revocación pondrá término a la delegación de

medidas de Derecho interno necesarias para la ejecución de los actos jurídicamente vinculantes de la Unión, el RGPD otorga a la Comisión competencias de ejecución por entender que se requieren dichas condiciones uniformes de ejecución de este acto jurídicamente vinculante[27].

Y, desde luego, no es menor el *elenco de materias* sobre el que el art. 86 del proyecto de RGPD atribuye a la Comisión la facultad de dictar *actos de delegación* con alcance normativo general: 1') especificar las condiciones de *licitud de un tratamiento* de datos basado en la existencia de *interés legítimo* del responsable del tratamiento, para diferentes sectores y situaciones, y, particularmente, cuando se pretenda el tratamiento de datos de niños; 2') la especificación de los criterios y condiciones aplicables a los métodos de obtención del consentimiento verificable de los *niños*; 3') el tratamiento de *categorías especiales* de datos; 4') la especificación de los criterios y condiciones para las solicitudes manifiestamente excesivas y los honorarios para el ejercicio de los derechos del interesado; 5') los criterios y requisitos relativos a la información al interesado y en relación con el derecho de *acceso*; 6') el derecho al *olvido* y de *cancelación*; 7') las medidas basadas en la elaboración de *perfiles*; 8') los criterios y requisitos vinculados a la responsabilidad tratamiento y la protección de datos desde el *diseño (by design)* y por *defecto (by default)*; 9') el *encargado* del tratamiento; 10') los criterios y requisitos relativos a la documentación y la *seguridad*; 11') los criterios y requisitos para determinar la existencia de una *violación* de los datos personales y su notificación a la autoridad de control, y sobre las circunstancias en que una violación pueda afectar negativamente al interesado; 12') los criterios y condiciones para las operaciones de tratamiento que requieren una *evaluación de impacto*; 13') los criterios y requisitos para determinar un alto grado de riesgos específicos que requieren *consulta previa*; 14') especificar los criterios y requisitos aplicables a las tareas, la certificación, el estatuto, las competencias y los recursos del *delegado de protección de datos*; 15') los *códigos de conducta*; 16') especificar los criterios y requisitos aplicables a los *mecanismos de certificación*, en particular las

los poderes que en ella se especifiquen pero no afectará a la validez de los actos delegados que ya estén en vigor. Además, tan pronto como la Comisión adopte un acto delegado, lo notificará simultáneamente al Parlamento Europeo y al Consejo. Y, por último, establece que los actos delegados entrarán en vigor únicamente en caso de que ni el Parlamento Europeo ni el Consejo hayan manifestado ninguna objeción en un plazo de dos meses a partir de la notificación de dicho acto al Parlamento Europeo y al Consejo, o en caso de que, antes de que expire ese plazo, el Parlamento Europeo y el Consejo hayan informado a la Comisión de que no formularán ninguna objeción. El plazo se podrá prorrogar dos meses a instancias del Parlamento Europeo o del Consejo.

[27] Sobre el procedimiento de examen y mecanismos de control de los actos de ejecución, véase el Reglamento (UE) 182/2011 del Parlamento Europeo y del Consejo de 16 de febrero de 2011» por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión» (*Diario Oficial de la Unión Europea* L 55 de 28.2.2011, págs. 13 a 18).

condiciones de concesión y revocación, así como los requisitos en materia de reconocimiento en la Unión y en terceros países; 17') especificar los criterios y requisitos aplicables *normas corporativas vinculantes*; 18') especificar las excepciones a las *transferencias internacionales*; 19') actualización de los importes de las *multas administrativas*; 20') especificar los criterios y requisitos de las garantías del tratamiento de datos personales para los fines relativos a la salud; 21') especificar los criterios y requisitos de las garantías del tratamiento de datos personales en el *ámbito laboral*; 22') especificar los criterios y requisitos del tratamiento de los datos personales con fines de *investigación histórica, estadística y científica* y las limitaciones necesarias a los derechos de información y de acceso[28].

Y, con la indisimulada intención de garantizar unas condiciones uniformes de aplicación del RGPD, a la anterior atribución a la Comisión Europea de competencias normativo-regulatorias adicionales, el proyecto de RGPD suma un *elenco* aún mayor si cabe de *nuevas competencias ejecutivas* sobre las que la Comisión podrá dictar los correspondientes *actos de ejecución* para especificar: 1') los formularios tipo para la obtención de datos de los *niños*; 2') los procedimientos y formularios para el ejercicio de *los derechos* de los interesados; 3') los formularios normalizados sobre *información* al interesado; 4') los formularios y procedimientos normalizados sobre el derecho de *acceso*; 5') especificar el formato electrónico, normas técnicas, modalidades y procedimiento para garantizar el derecho a la *portabilidad* de los datos; 6') los requisitos, criterios y normas técnicas relativos la protección de datos desde el *diseño y por defecto* y su documentación; 7') los requisitos específicos para garantizar la *seguridad* de los datos impidiendo cualquier acceso no autorizado, evitando cualquier forma no autorizada de comunicación, lectura, copia, modificación, supresión o cancelación de datos personales y garantizando la verificación de la legalidad del tratamiento.; 8') el formato estándar y los procedimientos para la *notificación de una violación* de los datos personales a la autoridad de control y su comunicación al interesado; 9') las normas y procedimientos para la *evaluación de impacto*; 10') los formularios y procedimientos de *autorización y consulta previa*; 11') *códigos de conducta* y normas técnicas y mecanismos de *certificación y sellos*; 12') el *nivel adecuado* de protección de un tercer país, un territorio, un sector en determinado tercer país o una organización internacional y las *normas corporativas vinculantes*; 13') las comunicaciones no autorizadas por el Derecho de la Unión; 14') formato y procedimiento de *asistencia mutua* entre autoridades de control; 15') las *operaciones conjuntas* de las autoridades de control; 16') las decisiones en el marco del mecanismo de *coherencia*[29].

[28] Los artículos del proyecto de RGPD en los que se faculta a la Comisión para dictar estos «actos delegados» son los siguientes: 6.7, 8.3, 9.3, 12.5, 14.7, 15.3, 17. 9, 20. 6, 22.4, 23. 3, 26. 5, 28.4, 30.3, 31.5, 32.5, 33.6, 34.8, 35.11, 37.2, 39.2, 43.3, 44.7, 79. 6, 81.3, 82. 3, y 83.3.

[29] Los artículos del proyecto de RGPD en los que se atribuye a la Comisión competencia para dictar estos «actos ejecutivos» son los siguientes: 8.4, 12.6, 14.8, 15.4, 18.3, 23.4, 28.6, 30.4, 31.6, 32.6, 33.7, 34.9, 39.3, 41.4, 43.4, 55.10 y 62.

Llama poderosísimamente la atención el giro copernicano que está próximo a sufrir el modelo regulatorio y ejecutivo del derecho a la protección de datos a la vista de las nuevas competencias normativas y ejecutivas que el proyecto de RGPD pretende transferir a la Comisión Europea. Y ello, especialmente, si lo ponemos en relación con las tímidas, casi marginales, competencias ejecutivas —que no normativas— de que goza todavía actualmente la Comisión al amparo de la Directiva 95/46 exclusivamente en materia de *transferencias internacionales de datos* a terceros países (y, singularmente, en la declaración de adecuación de terceros países y en la definición de cláusulas contractuales)[30].

2. Un regimen sancionador común: el reforzamiento de la estrategia represiva

La verdadera armonización de la normativa europea de protección de datos exige un régimen sancionador común como bien lo demuestra la nefasta experiencia anterior. La Directiva 95/46 apenas imponía a los Estados la obligación de adoptar medidas adecuadas para garantizar su plena aplicación y determinar, en particular, las sanciones aplicables en caso de incumplimiento. Pero este mandato de la Directiva se tradujo en una pavorosa asimetría europea sobre la que, sin duda, se ha construido una *doble velocidad europea* en el ritmo de garantía efectiva del derecho a la protección de datos personales. Siendo bien escasos los Estados miembros que contemplan un régimen sancionador económico disuasorio —a la cabeza, sin duda, desde el principio, España[31] e incorporados, du-

[30] http://ec.europa.eu/justice/data-protection/document/international-transfers/index_en.htm

[31] Una completa visión sobre el tema y, en particular, sobre el principio de proporcionalidad, puede consultarse en AAVV (2008): *La potestad sancionadora de la Agencia Española de Protección de Datos*, AEPD-Aranzadi, Pamplona. Buen ejemplo de este diferencial sancionador puede encontrarse en RALLO, A: «Development of the Agency's audit and sanctions policy in Spain. Trends regarding investigations, fines and other sanctions», *23rd Annual International Conference*, July 5-7-2010, St. John's College, Cambridge, UK, págs. 1 a 13. Otras intervenciones del autor sobre la relevancia de la actuación reguladora de la AEPD: «El papel del regulador en la protección de la intimidad. Perspectiva española», *Cumbre de Privacidad de la IAPP*, Washington, marzo 2008; «La protección de los datos personales en un mundo globalizado: el modelo español», II Seminario Internacional de Acceso a la Información y Protección de Datos Personales, México, noviembre 2008; «Instrumentos y estándares para métodos de control e inspección. Situación en España», *Taller de Autoridades de Estados Plurales y Federales*, Berlín, marzo 2009; «The International context of regulation», *Spring Conference of European Privacy and Data Protection Commissioner's*, Edimburgo, abril 2009; «What's on the regulatory agenda», *32nd International Conference of Data Protection and Privacy Commissioner's*, Jerusalen, octubre 2010; «La AEPD, Autoridad Independiente para la Protección de Datos Personales», *VI Seminario Internacional Jueces y Estado de Derecho*, Santiago de Chile, noviembre 2010; «The regulator's Priorities. View of the Spanish DPA», *IAPP Europe Data Protection Congress,* París, noviembre 2010.

rante los últimos años, otros Estados como Francia o Reino Unido—, la realidad europea general mostraba un páramo de flagrante impunidad ante las infracciones crecientes.

Por ello no puede extrañar —aunque resulte ciertamente llamativa y loable la ambición regulatoria evidenciada en este punto por el proyecto de RGPD— que el nuevo derecho europeo de la protección de datos se construya sobre un reforzamiento efectivo del régimen de sanciones a través, por un lado, de su generalización en todo el territorio de la Unión Europea y, de otro, de su naturaleza ciertamente actualizada y disuasoria aplicable a todo tipo de entidad pública y privada. Además, a través del *mecanismo de coherencia*, se busca armonizar, incluso, el régimen aplicativo en cada Estado miembro del régimen de sanciones económicas evitando divergencias en la aplicación de las mismas.

Así, aunque corresponda a los Estados miembros establecer normas sobre las sanciones aplicables a las infracciones previstas en el RGPD y adoptar todas las medidas necesarias para garantizar su cumplimiento, deberá *notificar* a la Comisión las disposiciones legislativas que adopte a tal efecto y, en todo caso, las sanciones deberán ser *efectivas, proporcionadas y disuasorias* en todos los casos. El importe de las multas se fijará teniendo en cuenta la naturaleza, gravedad y duración de la infracción, la intencionalidad o negligencia en la infracción, el grado de responsabilidad de la persona física o jurídica, la reincidencia, las medidas de carácter técnico y organizativo y los procedimientos aplicados por los responsables, el grado de cooperación con la autoridad de control para reparar la infracción.

En primer lugar, aun estando las Autoridades nacionales de control facultadas para realizar *advertencias o amonestaciones*, el proyecto de Reglamento prevé la existencia de un *apercibimiento* previo en el caso de un primer incumplimiento no deliberado del RGPD, que evitará la imposición de sanción en los siguientes *supuestos*: a) si quien realiza el tratamiento de datos personales es una persona física sin interés comercial; b) o si de trata de una empresa o una organización con menos de 250 personas empleadas que trate datos personales únicamente como actividad auxiliar de su actividad principal[32].

Pero, en segundo lugar, la autoridad de control podrá imponer *rigurosas multas* que recorrerán una *escala* de *tres niveles* atendiendo a si el infractor es una *persona física* (hasta 250.000, 500.000 o 1.000.000 de Euros) o una *empresa* (hasta el 0,5 %, 1% o 2% de su volumen de negocios anual a nivel mundial) y siempre que la infracción se haya cometido de forma deliberada o por negli-

[32] Resulta inevitable concluir que esta regulación parece tomar como referencia la reforma del régimen sancionador previsto la *Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal operada por la* Disposición final quincuagésima sexta de la Ley 2/2011, de 4 de marzo, de Economía Sostenible.

© UNED. *Revista de Derecho Político*
N.º 85, septiembre-diciembre 2012, págs. 13-56

gencia. Sí las cosas, puede observarse que el proyecto de RGPD con buen criterio, diferencia el régimen sancionador aplicable a un particular del que resultará predicable de una empresa y, sin lugar a dudas, el rigor de las sanciones económicas previstas adorna la exigencia disuasoria. Además, la responsabilidad de infractor vendrá igualmente modulada por su grado de intencionalidad pero, en todo caso, para su exigibilidad de se requiere de voluntariedad o negligencia.

La tipología de infracciones previstas se construye sobre la existencia de tres niveles de gravedad en los que cabe diferenciar: a) *infracciones leves* referidas a conductas que afectan, básicamente, a la deficiente facilitación documental, temporal o económica de los derechos; b) *infracciones graves* que versarían sobre la garantía efectiva de los derechos de información, trasparencia, acceso, rectificación, olvido, cancelación, portabilidad y oposición; así como a la determinación de responsabilidades, a la conservación de documentación o el respeto a determinadas normas sobre libertad de expresión, ámbito laboral o tratamiento de datos con fines de investigación histórica, estadística y científica; c) *infracciones muy graves* por vulneración de principios básicos sobre legitimación del tratamiento de datos, el consentimiento, categorías especiales de datos, elaboración de perfiles ausencia de políticas internas o de medidas adecuadas de protección, incumplimiento de las obligaciones impuestas por el responsable, notificación de una violación de datos a la autoridad de control o al interesado, ausencia de evaluación del impacto o de consulta previa a la autoridad de control, no designación de un agente de protección de datos, uso indebido de sellos y marcas, transferencias internacionales de datos, desobediencia al requerimiento o prohibición de la autoridad de control, desatender las obligaciones de cooperación con la autoridad de control o vulneración del secreto profesional.

3. *Viejas* autoridades europeas pero *nuevos* poderes: Consejo Europeo de Protección de Datos y supervisor europeo de protección de datos

El proyecto de RGPD crea un nuevo Consejo Europeo de Protección de Datos (CEPD) que, aunque formalmente aparenta sólo sustituir el anterior Grupo de Trabajo previsto en el art. 29 de la Directiva 95/46 (*art. 29 WP*), adquiere una nueva muy relevante posición institucional a la vista de la profunda centralización europea que preside la nueva normativa europea de protección de datos. El CEPD estará compuesto por el comisionado de cada autoridad nacional de control y por el Supervisor Europeo de Protección de Datos (SEPD). Para preservar y reforzar la independencia del nuevo CEPD, la Comisión Europea, aunque tendrá derecho a ser permanente informada y a participar en sus actividades y reuniones, abandona sus anteriores funciones como *secretaría permanente* del Grupo de Trabajo —que pasan a ser ejercidas, al igual que una *Vicepresidencia permanente*, por el SEPD—.

El elenco de funciones del CEPD recorre todo el ámbito regulatorio del RGPD de forma que, tras la apariencia básica de órgano consultivo, expande significativamente su potencialidad pues le corresponde «velar por la aplicación coherente» del RGPD y, a tal fin, asesorará a la Comisión sobre «toda cuestión relativa a la protección de datos» personales en la Unión; examinará «cualquier cuestión relativa a la aplicación del presente Reglamento»; emitirá directrices, recomendaciones y mejores prácticas «dirigidas a las autoridades nacionales de control» para promover la aplicación coherente del RGPD; dictaminará sobre los proyectos de decisión de las autoridades de control con arreglo al mecanismo de coherencia; y promoverá la cooperación, intercambios de información, documental y de personal y de programas de formación.

Resulta singularmente llamativa la *nueva posición institucional* que pasa a ocupar el Supervisor Europeo de Protección de Datos frente a la que le correspondía en el marco de la Directiva 95/46. Tradicionalmente, el *Article 29 WP* fue concebido como *órgano de coordinación* de las Autoridades nacionales de control que, en el marco de la Directiva, ostentaban la plana competencia aplicativa del derecho europeo de protección de datos. Tras su creación, el SEPD pasó a integrarse en el mismo si bien con un perfil institucional prefijado por sus limitadas competencias regulatorias sobre las instituciones comunitarias. Sin embargo, la extraordinaria agenda comunitaria del último lustro en protección de datos y su propio desarrollo institucional ha engrandecido la posición del SEPD convirtiéndolo *de facto* en una *secretaria bis* —junto con la que oficialmente ejerce la Unidad de Protección de Datos de la Comisión y con la que oficiosamente desempeña la Autoridad nacional que ostenta la Presidencia del Article 29 WP— que el proyecto de RGPD viene a oficializar e, incluso, a reforzar al otorgarle la condición de *Vicepresidente nato* del CEPD. La nueva secretaría del CEPD que acogerá el SEPD comportará la gestión diaria de las necesidades logísticas del CEPD pero, también, y en particular, la «preparación y redacción de los dictámenes y textos» adoptados por el CEPD. Con todo, si tenemos en cuenta el reconocimiento normativo de estas nuevas competencias del SEPD, su propia relación bilateral con una Comisión Europea poderosamente reforzada en competencias y las inevitables sinergias centrípetas que genera el funcionamiento de un órgano intergubernamental como el CEPD, cabe intuir que el SEPD *de facto* se convertirá funcionalmente en una *Agencia Europea de Protección de Datos*.

4. Los nuevos procedimientos de cooperación (asistencia mutua e investigaciones conjuntas) y coherencia como mecanismos efectivos de armonización europea

El incisivo nuevo modelo de armonización del derecho europeo de protección de datos que venimos ilustrando descansa, además, sobre una transformación efectiva del estatuto, funciones y relaciones intergubernamentales de las Auto-

ridades nacionales de control en una doble dirección: a) por un lado se homogeniza su diseño institucional (especialmente, en lo referido a sus funciones y poderes); b) y, por otro, se crean nuevos mecanismos europeos de *coordinación efectiva* entre ellas que, en la práctica, supondrán sustraerles ámbitos nacionales de decisión para forjar una armonizada aplicación del RGPD en el conjunto de la Unión.

El proyecto de RGPD diseña un *modelo de Autoridad Nacional de Control* que poco dista del ya existente hasta la hecha en cuanto al estatuto institucional concretado en la legislación nacional conforme a las *notas siguientes*: opción nacional única o plural de autoridades públicas de control; total independencia [33] y proscripción de instrucciones externas; régimen de incompatibilidades; suficiencia de recursos humanos, técnicos, materiales y financieros adecuados; personal propio nombrado por la autoridad de control; control financiero y presupuestos anuales propios; nombramiento gubernamental o parlamentario con mandato temporal fijo no inferior a cuatro años; renovable o no.

Sin embargo, la gran apuesta armonizadora del proyecto de RGPD se cierne sobre el *nuevo y exhaustivo diseño de funciones y poderes* de las autoridades nacionales de control de entre los que, en particular, destacan las *facultades de enforcement*: a) conocer e investigar todas las reclamaciones individuales o *colectivas* que se le presenten e informar a los interesados; b) compartir información con otras autoridades de control, prestar asistencia mutua y garantizar la coherencia aplicativa y el cumplimiento del RGPD; c) evaluar el impacto en la protección de datos personales de las tecnologías de la información y la comunicación y de las prácticas comerciales; c) notificar la violación de datos personales y ordenar su subsanación; d) ordenar que atiendan las solicitudes de ejercicio de los derechos; e) ordenar que se le facilite cualquier información útil para el desempeño de sus funciones; f) formular advertencia o amonestación al responsable o al encargado del tratamiento; g) ordenar la rectificación, supresión o destrucción de datos ilícitamente tratados; h) prohibir temporal o definitivamente el tratamiento; i) suspender los flujos internacionales de datos. Y, a los efectos de garantizar efectivamente el ejercicio de estas facultades de *enforcement*, se confiere a cada autoridad de control poderes de investigación que le permitan el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones y el acceso a los locales y equipamientos afectados. Y, como corolario a este reforzado modelo de garantía efectiva, las autoridades de control no sólo podrán ejercer acciones jurisdiccionales, sino que estarán facultadas para sancionar las infracciones administrativas a las que ya nos hemos referido.

[33] Sin duda, la Comisión Europea ha tenido muy en cuenta el caso resuelto el 9 de marzo de 2010 por el Tribunal de Justicia de la Unión Europea (Commission / Germany, Case C-518/07, ECR 2010 p. I-1885) en el que se censuraba a Alemania por no cumplir con las exigencias de independencia impuestas por la Directiva 95/46 a las Autoridades Nacionales de Control.

Ahora bien, si de lo anterior parece deducirse ineluctablemente un reforzamiento de los poderes de supervisión interna de las Autoridades nacionales de control —de los que la gran mayoría de ellas adolecen hasta la fecha—, lo cierto es que el proyecto de RGPD debilita notablemente estas expectativas al someterlos a *estrictos mecanismos y reglas de vigilancia europea* como los siguientes:

En primer lugar, si bien las Autoridades nacionales de control gozan de *plena competencia* en el territorio de su propio Estado miembro, cuando el tratamiento de los datos en un país lo realice una empresa activa en varios Estados miembros, la competencia para controlar sus actividades corresponderá a la autoridad de control del Estado miembro «en que esté situado el *establecimiento principal* del responsable o del encargado»; lo que, significa, en la práctica, sustraer buena parte de sus competencias de control a las Autoridades nacionales sobre el tratamiento de datos efectuados en sus respectivos países. Lo que, por lo demás, implica que las autoridades de control de los Estados en los que se residencian buena parte de las empresas multinacionales por tradición o trascendencia histórica o económica (Reino Unido, Francia o Alemania) o por estrategia empresarial (Irlanda) absorberán el ejercicio efectivo de las competencias de control de buena parte de los restantes Estados. Máxime si tenemos en cuenta que el proyecto de RGPD declara que toda medida ejecutoria adoptada por la autoridad de control de un Estado miembro se ejecutará en todos los Estados miembros afectados —aunque, ciertamente, carecerá de validez jurídica y no gozará de dicho valor ejecutivo si la autoridad de control no presenta el proyecto de medida al mecanismo de coherencia—. De ahí que, necesariamente, como estamos viendo, el proyecto de RGPD haya buscado superar las asimetrías existentes en los poderes de las Autoridades de control y establecer mecanismos de coordinación que eviten las disfunciones y recelos que esta regla competencial pudiera generar [34].

[34] Para entender la relevancia de estas nuevas disposiciones es indispensable ubicarlas en un contexto previo. Durante las últimos años las grandes multinacionales del sector de Internet (por ejemplo Google o Facebook) han ubicado su sede legal europea en Irlanda por razones a todas luces evidentes (entre otras, pero de forma especial, la menor presión fiscal del país y, particularmente, su legislación nacional de protección de datos —que, aun transponiendo la Directiva 95/46, adolece de un muy débil régimen sancionador y apuesta por un modelo proactivo de garantía del derecho a la protección de datos—). Con la eclosión de problemas para la privacidad derivados de los servicios de estas empresas de Internet, éstas han reivindicado su ubicación principal en Irlanda para rehuir el régimen investigador/sancionador del resto de países europeos (y, específicamente, de los más activos como España, Francia o Alemania) a lo que lsus Autoridades Nacionales de Protección de Datos han respondido con inevitable recelo ante la desprotección que entienden que se les provoca a los derechos de sus nacionales. A todo ello pretende dar respuesta la potente apuesta armonizadora del nuevo Proyecto de RGPD. Con anterioridad a la presentación de este último, una primera respuesta a esta problemática sobre la determinación de la ley aplicable al tratamiento de datos intentó proporcionarse en el Dictamen 8/2010 del Grupo de Trabajo del Artículo 29 (WP 179), adoptado el 16 de diciembre de 2010, sobre Derecho aplicable (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_es.pdf).

En segundo lugar, el proyecto de RGPD establece un *deber de asistencia mutua* entre Autoridades nacionales de control consistente en la obligación de facilitarse información útil y prestarse asistencia mutua —conforme a los formatos y procedimientos establecidos por la Comisión— sobre las solicitudes de autorización y consulta previas, las inspecciones, el curso de una investigación o la apertura de expedientes y su evolución; de forma que las autoridades de control no podrán rehuir dicho deber de asistencia debiendo informar de los resultados progresos o medidas adoptadas. Y ello por cuanto, en caso de no hacerlo en el plazo previsto, la autoridad de control solicitante podría adoptar medidas provisionales en su territorio y someter el caso al CEPD siguiendo el procedimiento de coherencia.

En tercer lugar, el nuevos sistema europeo de protección de datos busca dar respuesta efectiva a los nuevos retos que plantea la garantía efectiva de este derecho y, en particular, a la dimensión trasnacional[35] del mismo que obliga a establecer mecanismos reales de vigilancia y control que superen las barreras nacionales[36]. Así, el proyecto de RGPD prevé la existencia de *investigaciones conjuntas*[37]

[35] Un buen ejemplo de esta nueva realidad lo constituye el acuerdo de las Autoridades Europeas de Protección de Datos reunidas en sesión plenaria del Grupo de Trabajo del Artículo 29 en Bruselas los días 1 y 2 de febrero de 2012, para la realización de un análisis conjunto y coordinado de las nuevas políticas de privacidad presentadas por Google. La Carta de la Presidenta de la CNIL de 3 de febrero de 2012 dirigida a Google a iniciativa del Grupo de Trabajo del Artículo 29 les informaba de la apertura de una investigación por dicha Autoridad Nacional y de su liderazgo en el proceso de análisis de la nueva Política de Privacidad de Google: «En nombre de las autoridades de protección de datos en la UE, se ha decidido llevar a cabo una investigación después de este primer análisis de los detalles públicos más relevantes». Un antecedente a estas acciones coordinadas lo podemos encontrar en la Carta suscrita por las Autoridades de Protección de Datos —y presentada por las de España, Canadá e Israel en Washington el 20 de abril de 2010— dirigida al director ejecutivo de Google a raíz de los problemas suscitados por el lanzamiento de Google Buzz. En esta dirección de coordinación se inscribe la Resolución adoptada por la Conferencia Internacional de Autoridades de Protección de datos celebrada en México el 1 de noviembre de 2011 sobre «La coordinación para la aplicación legal de la privacidad de forma internacional».

[36] Sin lugar a dudas, el caso de referencia que ha alumbrado la necesidad de articular formalmente investigaciones conjuntas es el denominado *Google Street View*. Al igual que otras muchas Autoridades de Protección de Datos (no sólo europeas), la Agencia Española de Protección de Datos abrió el 19 de mayo de 2010 una investigación para determinar si Google había vulnerado la normativa española de protección de datos al captar y almacenar sin consentimiento datos de localización de redes WI-FI —y datos de tráfico asociados a esas redes— al fotografiar las calles de distintas ciudades para la aplicación Street View. La pluralidad de investigaciones abiertas, las dificultades técnicas del análisis, la relación bilateral de cada Autoridad con la compañía Google, la heterogeneidad de resoluciones (sancionatorias o no) ofrecieron un paisaje poco edificante que demuestra la imperiosa necesidad de una acción investigadora/sancionadora global.

[37] Estas previsiones dan por superado, afortunadamente, el limitado alcance de las llamadas «acciones conjuntas de control» que hasta la fecha venía realizando el Grupo de Trabajo del Artículo 29 y que, a modo de ejemplo, pueden consultarse en su Informe 1/2010 adoptado el 13 de julio de 2010

de las Autoridades de control operadas, incluso, por personal de varias autoridades de control de otros Estados. Así, la autoridad de control competente deberá invitar a la autoridad de control de cada uno de esos Estados miembros a tomar parte en las tareas de investigación conjuntas y, en su calidad de autoridad de control de acogida, podrá conferir competencias de investigación al personal de otras autoridades que participen en operaciones conjuntas bajo su orientación y en presencia de sus miembros. Y en caso de que la autoridad de control de origen no formule la invitación referida a las restantes, éstas podrán adoptar medidas provisionales en el territorio de su Estado y comunicarlas al CEPD y a la Comisión para su tramitar el mecanismo de coherencia.

En cuarto lugar, el *mecanismo de coherencia* previsto en el proyecto de RGPD constituye seguramente la *auténtica cláusula de salvaguarda* del nuevo sistema europeo de protección de datos que se pretende global y efectivamente armonizado. El RGPD, lejos de darse por satisfecho con su aplicabilidad directa, con la exhaustiva normación de todo el sistema de garantías efectivas y con la centralización de poderes en todas las instancias europeas (CE, CEPD y SEPD), ha querido proscribir cualquier intento asimétrico a nivel nacional en el plano aplicativo imponiendo un *mecanismo de coherencia* que, supuestamente deducido de las exigencias de cooperación, va destinado a imponer efectivamente, en los casos concretos, respuestas europeas a los disensos que puedan producirse en el nivel nacional.

El mecanismo de coherencia se construye sobre las siguientes *reglas básicas*:

1º) Sobre los *supuestos* que lo activan, las autoridades nacionales de control tienen la obligación de comunicar al CEPD y a la Comisión todo proyecto de medida que afecte a actividades en varios Estados miembros, a la libre circulación de datos personales, a los tratamientos objeto de consulta previa, a las cláusulas tipo relativas a transferencias internacionales o a la aprobación de normas corporativas vinculantes. Además, las autoridades de control o el CEPD podrán solicitar que cualquier asunto sea tratado por el mecanismo de coherencia una autoridad de control no presente dichos proyectos de medida o no cumpla con el deber de asistencia mutua o con las previsiones relativas a las investigaciones conjuntas. Y, sin condiciones adicionales, la Comisión podrá solicitar que cualquier asunto sea tratado por este mecanismo de coherencia.

2º) Tras el correspondiente intercambio de información, el CEPD emitirá un *dictamen* sobre el asunto frente al cual al autoridades de control concernidas comunicarán si mantienen o modifican su proyecto de medida. Además, la Comi-

(WP 172) sobre la segunda acción conjunta de control: *Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive* (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_fr.pdf).

sión podrá adoptar, para garantizar la aplicación correcta y coherente del RGPD, un dictamen sobre los asuntos planteados mediante el mecanismo de coherencia que deberá ser tenido en cuanta por autoridad de control afectada e informar a la Comisión y al CEPD sobre su intención de mantener o modificar su proyecto de medida —debiendo abstenerse de actuar entretanto—.

3º) Si una autoridad de control no se atiene al dictamen de la Comisión o cuando ésta perciba una aplicación incoherente del RGPD, la Comisión podrá suspender la adopción del proyecto de medida nacional a fin de aproximar posiciones o para adoptar un *acto de ejecución* que zanje la disputa planteada a través del mecanismo de coherencia —especialmente cuando una autoridad de control no haya presentado un proyecto de medida o haya anunciado que no tiene intención de atenerse al dictamen de la Comisión—. Es más, por razones de imperiosa urgencia debidamente justificadas en los intereses de los interesados, la Comisión podrá adoptar inmediatamente actos de ejecución inmediatamente aplicables.

En definitiva, el mecanismo de coherencia otorga a la Comisión Europea la *llave*[38] que cierra el círculo de la centralización del derecho a la protección de datos entorno a las instituciones europeas: la Comisión Europea no sólo gozará de poderes normativos delegados de desarrollo del RGPD y de poderes ejecutivos de alcance general para la definición de procedimientos y documentación sino que tendrá la posibilidad de resolver conflictos concretos generados por la aplicación del Reglamento en el nivel nacional.

E) Frente al tsunami tecnológico, más protección y nuevos derechos: *infancia, información, transparencia, olvido, y portabilidad. Reclamaciones colectivas, jurisdicción nacional y aplicabilidad de la legislación europea como nuevas garantías*

El tsunami tecnológico que vive la sociedad actual constituye, sin duda, unas de las principales preocupaciones del legislador europeo. Desde que se aprobó la Directiva 95/46, la nueva sociedad de la información y del conocimiento ha adquirido un desarrollo inimaginable y ha provocado un impacto insospechado dos décadas atrás en el flujo de información personal[39]. Y, lo que resulta aún más re-

[38] Muy crítico con este diseño se muestra el Supervisor Europeo de Protección de Datos («The main negative elements of the proposed Regulation are: … the role of the Commission in the consistency mechanis») y, he hecho, propuso su concreta revisión para limitar «the power of the Commission by deleting the possibility to overrule a decision of a national supervisory authority in a specific matter through an implementing act» (*Opinion of the European Data Protection Supervisor on the data protection reform package*, 7 March 2012, págs. V y 72).

[39] Sobre la trascendencia de la coyuntura actual, RALLO, A. (2010): «Protecting privacy in a fast, evolving more complex digital world», *Trends in glogal Communications: riding the next digital wave* (Barcelona: International Institute of Communications, 2010), 1-10 e «Internet of the

levante, las categorías tradicionales sobre las que se asienta el derecho a la protección de datos han evidenciado su debilidad y exigen una adecuación a los tiempos actuales que constituyen uno de los principales retos del proyecto de RGPD al actualizar su aplicación al nuevo entorno tecnológico y al crear *nuevos derechos digitales*.

En primer lugar, el proyecto de RGPD profundiza en las necesidades de *transparencia e información* al ciudadano al asumir que el flujo masivo de datos en el mundo digital y sus dificultades para perseguir y reparar las vulneraciones del derecho a proteger los datos requiere una mejora extraordinaria en los procesos de otorgamiento del consentimiento. El RGPD postula un consentimiento explícito permita una manifestación libre, específica e informada de la voluntad del interesado[40], y que garantice que la persona es consciente de que está dando su consentimiento, incluso mediante la selección de una casilla de un sitio web en internet. Esta obligación de ofrecer información transparente y de fácil acceso y comprensión se inspira especialmente en la Resolución de Madrid relativa a estándares internacionales sobre protección de datos personales y privacidad. El *principio de transparencia* exige que toda información sea fácilmente accesible y comprensible y que se utilice un lenguaje sencillo y claro, especialmente en entornos como la publicidad en línea o cuando los destinatarios son objeto de especial protección como los *niños*.

En segundo lugar, la *infancia*[41] constituye un grupo social sometido a un especial riesgo en el mundo *online* a causa de su masivo acceso a Internet y de la obtusidad de sus reglas y políticas de privacidad. Por ello, el RGPD se ocupa de los menores para otorgarles especial protección ante la oferta directa de servicios de la sociedad de la información destinada a los niños. Así, la obtención de datos de niños menores de 13 años solo será lícita si es autorizada por el padre o tutor

---

Things: the importance of privacy oriented strategies», *The 2nd Internet Annual of Things Europe*, Brussels, 2010, 1-8. Véase http://www.theinternetofthings.eu/. Sobre este último fenómeno, véase el Dictamen 9/2011 adoptado por el Grupo de Trabajo del Artículo 29 (WP 180) adoptado el 11 de febrero de 2011 relativo a la propuesta revisada de la Industria para un Marco de Evaluación del Impacto sobre protección de datos en las aplicaciones basadas en la Identificación por Radiofrecuencia (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_es.pdf).

[40] Sobre el alcance de estas condiciones, véase el Dictamen 15/2011, adoptado por el Grupo de Trabajo de Artículo 29 (WP 187), sobre la definición del consentimiento (http://ec.europa.eu/justice/data protection/article-29/documentation/opinion-recommendation/files/2011/wp188_es.pdf).

[41] De las dificultades —y, por lo tanto, del mérito de la propuesta de la Comisión— para abordar la protección online de los menores, da buena cuenta el limitado alcance —en plena efervescencia de la problemática del acceso masivo de los menores a los servicios de Internet— del Dictamen 2/2009 del Grupo de Trabajo del Artículo 29, adoptado el 11 de febrero de 2009 (WP 160), sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas) (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_es.pdf).

pero, para evitar las habituales prácticas fraudulentas, deberán adoptarse esfuerzos razonables para recabar un consentimiento verificable, al tenor de la tecnología disponible. Esta previsión está directamente embebida de las legislaciones norteamericana (13 años) y española (consentimiento verificable a tenor de la tecnología) pero no resuelve sus numerosos problemas aplicativos en Internet para lo cual la Comisión se reserva dictar actos delegados, que especifiquen los criterios y condiciones aplicables a los métodos de obtención del consentimiento verificable, y actos ejecutivos sobre formularios normalizados con métodos específicos de obtención del mismo.

En tercer lugar, el RGPD reconoce, como concreción en el ámbito digital del tradicional derecho de cancelación, el *derecho al* olvido[42], esto es, el derecho de toda persona a la cancelación y no tratamiento de los datos personales cuando ya no sean necesarios para los fines para los que fueron recogidos, cuando los interesados hayan retirado su consentimiento para su tratamiento, cuando se haya agotado el plazo previsto de conservación o cuando se opongan al mismo. Este derecho es estima especialmente aplicable a aquellos supuestos en que los interesados hubieran dado su consentimiento siendo niños, de forma que no fueran enteramente conscientes de los riesgos para su privacidad futura y más tarde quisieran suprimirlos (lo que resulta significativamente más relevante en Internet). La obligación de estos datos no sólo genera obligaciones a quien los hubiera recabado inicialmente sino que —y, de nuevo, pensemos en Internet y, particularmente, en las redes sociales[43] y los motores de búsqueda[44]— cuando el responsable hubiera hecho públicos los datos, adoptará todas las medidas razonables, incluidas las técnicas, para informar a terceros que estén tratando dichos datos de la petición de supresión de «cualquier enlace» a esos datos o copia o réplica de los mismos. A todos estos efectos, se deberán implementar mecanismos para garantizar que se respetan los plazos fijados para la supresión de datos y para el examen periódico de la necesidad de conservar los datos. Al *derecho olvido* se le oponen, sin embargo, como *límites*: la li-

[42] Unas breves reflexiones en RALLO, A. (2010): «A partir de la protección de Datos. El derecho al olvido y su protección», *TELOS. Cuadernos de Comunicación e Innovación* (*Los derechos fundamentales en Internet)*, págs. 104 a108 y en la intervención sobre «Search engines and rights of erasure and objection» en la sesión pública de la Comisión de Derechos Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (Bruselas, Enero, 2008). Un recorrido más general en WEBER, R. (2011): *The Right to Be Forgotten: More Than a Pandora's Box?*, 2, JIPITEC (http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8).

[43] Dictamen 5/2009 sobre las redes sociales en línea del Grupo de Trabajo del Art. 29 (01189/09/ES WP 163). http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_es.pdf)

[44] Al respecto, véanse la *Declaración sobre buscadores de Internet* publicada el 1 de diciembre de 2007 por la Agencia Española de Protección de Datos y el Dictamen adoptado el 4 de abril de 2008 por Grupo de Trabajo del Artículo 29 (WP 148) 1/2008 *sobre cuestiones de protección de datos relacionadas con motores de búsqueda* (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_es.pdf).

bertad de expresión, el interés publico relativo a la salud pública, los fines de investigación histórica, estadística y científica y las obligaciones legales europeas o nacionales que impongan la conservación de datos —ahora bien, estas obligaciones deberán respetar el contenido esencial de este derecho y ser proporcionales a la finalidad legítima perseguida—. Téngase, finalmente muy en cuenta, que el RGPD reserva a la Comisión la facultad de dictar *actos delegados* para fijar los criterios y requisitos del derecho al olvido según sectores y situaciones, las condiciones para la supresión de enlaces, copias o réplicas de datos procedentes de servicios de comunicación de acceso público.

En cuarto lugar, un nuevo derecho instrumental de protección de datos aflora, como auténtica novedad, en el proyecto de RGPD: *el derecho a la portabilidad de los datos*. Su alcance no puede entenderse cubierto —como sí ocurre con el derecho al olvido en relación con el derecho de cancelación u oposición— por el tradicional derecho de acceso sino que ambiciona dar respuesta a una problemática planteada por los más exitosos servicios de la era digital: las redes sociales[45]. El derecho a la portabilidad pretende que, sin dificultades que aborten tal posibilidad, los usuarios de una red social *on line* puedan cancelar sus cuentas abiertas en un concreto portal y trasladar todo el historial generado en su cuenta a una nueva red social. Esto es, que, cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el interesado tenga derecho a obtener del responsable del servicio online una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos; así como, tendrá derecho a transmitir dichos datos y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos de la red social de la que se retiren los datos personales. De la trascendencia de este nuevo derecho da buena cuenta una realidad en la que miles de millones de usuarios de redes sociales acumulan en sus cuentas on line un auténtico historial de vivencias y relaciones personales y sociales que resultaría abortado si se les negara tal derecho a la portabilidad o generaría un insufrible sometimiento del usuario a los designios de la red social de acogida que resultaría difícilmente conciliable con los estándares básicos de protección de datos y de su misma dignidad.

[45] Un recorrido amplio de las problemáticas vinculadas al fenómeno puede encontrarse en las diversas contribuciones recogidas en la obra colectiva coordinada por RALLO, A. y MARTINEZ, R. (2010): *Derecho y redes sociales*. Pamplona: Civitas-Thomson Reuters. También, GREGORIO, C. y ORNELAS, L. (2011): *Protección de datos personales en las redes sociales digitales: en particular de niños y adolescentes*, IFAI-IFI, México y GARCIA SANZ, R.M. (2010): «Redes sociales online: fuentes de acceso público o ficheros de datos personales privados (Aplicación de las Directivas de protección de datos y privacidad en las comunicaciones electrónicas)», *Revista de Derecho Político*, págs. 101 a 154.

En quinto lugar, el proyecto de RGPD atiende a dificultad que la nueva realidad de Internet plantea para *reaccionar jurisdiccionalmente* de forma eficaz frente a las vulneraciones de la normativa de protección de datos protagonizadas por los grandes servicios online que impactan en miles de usuarios los cuales, individualmente, raramente demandarán a los responsables de dichas infracciones por muy varias razones (limitada relevancia del daño individual, gravosos costes procesales, escasa información y conocimiento del alcance de la infracción, etc.). Por ello, tomando como referencia las *class actions* anglosajonas (singularmente, eficaces en el ámbito estadounidense) y al margen de las pertinentes reclamaciones individuales, se reconoce a todo organismo, organización o asociación que tenga por objeto proteger los derechos e intereses de los usuarios y esté debidamente constituida conforme a la legislación nacional el derecho a presentar una *reclamación colectiva* frente una autoridad nacional de control por cuenta de uno o más interesados si considera vulnerados sus derechos. Como garantías adicionales a la posibilidad de acción individual se habilita al particular afectado por una decisión de una autoridad de control de un Estado miembro en el que no tiene su *residencia habitual* a solicitar a la autoridad de control de su Estado de residencia habitual para que ejercite en su nombre una *acción contra la autoridad de control* competente en el otro Estado miembro. Y, lo que resulta más relevante, aunque los recursos contra una entidad deban ejercitarse ante los órganos jurisdiccionales del Estado en el que tenga un establecimiento, también podrán ejercitarse ante los órganos jurisdiccionales del Estado miembro en que el interesado tenga su *residencia habitual*. Todas estas previsiones se unen a las *nuevas reglas sobre legislación aplicable* que extienden la vigencia y aplicabilidad del RGPD al tratamiento de datos de individuos residentes en la Unión Europea por parte de *entidades no establecidas en la Unión*, cuando sus actividades persigan ofertar bienes o servicios o hacer un seguimiento del comportamiento de dichos particulares en la Unión. Esto es, el RGPD reafirma, por si cupiese duda alguna, su aplicabilidad a todo tratamiento de datos realizado a través de Internet aunque la empresa titular de un determinado servicio (red social, motor de búsqueda, etc.) tenga su sede en un tercer país (EEUU) y pretende la aplicación de la legislación nacional de este tercer país. Esto, junto con la posibilidad de recurrir judicialmente en el país de residencia, constituye un indiscutible avance en el sistema de garantías procesales del derecho a la protección de datos en la era digital.

F) Una potente nueva estrategia preventiva: privacidad desde el diseño y por defecto (PbD), evaluación de impacto (PIA), delegados de protección de datos (DPOs), sellos ynormas corporativas vinculantes (BCRs)

La *Big Data Age* difícilmente encontrará satisfacción a los riesgos que se ciernen sobre la protección de datos a través de mecanismos represores o sancionadores. Desde el convencimiento de que el derecho mejor garantizado es aquel sobre el que se evitan sus vulneraciones, el legislador europeo —aun construyendo un exigente y riguroso sistema sancionatorio— ha diseñado una *potente estrategia preventiva* que, mediante pluralidad de mecanismos e instrumentos, materializa las exigencias básicas del *accountability principle*[46].

En primer lugar, el proyecto de RGPD apuesta por la *protección de datos desde el diseño y por defecto* (*Privacy by Design*[47] *and by Default*) al imponer a las entidades que traten datos —teniendo en cuenta las técnicas existentes y los costes que genere su implantación—, la obligación de implementar medidas y procedimientos técnicos y organizativos apropiados para que el tratamiento de datos respete la normativa de protección de datos y, en particular: a) garantice la protección de los derechos individuales; b) garantice que, por defecto, sólo sean objeto de tratamiento los datos personales necesarios para cada fin específico; c) preserve, especialmente, que sólo se recojan conserven por el tiempo y cantidad mínimos (*data minimization principle*) necesarios para sus fines; d) y evite, por defecto, que sean accesibles a un público. Además, la Comisión se reserva la facultad de adoptar actos delegados, sobre nuevos criterios y requisitos aplicables a las medidas y mecanismos apropiados para garantizar la protección de datos desde el diseño, y actos de ejecución que especifiquen las normas técnicas.

En segundo lugar, el RGPD normativiza la práctica preventiva ya presente en sistemas anglosajones (y, singularmente, en el Reino Unido[48]) de las *Evalua-*

[46] Para profundizar en su alcance y en lasposibilidades que abre a una nueva estrategia de protección de datos sustentada en la prevención, véase el Dictamen 3/2010, adoptado el 13 de junio de 2010 por el Grupo de Trabajo del Artículo 29 (WP 173) sobre *the principle of accountability (http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm)*. La adopción del Dictamen anterior y su traslación al nuevo RGPD son deudores del impulso y de los trabajos desarrollados por el Center for Information Policy Leadership y de sus Documentos de Trabajo *Demonstrating and Measuring Accountability, Paris Project (2010) e Implementing Accountability in the Marketplace, Madrid Project* (2011).

[47] Al respecto, véanse las siguientes consideraciones del Comisionado alemán de protección de datos (SCHAAR, P.: «Privacy by Design», *Identity in the Information Society* (2010), 3 (2), págs. 267 a 274) y del Supervisor Europeo de Protección de Datos (HUXTIN, P.: «Privacy by Design: Delivering the Promises», *Identity in the Information Society* (2010) 3 (2), págs. 253 a 255»).

[48] Warren, A. (2009): «Privacy Impact Assessments: the UK experience» en *31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. Madrid, 4-6 de noviembre de 2009*. http://www.privacyconference2009.org/program/Presentaciones/common/pdfs/adam_warren_speech_en.pdf

[49] Un amplio análisis de obligada consulta en WRIGHT, D. y DE HERT, P. (2012): *Privacy Impact Assessment*, Springer, London-New York.

ciones de Impacto en protección de datos —Privacy Impact Assessments (PIAs)[49] — sobre el tratamiento de datos que, por su naturaleza, alcance o fines, entrañen *riesgos específicos* como, en particular, ocurre en *supuestos* como: 1) la evaluación sistemática y exhaustiva una persona física sobre su situación económica, localización, salud, preferencias personales, fiabilidad o comportamiento, mediante un sistema automatizado; 2) el tratamiento a gran escala de información sobre la vida sexual, salud, raza y origen étnico o destinada a atención sanitaria, investigaciones epidemiológicas o estudios sobre enfermedades mentales o infecciosas; 3) el seguimiento amplio de zonas de acceso público (videovigilancia); d) o en los ficheros con datos masivos de niños, o con datos genéticos o biométricos. Además, la entidad deberá obtener *autorización* de la autoridad de control antes de proceder a estos tratamientos de datos y deberá ser objeto de *consulta* cuando una evaluación del impacto indique probabilidad de riesgos. La autoridad de control, cuando los riesgos no estén suficientemente identificados o atenuados, podrá *prohibir* los tratamientos de datos.

En tercer lugar, otra de las grandes apuestas del RGPD reside en la generalización del *delegado de protección de datos* —de especial predicamento, hasta la fecha, en Alemania y Francia— en todos los organismos públicos, empresas con más de doscientos cincuenta trabajadores o cuando la naturaleza, alcance o fines de una entidad requiera un seguimiento periódico y sistemático. Esta nueva figura de garantía gozará de un estatuto singular pues sus restantes funciones profesionales no podrán ser incompatibles y tendrá un mandato mínimo de dos años, renovable y no destituible. Se relacionará directamente con la autoridad de control, el público y los interesados y ejercerá sus funciones con independencia y sin recibir instrucciones. Sus funciones se centrarán en informar y asesorar a la entidad de sus obligaciones y en supervisar las políticas internas de privacidad de forma especial respecto de la garantía de la protección de datos desde el diseño, por defecto, en la seguridad de los datos, la información, la notificación de violaciones de datos, evaluación de impacto y cooperar con la autoridad de control.

En cuarto lugar, si bien los códigos de conducta ya previstos en la normativa vigente no pueden considerarse una historia de éxito (más bien todo lo contrario [50]), el proyecto de RGPD mantiene su existencia pero opta decididamente por abrir otra vía de promoción de la autorregulación —las *certificaciones y sellos*— a las que no atribuye mayor relevancia jurídica que la que pueda otorgarle en el futuro la Comisión mediante sus actos de delegación (definiendo sus criterios, re-

[50] De sus limitados logros, constituye un singular ejemplo el Dictamen 4/2010 del Grupo de Trabajo del Artículo 29 (WP 174), de 13 de julio de 2010, relativo al «Código de conducta europeo de la FEDMA sobre utilización de datos personales en la comercialización directa»(http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion recommendation/files/2010/wp174_es.pdf).

quisitos, condiciones de concesión y revocación o su reconocimiento institucional) y ejecución. Los Estados y la Comisión deberán promover, la existencia de estos mecanismos de certificación y sellos en materia de protección de datos para que los ciudadanos puedan evaluar rápidamente el nivel de protección de datos que se ofrece.

En quinto lugar, las *transferencias internacionales de datos* han constituido uno de los principales quebraderos de cabeza de las instituciones europeas bajo la vigencia de la Directiva 95/46. El modelo vigente ha sido fuertemente cuestionado por burocrático, costoso, ineficiente y desarmonizado. Aunque han evidenciado su inoperancia, los mecanismos tradicionales (declaraciones de adecuación, cláusulas contractuales, etc.) se mantienen con ligeras modificaciones y emerge con gran relevancia un nuevo instrumento que, de limitado alcance hasta la fecha[51], se pretende más realista y adecuado a la fuerza globalizadora que hace imparable el flujo de transferencias internacionales —las *normas corporativas vinculantes* (*Binding Corporate Rules*, *BCRs*)[52]— y que obedece a una nueva estrategia sustentada sobre la exigencia de responsabilidad entendida como *rendición de cuentas* (accountability). Así, ante la inexistencia de una declaración de adecuación en favor de un tercer país, sólo cabe transferir datos a éste o a una organización internacional, si hubieran ofrecido garantías apropiadas de protección de datos, sin necesidad de nuevas autorizaciones, en un instrumento jurídicamente vinculante cómo, por ejemplo y entre otras posibilidades, las normas corporativas vinculantes que así las define el proyecto de RGPD: «las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro de la Unión para las transfe-

[51] Véase, el Documento del Grupo de Trabajo del Article 29 sobre *«Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, adoptado el 3 de junio de 2003 (WP74) (http://www.europa.eu.int/comm/ justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf). Igualmente, adelantaron las propuestas actuales de la Comisión los Documentos de Trabajo del Grupo de Trabajo del Artículo 29, adoptados el 24 de junio de 2008 (WP 153, 154 y 155) sobre Preguntas Frecuentes y establecimiento de un marco para la estructura y elementos de las Normas Corporativas Vinculantes (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm).

[52] Una aproximación al tema puede encontrarse en las aportaciones de A. PUENTE («International Data Transfers Based on the So-called "Binding Corporate Rules"»), B. BELLAMY *(«*Case Study of Binding Corporate Rules»), E. USTARAN («Adoption of Binding Corporate Rules: Action Plan»), C. KUNNER («The Point of View on BCRs from a Large International Business Organisation») en *Proceedings of the first European Congress on Data* Protection (2008), Fundación BBVA, Madrid, págs. 149 a 189. Más recientemente, PROUST, O. y BARTOLI, E.: «Binding Corporate Rules: a global solution for international data transfers», *International Data Privacy Law* (2012), págs. 35 a 39.

rencias o un conjunto de transferencias de datos personales a un responsable o encargado del tratamiento en uno o más países terceros, dentro de un grupo de empresas». Sus *elementos básicos* son: 1) aplicarse la estructura completa de un grupo de empresas; 2) prever transferencias internacionales de datos a terceros países; 3) proclamar su carácter jurídicamente vinculante, tanto a nivel interno como externo; 4) establecer una política de protección de datos con sus correspondientes principios aplicables; 5) garantizar los derechos de los interesados y establecer los medios para ejercerlos: por ejemplo, no ser objeto elaboración de perfiles, derecho a recurso ante la autoridad de control y los órganos jurisdiccionales competentes, derecho a obtener una reparación o indemnización por violación de las normas corporativas, etc.; 6) facilita a los interesados información efectiva; 7) identificar las funciones del delegado de protección de datos relativas a la supervisión de la formación y la tramitación de las reclamaciones; 8) la cooperación con la autoridad de control. Corresponde a la autoridad de control aprobar estas normas corporativas vinculantes pero, antes de hacerlo, comunicará el proyecto de medida al CEPD y a la Comisión pudiendo éste o cualquier autoridad de control activar el mecanismo de coherencia.

No cabe concluir sin señalar que el éxito de la nueva estrategia preventiva diseñada por el RGPD dependerá de su eficacia y, en consecuencia, credibilidad en la garantía efectiva del derecho a la protección de datos. Es verdad que la Unión Europea —tras casi dos décadas de vigencia de un modelo exigente e imperativo para la protección efectiva de los datos personales, puede permitirse complementarlo con instrumentos alternativos proactivos que completen el diseño original y que den la mejor respuesta posible a una realidad que, a todas luces, genera riesgos inmensos de difícil persecución. En definitiva, no se trata de pasar del «palo» a la «zanahoria» sino de combinar la acción conjunta de ambos: *stick & carrot*.

Title:

TOWARDS A NEW DATA PROTECTION EUROPEAN LEGAL SYSTEM: THE KEYS OF THE REFORM

Summary:

1. Introduction: january 25, 2012, the announcement of the reform. 2. Background. The Communication of the European Commission in 2009 on «*a comprehensive approach on personal data protection in the european union*: from the Directive 95/46 to the art. 8 CDFUE. 3. The keys of the reform: main ideas. A) Weakness of the old legal framework. B) The new legal basis: article 16 TFUE, article 6 TUE and article 8 CDFUE. C) The new legal instruments: regulation *vs.* directive and directive *vs.* framework decision. D) The trend towards the european cen-

tralization: 1. the strengthening of the european commission powers: delegated implementing acts. 2. A common sanction regime: the strengthening of the reactive strategy. 3. Old european authorities but with new powers: european data protection council and european data protection supervisor. 4. The new procedures of cooperation (mutual assistance and joint investigations) and consistency as mechanisms for strengthening european harmonization. E) Faced with the technological tsunami, more protection and new rights: children, information, transparency, to be forgotten and portability. collective complaints, national jurisdiction and european aplicable law as new guarantees. F) A powerful new preventive strategy: privacy by design (PBD) and by default, impact assessment (PIA), data protection officers (DPOS), seals and binding corporate rules (BCRS).

Resumen:

La Comisión Europea ha presentado sendas iniciativas legislativas dirigidas a reformar el sistema europeo de protección de datos: un proyecto de Reglamento General de Protección de Datos y un proyecto de Directiva en el ámbito de la Policía y la Justicia Penal. Estas propuestas suponen una revisión global del sistema europeo de protección de datos pues se sustentan sobre la base de un diferente instrumento normativo frente a la anterior Directiva 95/46 y abordan nuevas problemáticas que no estaban siendo satisfactoriamente resueltas por la normativa vigente (por ejemplo, el impacto de las nuevas tecnologías y de Internet). Estas iniciativas están llamadas a revolucionar el marco global europeo de la protección de datos y a provocar un extraordinario impacto en el sistema español al resultar de directa e inmediata aplicación el reglamento europeo y al proporcionar nuevos derechos a los ciudadanos.

Esta nueva normativa europea de protección de datos está marcada por una inequívoca tendencia a la centralización comunitaria como se evidencia con el reforzamiento de los poderes de la Comisión Europea a través del recurso a los actos de delegación y de ejecución, con el establecimiento de un régimen sancionador común que fortalece la política represiva, con el otorgamiento de nuevos poderes a instituciones y organismos emergentes como el Consejo Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos y con la previsión de nuevos procedimientos europeos de cooperación y coherencia para garantizar la asistencia mutua, las investigaciones conjuntas y, en definitiva, la efectiva armonización europea. Además, este nuevo marco europeo busca hacer frente a la revolución tecnológica de nuestro tiempo otorgando más protección a los derechos de los ciudadanos —

en particular, a los menores de edad— mediante la información y la transparencia, nuevos derechos como el olvido y la portabilidad y nuevas reglas procesales y jurisdiccionales. Por último, la nueva normativa busca reforzar una estrategia preventiva eficaz que contemple la protección de la privacidad desde el diseño y por defecto, mediante evaluaciones de impacto, con la existencia de delegados de protección de datos y, ante las transferencias internacionales, reconociendo jurídicamente el valor de las normas corporativas vinculantes.

Abstract:

The European Commission has presented legislative initiatives aimed at reforming the European legal system for data protection: a draft General Data Protection Regulation and a draft Directive in the area of Police and Criminal Justice. These proposals represent a comprehensive European data protection legal system review because they support on the basis of a different standard-setting instrument versus the previous Directive 95/46 and addresses new issues which were not being satisfactorily resolved by current rules (for example, the impact of new technologies and the Internet). These initiatives are called to revolutionize the global European data protection framework and make a special impact in the Spanish legal system because of the direct and immediate application of European Regulation and providing new rights to citizens.

This new European data protection regulation is marked by a clear trend towards European centralization as evidenced with the strengthening of the powers of the European Commission through the use of the delegated and implementing acts, with the laying down of a common system of penalties which strengthens the repressive policy, with the recognizing of new powers to current institutions and organizations as the European Data Protection Board and the Data Protection European Supervisor and with the forecast of new European procedures for cooperation and consistency to ensure mutual assistance, joint investigations and, ultimately, effective European harmonisation. In addition, this new European framework seeks to address the technological revolution of our time giving more protection to the rights of citizens —in particular, minors— through information and transparency, new rights as to be forgotten and portability and new procedural and jurisdictional rules. Finally, the new legislation seeks to enhance an effective preventive strategy that takes into account the privacy by design and by default, through impact assessments, with

the existence of data protection officers and, related to international transfers, legally recognizing the value of binding corporate rules.

Palabras clave:

protección de datos, privacidad, Unión Europea

Key words:

data protection, privacy, European Union