EUROPEAN DATA PROTECTION SUPERVISOR

Dictamen 3/2015

La gran oportunidad de Europa

Recomendaciones del SEPD sobre las opciones de la UE en cuanto a la reforma de la protección de datos

28 de julio de 2015

El 24 de junio de 2015, las tres instituciones principales de la UE, el Parlamento Europeo, el Consejo y la Comisión Europea, entablaron las negociaciones de codecisión relativas a la propuesta de Reglamento general de protección de datos (RGPD), un procedimiento conocido como «diálogo tripartito» informal.[1] La base del diálogo tripartito es la propuesta de la Comisión de enero de 2012, la resolución legislativa del Parlamento Europeo de 12 de marzo de 2014 y el planteamiento general del Consejo de 15 de junio de 2015.[2] Las tres instituciones se han comprometido a tratar el RGPD como parte de una reforma más amplia del paquete de protección de datos, que incluye la propuesta de Directiva relativa a las actividades policiales y judiciales. El proceso debería concluir a finales de 2015 y, probablemente, permitiría la adopción formal de los dos instrumentos a comienzos de 2016, a lo que seguiría un período transitorio de dos años.[3]

*El Supervisor Europeo de Protección de Datos (SEPD) es una institución independiente de la UE. El Supervisor no participa en el diálogo tripartito, pero vela, con arreglo al artículo 41, apartado 2, del Reglamento (CE) 45 /2001, «*por lo que respecta al tratamiento de los datos personales, [...] por que los derechos y libertades fundamentales de las personas físicas, en particular el derecho de las mismas a la intimidad, sean respetados por las instituciones y los organismos comunitarios *y* asesorará a las instituciones y a los organismos comunitarios, así como a los interesados, en todas las cuestiones relacionadas con el tratamiento de datos personales*». El Supervisor y el Supervisor Adjunto fueron designados en diciembre de 2014, con el mandato concreto de ser más constructivos y activos, y en marzo de 2015 publicaron una estrategia quinquenal en la que indican cómo pretenden llevar a la práctica dicho mandato y rendir cuentas al respecto.[4]*

Este dictamen es el primer hito en la estrategia del SEPD. Sobre la base de los debates celebrados con las instituciones de la UE, los Estados miembros, la sociedad civil, la industria y otras partes interesadas, nuestro dictamen tiene por objeto ayudar a los participantes en el diálogo tripartito a alcanzar a tiempo el consenso adecuado. Trata sobre el RGPD en dos partes:

- *la visión del SEPD respecto a normas sobre protección de datos de futuro, con ejemplos ilustrativos de nuestras recomendaciones y*
- *un anexo («Anexo al Dictamen 3/2015: Cuadro comparativo de textos del RGPD con la recomendación del SEPD»), que incorpora un cuadro de cuatro columnas para la comparación, artículo por artículo, de la versión del RGPD aprobada, respectivamente, por la Comisión, el Parlamento y el Consejo, junto a la recomendación del SEPD.*

El Dictamen se publica en nuestro sitio web y a través de una aplicación móvil. Se complementará en otoño de 2015 con recomendaciones referidas tanto a los considerandos del RGPD como, una vez que el Consejo haya adoptado su posición común en relación con la Directiva, a la protección de datos aplicable a las actividades policiales y judiciales.

Sigue siendo vigente el exhaustivo Dictamen del SEPD sobre el paquete de reformas propuesto por la Comisión en 2012. Tres años después, no obstante, tenemos que actualizar nuestro dictamen para abordar más directamente las posiciones de los

colegisladores y ofrecer recomendaciones concretas. [5] *Al igual que el Dictamen de 2012, este se atiene a las opiniones y declaraciones del Grupo de trabajo del artículo 29, incluido el «Apéndice» sobre «Temas principales en vista de la celebración del diálogo tripartito» aprobado el 18 de junio, al que el SEPD contribuyó en calidad de miembro de pleno derecho del Grupo de trabajo.*[6]

Una oportunidad única: ¿Por qué es tan importante esta reforma?

La UE se halla en el último tramo del esfuerzo maratoniano emprendido para reformar sus normas sobre información personal. El Reglamento general de protección de datos afectará potencialmente, durante los próximos decenios, a todas las personas de la UE, a todas las organizaciones de la Unión que tratan datos personales y a las organizaciones externas a la UE que tratan datos personales referidos a personas en la UE.[7] Ha llegado la hora de proteger los derechos y libertades fundamentales de las personas en la sociedad de la información del futuro.

Una protección de datos eficaz capacita a la persona y supone un impulso para las empresas responsables y para las autoridades. La legislación en este ámbito es compleja y técnica y exige recomendaciones especializadas procedentes, sobre todo, de autoridades de protección de datos independientes que comprendan las dificultades que entraña el cumplimiento. Es probable que el RGPD se convierta en uno de los textos más largos de la legislación de la Unión, por lo que procede que la UE trate de ser selectiva y se centre en las disposiciones que son realmente necesarias, evitando detalles que pudieran acarrear como consecuencia imprevista el interferir indebidamente en las futuras tecnologías. Los textos de cada institución predican claridad e inteligibilidad en el tratamiento de los datos personales: así pues, el RGPD debe predicar con el ejemplo, siendo tan conciso e inteligible como sea posible.

Corresponde al Parlamento y al Consejo, en calidad de colegisladores, determinar el texto jurídico final auxiliados por la Comisión, en su calidad de iniciadora de la legislación y guardiana de los Tratados. El SEPD no forma parte de las negociaciones «tripartitas», aunque sí le corresponde la competencia jurídica de ejercer una función consultiva de manera activa, con arreglo al mandato encomendado al Supervisor y el Supervisor Adjunto en el momento de su nombramiento y a la estrategia reciente del SEPD. El Dictamen se articula sobre más de un decenio de experiencia en la supervisión del cumplimiento de la protección de datos y el asesoramiento en materia de políticas con objeto de ayudar a las instituciones a lograr unos resultados que redunden en interés de las personas.

La legislación es el arte de lo posible. Las opciones encima de la mesa, en la forma de los correspondientes textos preferidos por la Comisión, el Parlamento y el Consejo, contienen numerosas disposiciones valiosas, aunque todos ellos pueden mejorarse. El resultado no será perfecto, en nuestra opinión, aunque tenemos la intención de prestar apoyo a las instituciones para lograr el mejor resultado posible. Por este motivo, nuestras recomendaciones se ciñen a los límites de los tres textos. Nos impulsan tres preocupaciones constantes:

- lograr un mejor acuerdo para los ciudadanos,
- definir unas normas que funcionen en la práctica,
- definir unas normas que perduren a lo largo de una generación.

El presente Dictamen es un ejercicio de transparencia y responsabilidad, dos principios que representan, acaso, la más destacada novedad del RGPD. El proceso de diálogo tripartito está siendo objeto de un examen más riguroso que nunca. Nuestras recomendaciones son públicas e instamos a las instituciones de la UE a que tomen la

iniciativa y prediquen con el ejemplo, de manera que esta reforma legislativa sea el resultado de un proceso transparente y no un compromiso secreto.

La UE precisa de un nuevo acuerdo sobre protección de datos, un nuevo capítulo. El resto del mundo observa atentamente. Son fundamentales calidad de la nueva legislación y el modo en que interaccione con los sistemas jurídicos y las tendencias mundiales. Con el presente Dictamen, el SEPD pone de manifiesto su voluntad y disposición a contribuir a que la UE aproveche al máximo esta oportunidad histórica.

I. ÍNDICE

1 Lograr un mejor acuerdo para los ciudadanos

Las normas de la UE han tratado siempre de facilitar el flujo de datos dentro de la UE y entre esta y sus socios comerciales, si bien con una preocupación constante por los derechos y libertades de la persona. Internet ha permitido un grado de conectividad y expresión y ofrecido un margen para la creación de valor sin precedentes para las empresas y los consumidores. Sin embargo, la privacidad tiene más importancia que nunca para los europeos. Según la encuesta del Eurobarómetro sobre protección de datos de junio de 2015, [8] más de seis de cada diez ciudadanos no confían en las empresas en línea, mientras que dos terceras partes de los encuestados se muestran preocupados por no ejercer un control completo sobre la información que facilitan por Internet.

El marco reformado tiene que mantener y, donde sea posible, elevar el nivel de protección de las personas. El paquete de reforma de la protección de datos se propuso, en un principio, a modo de vehículo para el «fortalecimiento de los derechos de privacidad en línea» garantizando que las personas estén «mejor informadas sobre sus derechos y ejerzan un mayor control sobre su información».[9] Los representantes de las organizaciones de la sociedad civil enviaron, en abril de 2015, una carta a la Comisión en la que urgían a las instituciones a que se atuvieran a estas intenciones.[10]

Los principios vigentes recogidos en la Carta, la legislación **primaria**/de base? de la UE, deben aplicarse de manera coherente, dinámica e innovadora, de manera que sean eficaces para el ciudadano en la práctica. La reforma tiene que ser exhaustiva, de ahí el compromiso con el desarrollo de un paquete, aunque, dado que es probable que el tratamiento de datos se aborde en instrumentos jurídicos distintos, habrá de establecerse con claridad su ámbito de aplicación exacto y el modo en que aquellos interactúan, de manera que no existan lagunas que permitan vulnerar las salvaguardias.[11]

Para el SEPD, el punto de partida es la dignidad de la persona, que trasciende las cuestiones referidas al mero cumplimiento jurídico de la normativa.[12] Nuestras recomendaciones se basan en una evaluación de cada artículo del RGPD, de manera individual y acumulativa, conforme a si supondrá una mejora de la situación de la persona en comparación con el marco vigente. El punto de referencia son los principios en los que se fundamenta la protección de datos, es decir, los recogidos en el artículo 8 de la Carta de los Derechos Fundamentales.[13]

1. Definiciones: aclaremos qué es información personal

- Las personas deben ejercer de un modo más eficaz sus derechos en lo tocante a cualquier información que pueda servir para identificarlas o señalarlas, incluso si la información se considera «seudonimizada».[14]

2. Todo tratamiento de datos debe ser *tanto* legal *como* estar justificado

- Las exigencias con arreglo a las que todo tratamiento de datos ha de limitarse a una finalidad concreta y basarse en un fundamento jurídico son acumulativas, no alternativas. Recomendamos evitar cualquier fusión que debilite estos principios. En lugar de ello, la UE debe conservar, simplificar y hacer operativo el

concepto de que los datos personales solo deben emplearse de manera compatible con la finalidad original para la que fueron recopilados.[15]

- El consentimiento es un fundamento jurídico posible para el tratamiento, aunque hemos de evitar formularios que contengan casillas coercitivas en las que no se ofrezcan a la persona opciones razonables o exijan la aportación de unos datos cuyo tratamiento no sea en absoluto necesario. Recomendamos permitir que las personas otorguen un consentimiento amplio o restringido a la realización, por ejemplo, de un examen clínico, que se respete y que pueda retirarse.[16]

- El SEPD apoya unas soluciones sólidas e innovadoras para la transferencia internacional de información nacional que facilite los intercambios de datos y respete los principios de protección y supervisión de los datos. Recomendamos enérgicamente que no se permitan las transferencias basadas en los intereses legítimos del responsable del tratamiento en vista del grado insuficiente de protección de la persona, y que no se abran las puertas de la UE al acceso directo a datos ubicados en su territorio por parte de autoridades de terceros países. Cualquier solicitud de transferencia expedida por las autoridades de un tercer país se reconocerá únicamente si respeta las normas establecidas en tratados bilaterales de asistencia jurídica, acuerdos internacionales u otros canales jurídicos de cooperación internacional.[17]

3. Una supervisión más independiente y fidedigna

- Las autoridades de protección de datos de la UE deben estar listas para ejercer sus funciones en el momento en que entre en vigor el RGPD y el Consejo Europeo de Protección de Datos habrá de estar plenamente operativo tan pronto como el Reglamento empiece a aplicarse.[18]

- Las autoridades deben estar en condiciones de escuchar e investigar las quejas y reclamaciones que les presenten interesados u organismos, organizaciones y asociaciones.

- El ejercicio de los derechos individuales exige un sistema de responsabilidad eficaz y la indemnización por los daños causados por el tratamiento ilícito de los datos. Habida cuenta de los claros obstáculos que impiden obtener una compensación en la práctica, las personas podrán ser representadas por órganos, organizaciones y asociaciones en los procedimientos judiciales.[19]

2 Definir unas normas que funcionen en la práctica

Las salvaguardias no han de confundirse con meras formalidades. Un exceso de detalles o el intento de «microgestionar» los procesos operativos entraña el riesgo de obsolescencia en el futuro. Aquí cabría seguir el ejemplo del manual de competencia de la UE, en el que un corpus limitado de legislación secundaria se aplica de manera rigurosa y fomenta una cultura de la responsabilidad y la concienciación entre las empresas.[20]

Cada uno de los tres textos exige una claridad y una simplicidad mayores por parte de los responsables del tratamiento de la información personal.[21] Igualmente, las

obligaciones técnicas deben ser asimismo concisas y fácilmente comprensibles si lo que se pretende es que los responsables del control las apliquen correctamente.[22]

Los procedimientos existentes no son sacrosantos: nuestras recomendaciones aspiran a identificar métodos de desburocratizar y minimizar las exigencias de documentación y de trámites irrelevantes. Recomendamos legislar únicamente donde sea verdaderamente necesario. Ello ofrece margen de maniobra a las empresas, las autoridades públicas o las autoridades de protección de datos: un espacio que ha de colmarse con responsabilidad y orientaciones procedentes de las autoridades de protección de datos. En general, nuestras recomendaciones darían lugar un texto del RGPD casi un 30 % más breve que la longitud media de los documentos de las tres instituciones.[23]

1. Salvaguardias eficaces, no procedimientos

- La documentación debe constituir un medio, no un fin para el cumplimiento; la reforma ha de centrarse en los resultados. Recomendamos un planteamiento «escalable» que reduzca las obligaciones en materia de documentación impuestas sobre los responsables del control y establezca un política única sobre el modo en que aquellos cumplirán la reglamentación, teniendo en cuenta los riesgos, y demostrarán el cumplimiento de manera transparente en lo que concierne a las transferencias, los contratos con los responsables del tratamiento o las notificaciones de infracciones.[24]

- Sobre la base de unos criterios de evaluación del riesgo explícitos, y ateniéndonos a nuestra experiencia en la supervisión de las instituciones de la UE, recomendamos exigir la notificación de las infracciones en materia de tratamiento de datos a la autoridad de control y la realización de evaluaciones de impacto de la protección de datos únicamente en caso de que los derechos y las libertades de los interesados se encuentren en peligro.[25]

- Deben fomentarse activamente las iniciativas de la industria, bien a través de normas empresariales vinculantes o de distintivos de protección de la intimidad.[26]

2. Un mejor equilibrio entre el interés público y la protección de los datos personales

- Las normas sobre protección de datos no deben obstaculizar la realización de investigaciones históricas, estadísticas y científicas que redunden verdaderamente en el interés público. Los responsables habrán de establecer los regímenes necesarios para evitar que la información personal se utilice en contra de los intereses de la persona y prestarán especial atención a las normas que regulan el tratamiento de la información sanitaria sensible, por ejemplo.[27]

- Los investigadores y archiveros deberán estar en condiciones de conservar los datos durante todo el tiempo que sea preciso ateniéndose a tales salvaguardias.[28]

3. Confianza en las autoridades de control y capacitación de estas

- Recomendamos que las autoridades de control puedan publicar orientaciones para los responsables del tratamiento de datos y que puedan desarrollar sus

propios reglamentos internos en el marco de una aplicación simplificada y más sencilla del RGPD a través de una única autoridad de control («ventanilla única») próxima al ciudadano («proximidad»). [29]

- Las autoridades deben estar en condiciones de imponer unas sanciones compensatorias y administrativas eficaces, proporcionadas y disuasorias basadas en todas las circunstancias pertinentes.[30]

3 Definir unas normas que perduren a lo largo de una generación

El pilar fundamental del marco vigente, la Directiva 95/46/CE, ha sido un modelo para el desarrollo de legislación adicional en materia de tratamiento de datos en la UE y en todo el mundo e incluso ha constituido la base para la formulación del derecho a la protección de los datos personales recogida en el artículo 8 de la Carta de los Derechos Fundamentales. Esta reforma dará forma al tratamiento de datos para una generación que no recuerde haber vivido sin Internet. La UE debe, pues, comprender plenamente las repercusiones de este acto en las personas y su sostenibilidad en vista del desarrollo tecnológico.

A lo largo de los últimos años se ha producido un incremento exponencial de la recopilación de datos, el análisis y el intercambio de información personal, el resultado de innovaciones tecnológicas como la «Internet de las cosas», la computación en nube, los macrodatos (big data) y los datos de libre acceso (open data), cuya explotación se considera esencial en la UE para su competitividad.[31] A juzgar por la longevidad de la Directiva 95/46/CE, es razonable prever un plazo similar antes de que se produzca la siguiente revisión importante de la normativa de protección de datos, acaso no antes del decenio de 2030. Mucho antes de dicha fecha, cabe prever una convergencia de las tecnologías basadas en los datos con la inteligencia artificial, el procesamiento de lenguajes naturales y los sistemas biométricos, lo que permitirá el desarrollo de aplicaciones dotadas de una capacidad de aprendizaje artificial y una inteligencia avanzada.

Estas tecnologías suponen un desafío para los principios de la protección de datos. Una reforma orientada hacia el futuro debe fundamentarse, pues, en la dignidad de la persona y estar basada en criterios éticos. Debe corregir el desequilibrio entre la innovación en la protección de los datos personales y su explotación, estableciendo unas salvaguardias eficaces en nuestra sociedad digital.

1. Prácticas empresariales responsables y técnicas innovadoras

- La reforma debe invertir la tendencia reciente hacia el seguimiento secreto y la adopción de decisiones basada en perfiles ocultos de la persona. El problema no es la publicidad personalizada o la práctica de la elaboración de perfiles, sino, más bien, la falta de información adecuada sobre la lógica algorítmica a partir de la que se desarrollan tales perfiles y que repercute en el interesado.[32] Recomendamos un mayor grado de transparencia por parte de los responsables del tratamiento de datos.

- Apoyamos firmemente, asimismo, la introducción de los principios de la protección de datos desde la fase de concepción y por defecto como medio para

impulsar unas soluciones comerciales en la economía digital. Recomendamos una formulación más sencilla de las exigencias de integración de los derechos e intereses de la persona en el desarrollo de productos y en las opciones por defecto.[33]

2. Personas capacitadas

- La transferibilidad de los datos es la puerta que, en el medio digital, conduce al control del usuario del que los ciudadanos están dándose cuenta de que carecen. Recomendamos habilitar la transferencia directa de datos de un responsable de su tratamiento a otro a petición del interesado y facultar a este para recibir una copia de los datos que pueda transferir a otro responsable.[34]

3. Normas a prueba de la evolución futura

- Recomendamos evitar un lenguaje y unas prácticas proclives a quedar desfasados o tornarse debatibles.[35]

4 Asunto inconcluso

La adopción de un paquete de reforma de la legislación en materia de datos de futuro constituirá un logro impresionante y, pese a todo, incompleto.

Todas las instituciones están de acuerdo en que los principios del RGPD deben aplicarse de manera coherente a todas las instituciones de la UE. Hemos abogado por la seguridad y uniformidad jurídicas del marco jurídico, sin dejar de reconocer el carácter único del sector público de la UE y la necesidad de evitar cualquier debilitamiento del nivel actual de las obligaciones (así como la necesidad de ofrecer la base jurídica y organizativa necesaria para el SEPD). La Comisión debería, pues, presentar una propuesta coherente con el RGPD para la revisión del Reglamento (CE) nº 45/2001 tan pronto como sea posible, una vez hayan concluido las conversaciones sobre el Reglamento general, de manera que ambos textos entren en vigor al mismo tiempo.[36]

En segundo lugar, está claro que la Directiva 2002/58/CE (sobre la privacidad y las comunicaciones electrónicas) tendrá que modificarse. Y, lo que es mucho más importante, la UE precisa de un marco claro en cuanto a la confidencialidad de las comunicaciones, un elemento integrante del derecho a la intimidad que rija todos los servicios que incluyan comunicaciones, no solamente los prestados por los proveedores de comunicaciones electrónicas de acceso público. Ello ha de llevarse a cabo por medio de un reglamento de armonización que genere seguridad jurídica y establezca, cuando menos, los mismos niveles de protección que la Directiva sobre la privacidad y las comunicaciones electrónicas en una situación de igualdad de condiciones.

El presente Dictamen recomienda, pues, que se alcance un compromiso para la adopción rápida, lo antes posible, de propuestas en estos dos ámbitos.

5 Un momento crucial para los derechos digitales dentro y fuera de Europa

Por vez primera en una generación, la UE tiene la opción de modernizarse y armonizar las normas con arreglo a las que se gestiona la información personal. La privacidad y la

protección de datos no están en conflicto con el crecimiento económico y el comercio internacional ni con la prestación de servicios o la oferta de productos excelentes: forman parte de una propuesta de calidad y valor. Tal como reconoce el Consejo Europeo, la confianza es una condición previa necesaria para unos productos y servicios innovadores que se basen en el tratamiento de los datos personales.

En 1995, la UE se situó a la vanguardia de la protección de datos. Hoy, más de 100 países de todo el mundo disponen de leyes de protección de datos y menos de la mitad de ellos son países europeos.[37] La UE, no obstante, sigue siendo objeto de una atenta observación por parte de los países que están considerando establecer o revisar sus marcos jurídicos. La situación actual, en la que la confianza de la ciudadanía en las empresas y los gobiernos se ha visto menoscabada por la revelación de la existencia de actividades masivas de vigilancia e infracciones de los derechos a la protección de los datos, conlleva una gran responsabilidad impuesta sobre los legisladores de la UE, pues cabe prever que las decisiones que adopten este año tengan repercusiones dentro y fuera de Europa.

En opinión del SEPD, los textos del RGPD se hallan en el buen camino, aunque siguen existiendo ciertos motivos de preocupación, en algunos casos de índole muy grave. En el marco del proceso de codecisión, existe siempre el riesgo de que determinadas disposiciones se vean debilitadas por la actuación de negociadores bienintencionados que pretenden lograr un compromiso político. El caso de la reforma de la legislación de protección de datos es distinto, ya que se trata de derechos fundamentales y del modo en que estos se protegerán a lo largo de una generación.

Sobre esta base, el presente Dictamen desea asistir a las principales instituciones de la UE en la resolución de problemas. No solo deseamos unos derechos más sólidos para los interesados y un mayor grado de responsabilidad para el responsable del tratamiento, también queremos facilitar la innovación con un marco jurídico que sea neutral en materia tecnológica y favorable en lo que atañe a las ventajas que la tecnología puede aportar a la sociedad.

Con las negociaciones en su tramo final, esperamos que nuestras recomendaciones ayuden a la UE a alcanzar la línea de meta con una reforma que siga siendo apta a lo largo de los años y los decenios venideros: un nuevo capítulo para la protección de datos con una perspectiva global y con la UE al frente, predicando con el ejemplo.

Bruselas, 28 de julio de 2015

Giovanni BUTTARELLI

El Supervisor Europeo de Protección de Datos

Notas

[1] Declaraciones comunes, Declaración común del Parlamento Europeo, el Consejo y la Comisión sobre las modalidades prácticas del procedimiento de codecisión (artículo 251 del Tratado CE) (2007/C 145/02), DO C 145, 30.6.2007.

[2] COM(2012) 11 final; Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento 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 organismos comunitarios y a la libre circulación de estos datos (Reglamento general sobre protección de datos), COM(2012) 11 final, P7_TA(2014)0212; Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), preparación de un planteamiento general, documento del Consejo 9565/15, 11.06.2015.

[3] El título extenso es «Propuesta de Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos», COM(2012)10 final; Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, P7_TA(2014)0219. Sobre los plazos y el alcance del diálogo tripartito, véanse las Conclusiones del Consejo Europeo de 25-26 de junio de 2015 (EUCO 22/15); en la conferencia de prensa conjunta Parlamento-Consejo-Comisión relativa al diálogo tripartito, se hizo mención de una «hoja de ruta»: http://audiovisual.europarl.europa.eu/AssetDetail.aspx?id=690e8d8d-682d-4755-bfb6-a4c100eda4ed [consultado por última vez el 20.7.2015], aunque aquella no se ha publicado de manera oficial. El RGPD entrará en vigor 20 días después de su publicación en el Diario Oficial y está previsto que sea plenamente aplicable dos años después de su entrada en vigor (artículo 91).

[4] Vacante para el puesto de Supervisor Europeo de Protección de Datos, COM/2014/10354 (2014/C 163 A/02), DO C 163 A/6 28.5.2014. En la Estrategia del SEPD 2015-2019 se prometió «buscar soluciones que eviten la burocracia, conserven la flexibilidad para la innovación tecnológica y los flujos de datos transfronterizos y permitan a las personas ejercer sus derechos más eficazmente en Internet y fuera de Internet»; Leading by example: The EDPS Strategy 2015-2019, marzo de 2015.

[5] Dictamen del SEPD sobre el paquete de reforma de la legislación en materia de protección de datos, 7.3.2015.

[6] Véase el anexo a la carta del Grupo de trabajo del artículo 29 a Věra Jourová, Comisaria de Justicia, Consumidores e Igualdad de Género, 17.6.2015.

[7] No es fácil resumir sucintamente el ámbito de aplicación material y territorial del RGPD. Las instituciones parecen convenir, al menos, en que dicho ámbito comprende las organizaciones establecidas en la UE y responsables del tratamiento de datos personales dentro o fuera de la Unión y las organizaciones establecidas fuera de la UE que tratan datos personales de personas en la UE al ofrecerles productos o servicios o que efectúan un seguimiento individualizado en la UE. (Véase el artículo 2 en relación con el ámbito de aplicación material y el artículo 3 en lo que atañe al territorial).

[8] Otros resultados incluyeron que siete de cada diez encuestados expresara preocupación por que la información se utilice con fines distintos de aquel para el que se recabó, que uno de cada siete declarara que se le debería pedir su aprobación explícita en todos los casos antes de recopilar y tratar sus datos y que dos de cada tres considerara importante que se pudiera transferir información de un proveedor de servicios anterior a otro nuevo; Eurobarómetro especial 431 sobre protección de datos, junio de 2015. Se obtuvieron resultados comparables en el estudio Pew de 2014, con arreglo al que un 91 % de los estadounidenses expresó su percepción de haber perdido el control sobre el modo en que las empresas recogen y utilizan la información personal, un 80 % de los usuarios de redes sociales se manifestó preocupado por el modo en que terceros, como anunciantes o empresas, obtienen sus datos y un 64 % declaró que el Gobierno debería hacer algo más para regular la actuación de los anunciantes; Pew Research Privacy Panel Survey, enero de 2014.

[9] La Comisión propone una reforma exhaustiva de las normas de protección de datos para incrementar el control de los usuarios con respecto a sus datos y ahorrar costes a las empresas.

[10] Carta de ONG al Presidente Juncker, 21.4.2015 https://edri.org/files/DP_letter_Juncker_20150421.pdf y respuesta del Jefe de Gabinete del Vicepresidente Timmermans, 17.7.2015 https://edri.org/files/eudatap/Re_EC_EDRi-GDPR.pdf [consultadas el 23.7.2015]. El SEPD se reunió, en mayo de 2015, con representantes de varias de estas ONG para debatir sobre sus preocupaciones. Comunicado de prensa EDPS/2015/04, 1.6.2015, Reforma del régimen de protección de datos de la UE: SEPD se reúne con grupos internacionales de defensa de las libertades civiles; grabación íntegra del debate disponible en el sitio web del SEPD (https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Pressnews/Videos/GDPR_civil_soc).

[11] Artículo 2, apartado 2, letra e).

[12] Artículo 1.

[13] El artículo 8 de la Carta establece lo siguiente [se ha añadido el énfasis]:

> *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 le conciernan y a obtener su* ***rectificación****.*
>
> *3. El respeto de estas normas estará sujeto al* ***control de una autoridad independiente****.*

[14] Artículo 10. A menos que exista una definición clara y vinculante de «datos seudonimizados» distinta de la de «datos personales», este tipo de datos debe mantenerse dentro del ámbito de protección de las normas de protección de datos.

[15] Artículos 6.2 y 6.4. En vista de que hay cierta incertidumbre a propósito del significado de «compatibilidad», recomendamos ceñirse al Dictamen del GT29 sobre la limitación de la finalidad, criterios generales para la evaluación de si el tratamiento es compatible (véase el artículo 5, apartado 2).

[16] Una separación funcional efectiva constituye un medio de garantizar un tratamiento legal en ausencia de consentimiento, aunque la interpretación del interés legítimo no ha de llevarse al extremo. Un derecho de exclusión (opt out) incondicional también puede constituir una alternativa adecuada en ciertas situaciones. Evaluar si el consentimiento se otorga libremente depende en parte de a) si existe un desequilibrio significativo entre el interesado y el responsable del tratamiento y b) en casos en que el tratamiento se ciña a lo dispuesto en el artículo 6, apartado 1, letra b), si la ejecución de un contrato o la prestación de un servicio se supedita a un consentimiento del tratamiento de datos que no es necesario para tales fines.

(Véase el artículo 7, apartado 4). Ello refleja la disposición recogida en la legislación de protección del consumidor de la UE: con arreglo al artículo 3, apartado 1, de la Directiva 93/13/CEE, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores, «las cláusulas contractuales que no se hayan negociado individualmente se considerarán abusivas si, pese a las exigencias de la buena fe, causan en detrimento del consumidor un desequilibrio importante entre los derechos y obligaciones de las partes que se derivan del contrato».

[17] Tales normas comprenden decisiones sobre idoneidad referidas a sectores y territorios específicos, revisiones periódicas de las decisiones sobre idoneidad y normas empresariales vinculantes. Véanse los artículos 40 a 45.

[18] Artículo 73.

[19] Artículo 76. A propósito de la dificultad de obtener una compensación en caso de infracción de las normas de protección de datos, consúltese el informe de la Agencia de Derechos Fundamentales, «Acceso a las vías de recurso en materia de protección de datos en los Estados miembros de la Unión Europea», 2013.

[20] Las normas de la UE hacen hincapié en la autoevaluación de las empresas en lo que concierne al cumplimiento de lo dispuesto en el artículo 101 del TFUE sobre la prohibición de los acuerdos contrarios a la competencia, mientras que a las empresas dominantes en un mercado les corresponde la «responsabilidad especial» de evitar cualquier actuación que pueda menoscabar la competencia efectiva (apartado 9 de las Orientaciones de la Comisión 2009/C 45/02); véase el Dictamen preliminar del SEPD sobre la privacidad y la competitividad en la era de los macrodatos, 14.3.2014.

[21] Los tres textos se refieren de manera diversa al «modo y forma inteligibles, utilizando para ello un lenguaje sencillo y claro» (considerando 57, PE; artículo 19 COM y Consejo), y a ser «claros e inequívocos» (considerando 99, PE; artículo 10 bis, PE) y ofrecer «información clara y fácilmente comprensible» (artículo 10, PE, artículo 11, PE) e información que sea «concisa, transparente, sencilla y fácilmente accesible» (considerando 25, PE, COM y Consejo; artículo 11, PE).

[22] Las disposiciones relativas a los actos delegados se han eliminado en su mayoría en las versiones del Parlamento y el Consejo. Creemos que la UE podría ir más allá y someter estos asuntos técnicos al criterio experto de autoridades independientes.

[23] Nuestras recomendaciones darían lugar a un texto de unas 20 000 palabras; la longitud media de los textos de las tres instituciones es de aproximadamente 28 000 palabras.

[24] Artículo 22.

[25] Artículos 31 y 33.

[26] Artículo 39.

[27] Artículo 83. La investigación y el archivo no constituyen, en sí mismos, un fundamento jurídico para el tratamiento, motivo por el que recomendamos la supresión del artículo 6, apartado 2.

[28] Artículo 83 bis.

[29] El GT29 ha desarrollado una visión en lo que atañe a la gobernanza, el mecanismo de coherencia y la ventanilla única basada en la confianza en unas autoridades responsables del tratamiento de datos independientes y la ha establecido en tres niveles:

- la autoridad concreta, fuerte y plenamente dotada de los recursos necesarios para tratar los asuntos que le competen;
- una cooperación eficaz entre las autoridades y una definición clara de la competencia en casos transfronterizos;

- el CEPD, que debe ser autónomo, estar dotado de una personalidad jurídica propia y de fondos suficientes, integrado por autoridades responsables del tratamiento equivalentes que cooperen solidariamente y facultado para adoptar decisiones vinculantes y contar con el apoyo de una secretaría que preste su servicio al consejo a través de la presidencia.

[30] También recomendamos clarificar las competencias de las autoridades de control y la designación de una autoridad principal en casos de tratamiento internacional, conservando las primeras la capacidad de tramitar asuntos enteramente locales. Recomendamos simplificar el mecanismo de coherencia, aclarando en mayor medida el modo de identificar los casos en que las autoridades de control tendrán que consultar al Consejo Europeo de Protección de Datos y aquellos en que dicho Consejo tendrá que emitir una resolución vinculante para garantizar la aplicación coherente del Reglamento.

[31] Comunicación de la Comisión sobre una Estrategia para el Mercado Único Digital de Europa, COM(2015) 192 final; Conclusiones del Consejo Europeo de junio de 2015, EUCO 22/15; Conclusiones del Consejo sobre la transformación digital de la industria europea, 8993/15.

[32] Artículo 14, letra h).

[33] Artículo 23.

[34] Artículo 18. Recomendamos asimismo que, para garantizar su eficacia, se establezca un ámbito de aplicación amplio al derecho de transferibilidad de los datos y que aquel no se aplique únicamente a las operaciones de tratamiento que utilicen datos aportados por el interesado.

[35] Recomendamos, por ejemplo, omitir términos como «en línea», «por escrito» y «la sociedad de la información».

[36] Preferiríamos la opción de incluir una disposición en el propio RGPD.

[37] Greenleaf, Graham, «Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority» (30 de enero de 2015); (2015) 133 Privacy Laws & Business International Report, febrero de 2015; UNSW Law Research Paper Nº 2015-21.