COMISIÓN EUROPEA

Bruselas, 25.1.2012
COM(2012) 9 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES

La protección de la privacidad en un mundo interconectado
Un marco europeo de protección de datos para el siglo XXI

(Texto pertinente a efectos del EEE)

[…]

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES

La protección de la privacidad en un mundo interconectado
Un marco europeo de protección de datos para el siglo XXI

(Texto pertinente a efectos del EEE)

1. RETOS ACTUALES PARA LA PROTECCIÓN DE DATOS

La velocidad a la que se suceden las innovaciones tecnológicas y el fenómeno de la globalización han transformado profundamente los métodos de recogida, acceso, utilización y transferencia de un volumen de datos personales en constante crecimiento. Las nuevas formas de compartir información en las redes sociales y el almacenamiento remoto de grandes cantidades de datos han pasado a formar parte de la existencia cotidiana de una amplia proporción de los 250 millones de usuarios de Internet en Europa. Al mismo tiempo, los datos personales se han convertido en un activo para numerosas empresas, una parte importante de cuyas actividades económicas[1] consiste en la recogida, agregación y análisis de los datos de clientes potenciales.

En este nuevo entorno digital, **los ciudadanos tienen derecho a ejercer un control efectivo sobre su información personal**. La protección de datos es en Europa un derecho fundamental consagrado tanto en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea como en el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea, por lo que debe salvaguardarse adecuadamente.

La falta de confianza provoca en los consumidores cierta reticencia a la hora de hacer compras en línea y de aceptar nuevos servicios. Por lo tanto, la existencia de un alto nivel de protección de datos es también crucial para infundir confianza en los servicios en línea y explotar el potencial de la economía digital, propiciando con ello **el crecimiento económico y la competitividad de las industrias de la UE.**

Es preciso disponer en toda la UE de normas modernas y coherentes que permitan la libre circulación de datos entre los Estados miembros. Las empresas necesitan reglas claras y uniformes que aporten seguridad jurídica y reduzcan las cargas administrativas. Así lo exigen el funcionamiento del mercado único y la necesidad de **estimular el crecimiento económico, crear puestos de trabajo y fomentar la**

[1] El mercado del análisis de conjuntos muy amplios de datos está creciendo a un ritmo del 40 % anual en todo el mundo. http://www.mckinsey.com/mgi/publications/big_data/.

innovación[2]. Una modernización de la normativa de la UE en materia de protección de datos que potencie la dimensión de mercado interior garantizará a los ciudadanos un alto nivel de protección de datos y fomentará la seguridad, la claridad y la coherencia jurídicas. Por lo tanto, ocupa un lugar destacado en el Plan de Acción de Estocolmo de la Comisión Europea[3], en la Agenda Digital para Europa[4] y, de forma más general, en la estrategia de crecimiento de la UE Europa 2020[5].

La Directiva de la UE de 1995[6], instrumento legislativo básico para la protección de los datos personales en Europa, marcó un hito en la historia de la protección de datos. Sus objetivos, a saber, asegurar el funcionamiento del mercado único y la protección efectiva de los derechos y las libertades de los ciudadanos, siguen siendo válidos. No obstante, se adoptó hace diecisiete años, momento en que Internet estaba aún en una fase incipiente. En el nuevo y complejo entorno digital actual, las normas vigentes no aportan ni el grado de armonización requerido ni la eficacia necesaria para preservar el derecho a la protección de datos personales. Tal es el motivo de que la Comisión Europea proponga una reforma fundamental del marco jurídico de protección de datos en la UE.

Además, el Tratado de Lisboa ha creado, a través del artículo 16 del TFUE, una nueva base jurídica para un planteamiento moderno y global de la protección y la libre circulación de datos personales, que abarca también la cooperación policial y judicial en materia penal[7]. Ese enfoque se refleja en las Comunicaciones de la Comisión Europea sobre el Programa de Estocolmo y el Plan de Acción de Estocolmo[8], que subrayan la necesidad de que la Unión se dote de un «régimen único de protección de los datos personales que cubra el conjunto de las competencias de la Unión» y garantice «la aplicación coherente del derecho fundamental a la protección de datos».

Para preparar la reforma del marco jurídico de protección de datos de la UE de manera transparente, la UE ha organizado, desde 2009, varias rondas de consultas públicas sobre protección de datos[9] y ha entablado un diálogo intensivo con los interesados[10]. El 4 de noviembre de 2010, la Comisión publicó una Comunicación

---

2 Véanse también las conclusiones del Consejo Europeo de 23 de octubre de 2011, en las que se subraya el papel crucial del mercado único «para la creación de crecimiento y empleo», así como la necesidad de implantar el mercado único digital antes de que termine 2015.

3 COM(2010) 171 final.

4 COM(2010) 245 final.

5 COM(2010) 2020 final.

6 Directiva 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, DO L 281 de 23.11.1995, p. 31.

7 Las normas específicas para el tratamiento de datos del ámbito de la Política Exterior y de Seguridad Común por parte de los Estados miembros se fijarán en una Decisión del Consejo basada en el artículo 39 del TFUE.

8 Véanse, respectivamente, los documentos COM(2009) 262 y COM(2010) 171.

9 Se han abierto dos consultas públicas sobre la reforma de la protección de datos: la primera se desarrolló entre julio y diciembre de 2009 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm) y la segunda entre noviembre de 2010 y enero de 2011 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm).

10 En 2010 se llevaron a cabo consultas específicas con las autoridades y los interesados del sector privado de los Estados miembros. En noviembre de 2010, la Comisaria de Justicia Viviane Reding organizó una mesa redonda sobre la reforma de la protección de datos. A lo largo de 2011 se celebraron otros talleres y seminarios sobre aspectos específicos (por ejemplo, notificaciones de las violaciones de datos).

acerca del enfoque global de la protección de los datos personales en la Unión Europea[11] en la que se exponían los principales aspectos de la reforma. Entre septiembre y diciembre de 2011, la Comisión participó en un diálogo intensificado con las autoridades nacionales de protección de datos en Europa y con el Supervisor Europeo de Protección de Datos a fin de explorar las opciones que podrían conducir a una aplicación más coherente de las normas de protección de datos en todos los Estados miembros de la UE[12].

Estas conversaciones dejaron claro que tanto los ciudadanos como las empresas deseaban que la Comisión Europea procediese a una reforma general de las normas de protección de datos de la UE. Tras evaluar las repercusiones de las distintas opciones[13], la Comisión Europea ha decidido proponer **un marco legislativo sólido y coherente que cubre todas las políticas de la Unión, refuerza los derechos individuales, potencia la dimensión de mercado único de la protección de datos y reduce los trámites burocráticos engorrosos para las empresas**[14]. Así pues, la Comisión propone que el nuevo marco conste de:

– Un **Reglamento** (que sustituye a la Directiva 95/46/CE) en el que se fija el marco jurídico general de protección de datos de la UE[15]

– y una Directiva (que sustituye a la Decisión Marco 2008/977/JAI[16]), que fija las normas sobre la protección de los datos personales tratados con fines de **prevención, detección, investigación o persecución de delitos y para las actividades judiciales correspondientes**.

En la presente Comunicación se exponen los principales componentes de la reforma del marco jurídico para la protección de datos de la UE.

2. CONTROL DE LOS CIUDADANOS SOBRE SUS DATOS PERSONALES

Conforme a la Directiva 95/46/CE, principal acto legislativo de la UE actualmente vigente en el ámbito de la protección de datos, las vías de que disponen los

---

11 COM (2010) 609.

12 Véase la carta de la Comisaria de Justicia de la UE, Viviane Reding, de 19 de septiembre de 2011 a los miembros del Grupo de trabajo del artículo 29, publicada en http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm

13 Véase la evaluación de impacto SEC(2012) 72.

14 Esta intervención incluirá, en una fase posterior, modificaciones destinadas a armonizar instrumentos específicos y sectoriales, en particular el Reglamento (CE) nº 45/2001 (DO L 8 de 12.1.2001, p. 1).

15 El Reglamento introduce asimismo un número limitado de ajustes técnicos en la Directiva sobre privacidad y comunicaciones electrónicas (Directiva 2002/58/CE, modificada en último lugar por la Directiva 2009/136/CE, DO L 337 de 18.12.2009, p. 11) que reflejan la transformación de la Directiva 95/46/CE en Reglamento. Las consecuencias legales sustantivas del nuevo Reglamento y de la nueva Directiva para la Directiva sobre privacidad en las comunicaciones electrónicas serán objeto, en su momento, de un examen por parte de la Comisión en el que se tendrá en cuenta el resultado de las negociaciones de las propuestas actuales con el Parlamento Europeo y el Consejo.

16 Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de los datos personales tratados en el marco de la cooperación policial y judicial en materia penal, DO L 350 de 30.12.2008, p. 60. Como parte del paquete de reforma de las normas de protección de datos, se ha adoptado un informe sobre la aplicación de la Decisión Marco por parte de los Estados miembros (COM(2012)12).

ciudadanos para ejercer el derecho a la protección de sus datos no están lo suficientemente armonizadas entre los Estados miembros. Idéntica deficiencia presentan las facultades de las autoridades nacionales de protección de datos, lo que les impide asegurar una aplicación coherente y efectiva de las normas. Dicho de otro modo, el ejercicio efectivo de esos derechos (especialmente cuando se trata de datos en línea) es más difícil en unos Estados miembros que en otros.

Esas dificultades se derivan también del enorme volumen de datos recogidos diariamente y del hecho de que los usuarios a menudo no son plenamente conscientes de que sus datos están siendo recogidos. Si bien son muchos los europeos que consideran que la comunicación de sus datos personales forma cada vez más parte de la vida moderna[17], el 72 % de los usuarios de Internet en Europa siguen preocupados ante la excesiva cantidad de datos personales que se les solicita en línea[18]. Ello les procura la sensación de haber perdido el control sobre sus datos, puesto que no reciben información adecuada acerca del destino de sus datos personales, a quién se transmiten y con qué fines. A menudo, no saben cómo ejercer sus derechos en línea.

El «derecho al olvido»

Un estudiante europeo suscrito a un servicio de red social en línea decide solicitar acceso a todos sus datos personales archivados por la red. Es entonces cuando se da cuenta de que esos datos son muchos más de lo que había imaginado y de que algunos de sus datos personales que, en teoría, habían sido suprimidos, se siguen conservando.

La reforma de las normas sobre protección de datos de la UE garantizarán que esa situación deje de producirse, mediante la introducción de las disposiciones siguientes:

- un requisito explícito que obliga a los servicios de redes sociales en línea (y a todos los demás responsables del tratamiento de datos) a minimizar el volumen de datos personales de usuarios recogidos y tratados;

- el requisito de que la configuración por defecto garantice que los datos no se hacen públicos;

- la obligación explícita para los responsables del tratamiento de datos de suprimir los datos personales de quienes así lo soliciten explícitamente, cuando no exista ninguna razón legítima para conservarlos.

En el ejemplo antes expuesto, este requisito obligaría al proveedor de la red social a suprimir inmediata y totalmente los datos del estudiante.

Como ya se pone de manifiesto en la Agenda Digital para Europa, las preocupaciones acerca de la falta de privacidad se encuentran entre las razones más frecuentes por las que los ciudadanos no compran bienes ni contratan servicios en línea. Habida cuenta de la contribución del sector de las tecnologías de la información y la comunicación (TIC) al aumento de la productividad general en Europa (un 20 % procede directamente del sector de TIC, y un 30 % de las

[17] Véase el Eurobarómetro especial 359 – Actitudes frente a la protección de datos y a la identidad electrónica en la Unión Europea, junio de 2011, p. 23.

[18] *Ibídem*, apartado 54.

inversiones en TIC[19]), la confianza en esos servicios es vital para estimular el crecimiento de la economía de la UE y la competitividad de la industria europea.

Notificaciones de las violaciones de datos

Unos piratas informáticos asaltaron un servicio de juegos en línea dirigido a usuarios de la UE. Esa violación afectó a bases de datos que contenían datos personales (incluidos los nombres y apellidos, las direcciones y posiblemente los datos de las tarjetas de crédito) de millones de usuarios de todo el mundo. La empresa dejó pasar una semana antes de notificar el suceso a los usuarios afectados.

La reforma de las normas sobre protección de datos de la UE asegurará que esa situación deje de producirse. Las nuevas normas obligarán a las empresas:

- a reforzar sus medidas de seguridad para impedir y evitar violaciones;

- a notificar las violaciones de datos tanto a las autoridades nacionales de protección de datos (en un plazo de 24 desde la detección de la violación, siempre que sea posible) como a las personas afectadas, sin demora indebida.

El objetivo de los nuevos actos legislativos propuestos por la Comisión es reforzar los derechos vigentes, otorgar a los ciudadanos medios eficaces y operativos para asegurarse de que están plenamente informados del destino de sus datos personales y posibilitarles un ejercicio más efectivo de sus derechos.

Para reforzar los derechos de los ciudadanos a la protección de sus datos, la Comisión propone nuevas normas que:

Aumentarán el control de los ciudadanos sobre sus datos:

- asegurando que, siempre que se requiera su **consentimiento**, este se otorgue **de forma explícita, a saber, mediante una declaración o una actuación clara y afirmativa por parte del interesado**, y libre;

- dotando a los usuarios de Internet de un **derecho efectivo al olvido** en el entorno en línea: el derecho a que se supriman sus datos si retiran su consentimiento y no existen otros motivos legítimos para conservarlos;

- garantizando un **acceso fácil a los datos propios** y un derecho de **portabilidad de los datos**: el derecho a obtener del responsable del tratamiento una copia de los datos conservados y la libertad de transferirlos de un proveedor de servicio a otros sin trabas;

- reforzando el **derecho a la información** de tal forma que los ciudadanos comprendan plenamente cómo se tratan sus datos personales, especialmente cuando esas actividades afecten a **niños**.

Mejorarán los medios que permiten a los ciudadanos ejercer sus derechos:

- reforzando la **independencia y las competencias de las autoridades nacionales de protección de datos** de forma que estén adecuadamente equipadas para dar curso eficazmente a las reclamaciones, estén facultadas para llevar a cabo

[19] Véase la Agenda Digital para Europa, p.4.

investigaciones efectivas, adopten decisiones vinculantes e impongan sanciones efectivas y disuasorias;

- ensanchando **las vías de recurso administrativo y judicial** en caso de **violación** de los derechos de protección de datos. Concretamente, las asociaciones debidamente habilitadas podrán ejercitar acciones judiciales en nombre de los particulares.

Reforzarán la seguridad de los datos:

- fomentando el uso de **tecnologías que protejan la privacidad** (tecnologías que, al minimizar la conservación de datos personales, resguardan la privacidad de la información), **configuraciones por defecto respetuosas de la privacidad** y **regímenes de certificación de la privacidad**;

- imponiendo a los responsables del tratamiento de los datos **una obligación general**[20] **de notificar, sin demora indebida, toda violación de datos** tanto a las autoridades competentes en materia de protección de datos (en un plazo de 24 horas siempre que sea posible) como a los afectados.

Acrecentará la responsabilidad de quienes tratan datos, concretamente:

- exigiendo a los responsables del tratamiento de los datos que nombren a un **Delegado de Protección de Datos** en las empresas con más de 250 empleados y en las empresas que efectúen operaciones de tratamiento de datos que entrañen cierto riesgo;

- introduciendo el principio de «**privacidad desde el diseño**» a fin de asegurar que las garantías de protección de los datos se incorporan ya en la fase de planificación de los procedimientos y sistemas;

- imponiendo a las organizaciones que lleven a cabo operaciones de tratamiento que entrañen cierto riesgo la obligación de llevar a cabo **evaluaciones de impacto sobre la protección de los datos**.

3. NORMAS DE PROTECCIÓN DE DATOS ADAPTADAS AL MERCADO ÚNICO DIGITAL

A pesar de que la Directiva vigente tiene el objetivo de asegurar un nivel equivalente de protección de datos en toda la UE, se observan aún considerables divergencias entre las normas aplicables en los distintos Estados miembros. De tal modo, los responsables del tratamiento de datos pueden tener que hacer frente a 27 legislaciones nacionales y requisitos diferentes. El resultado de esa situación es un **entorno jurídico fragmentado** que ha generado **inseguridad jurídica** y protección desigual de las personas físicas. Además, ha generado **costes innecesarios y cargas administrativas** para las empresas y actúa como desincentivo para aquellas que operan en el mercado único y desearían expandir sus operaciones a otros países.

[20] Actualmente, tal obligación existe únicamente en el sector de las telecomunicaciones, en virtud de la Directiva sobre privacidad y comunicaciones electrónicas.

Los recursos y las competencias de las autoridades nacionales de protección de datos varían considerablemente entre los Estados miembros[21]. En algunos casos, dichas autoridades se ven en la imposibilidad de ejercer satisfactoriamente sus funciones coercitivas. La cooperación a nivel europeo entre estas autoridades a través del grupo consultivo existente (el llamado Grupo de trabajo del artículo 29)[22] no siempre conduce a una aplicación coherente de las normas, aspecto que también es susceptible de mejora.

Aplicación coherente de las normas de protección de datos en toda Europa

Una empresa multinacional con varios establecimientos en la UE ha desplegado un sistema de cartografía en línea en toda Europa que capta imágenes de todos los edificios privados y públicos, por lo que puede al mismo tiempo obtener fotografías de los viandantes. En un Estado miembro, la inclusión de fotografías no desenfocadas de personas que no eran conscientes de haber sido fotografiadas se consideró ilegal, mientras que en otros Estados miembros ese hecho no supuso ninguna infracción de las leyes de protección de datos. Por consiguiente, las autoridades nacionales de protección de datos no ofrecieron una respuesta homogénea para poner remedio a esta situación.

La reforma de las normas de protección de datos de la UE asegurará que esa situación deje de producirse, dado que:

- los requisitos y las garantías de protección de datos se establecerán en un Reglamento de la UE, de aplicación directa en toda la Unión;

- únicamente la autoridad de protección de datos del país donde la empresa tenga su establecimiento principal será responsable de determinar si la actuación de la empresa se ajusta a Derecho;

- una coordinación rápida y eficaz entre las autoridades nacionales de protección de datos (habida cuenta de que el servicio se destina a ciudadanos de varios Estados miembros) contribuirá a asegurar que las nuevas normas de protección de datos de la UE sean objeto de aplicación y ejecución coherentes en todos los Estados miembros.

Es preciso conceder refuerzos a las autoridades nacionales e intensificar sus actividades de cooperación para asegurar una ejecución coherente y, en definitiva, una aplicación uniforme de las reglas en toda la UE.

La existencia de un marco legislativo sólido, claro y uniforme al nivel de la UE contribuirá a liberar el potencial del mercado único digital y propiciará el crecimiento económico, la innovación y la creación de empleo. Mediante un Reglamento, se acabará con la fragmentación de regímenes legales en los 27 Estados miembros y se eliminarán los obstáculos que entorpecen al acceso al mercado, factor de especial importancia para las microempresas y para las pequeñas y medianas empresas.

Las nuevas normas otorgarán además a las empresas de la UE una ventaja competitiva mundial. Gracias al marco regulador reformado, podrán asegurar a sus clientes que toda información personal valiosa será tratada con la diligencia y el cuidado debidos. La confianza en un régimen regulador coherente de la UE

[21] Para más pormenores sobre esta cuestión, véase la evaluación de impacto adjunta a las propuestas legislativas, SEC(2012) 72.

[22] El Grupo de trabajo del artículo 29, que se creó en 1996 (en virtud del artículo 29 de la Directiva) con carácter consultivo, se compone de representantes de las autoridades nacionales de protección de datos, el Supervisor Europeo de Protección de Datos (SEPD) y la Comisión. Para más información sobre sus actividades véase: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

constituirá una ventaja esencial para los proveedores de servicios, además de un incentivo para los inversores en busca de condiciones óptimas para la localización de servicios.

Con el fin de potenciar la **dimensión de mercado único de la protección de datos**, la Comisión propone:

- fijar las normas de protección de datos al nivel de la UE mediante un **Reglamento directamente aplicable en todos los Estados miembros**[23], lo que pondrá fin a la aplicación acumulativa y simultánea de distintas leyes nacionales de protección de datos; **solo en el capítulo de cargas administrativas**, esto supondrá **para las empresas un ahorro neto de unos 2 300 millones EUR;**

- **simplificar el entorno regulador mediante una drástica reducción de los trámites burocráticos** y la eliminación de determinadas **formalidades**, como los requisitos generales de notificación (solo en el capítulo de cargas administrativas, esto supondrá un ahorro neto de 130 millones EUR anuales); habida cuenta de su importancia para la competitividad de la economía europea, se otorgará especial atención a las necesidades específicas de las microempresas y de las pequeñas y medianas empresas;

- **ampliar la independencia y las facultades de las autoridades nacionales de protección de datos**, habilitándolas para llevar a cabo investigaciones, adoptar decisiones vinculantes e imponer sanciones efectivas y disuasorias, y obligar a los Estados miembros a que les faciliten los **recursos suficientes** para el desempeño de esas tareas;

- **crear un sistema de «ventanilla única» para la protección de datos en la UE:** los responsables del tratamiento de datos de la UE tendrán como único interlocutor a **una autoridad nacional de protección de datos**, a saber, la del Estado miembro donde esté sito el establecimiento principal;

- crear las condiciones necesarias para una **cooperación presta y eficaz entre autoridades nacionales de protección de datos**, lo que incluirá la obligación para cualquiera de ellas de llevar a cabo investigaciones e inspecciones a petición de cualquier otra y el reconocimiento mutuo de sus decisiones;

- **crear un mecanismo de coherencia** al nivel de la UE para asegurar que las decisiones de las autoridades nacionales de protección de datos que tengan mayor repercusión europea tengan plenamente en cuenta los puntos de vista de las demás autoridades de protección de datos interesadas y se ajusten plenamente al Derecho de la UE;

- elevar el rango del Grupo de trabajo del artículo 29, convirtiéndolo en un **Consejo Europeo de Protección de Datos** a fin de mejorar su contribución a la aplicación coherente de la legislación en materia de protección de datos y de sentar unas sólidas bases de cooperación entre las autoridades de protección de datos,

[23] Para establecer las normas aplicables a la cooperación policial y judicial en materia penal (véase el apartado 4), se propone una Directiva, instrumento que otorgará a los Estados miembros más flexibilidad en este ámbito específico.

incluido el Supervisor Europeo de Protección de Datos, y potenciar las sinergias y la eficacia disponiendo que este último asuma las tareas de la Secretaría del Consejo Europeo de Protección de Datos.

El nuevo Reglamento de la UE garantizará una firme protección del derecho fundamental a la protección de datos en toda la Unión Europea y consolidará el funcionamiento del mercado único. Al mismo tiempo, habida cuenta de que, según ha subrayado el Tribunal de Justicia de la UE[24], el derecho a la protección de los datos personales no constituye un derecho absoluto, sino que debe considerarse en relación con su función dentro de la sociedad[25] y presentar un equilibrio con otros derechos fundamentales, de conformidad con el principio de proporcionalidad[26], el Reglamento incluirá disposiciones explícitas que garanticen el respeto de otros derechos fundamentales, como la libertad de expresión y de información y el derecho de defensa, así como el secreto profesional (por ejemplo, para la abogacía), sin perjuicio del estatuto jurídico de las iglesias conforme a las leyes de los Estados miembros.

4. UTILIZACIÓN DE LOS DATOS PARA LA COOPERACIÓN POLICIAL Y JUDICIAL EN MATERIA PENAL

La entrada en vigor del Tratado de Lisboa y, concretamente, la introducción de una nueva base jurídica (artículo 16 del TFUE) permiten establecer un marco completo de protección de datos que asegure un alto nivel de protección de los datos personales sin menoscabo de la naturaleza específica de la cooperación policial y judicial en materia penal. En particular, permite que el marco revisado de protección de datos de la UE regule el tratamiento tanto nacional como internacional de datos personales. En principio, ello recortará las diferencias entre las legislaciones de los distintos Estados miembros, lo que probablemente redundará en beneficio de la protección de datos personales en general. También podría dar lugar a un intercambio más fluido de información entre las autoridades policiales y judiciales de los Estados miembros, lo que mejorará la cooperación en la lucha contra la delincuencia grave en Europa. Actualmente, el tratamiento de datos por las autoridades policiales y judiciales en materia penal lo regula esencialmente la Decisión Marco 2008/977/JAI, anterior a la entrada en vigor del Tratado de Lisboa. Dado que se trata de una Decisión marco, la Comisión carece de competencia para exigir el cumplimiento de sus disposiciones, lo que ha contribuido a su desigual aplicación. Además, el ámbito de aplicación de la Decisión Marco se limita a las actividades de tratamiento de datos internacionales[27]. Esto significa que el

---

24 Tribunal de Justicia de la UE, sentencia de 9.11.2010 en los asuntos acumulados C-92/09 y C-93/09, Volker y Markus Schecke y Eifert [2010], aún no publicada en la Recopilación.

25 De conformidad con el artículo 52, apartado 1, de la Carta, pueden imponerse limitaciones al ejercicio del derecho a la protección de datos, siempre que esas limitaciones hayan sido establecidas por ley, respeten el contenido esencial del derecho y las libertades y, en cumplimiento del principio de proporcionalidad, sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión Europea o a la necesidad de protección de los derechos y libertades de los demás.

26 Tribunal de Justicia de la UE, sentencia de 6.11.2003, C-101/01, Lindqvist [2003], Rec. I-12971, apartados 82-90; sentencia de 16.12.2008, C-73/07, Satamedia [2008], Rec. I-9831, apartados 50-62.

27 Más precisamente, la Decisión Marco se aplica a los datos personales que son o han sido transmitidos o puestos a disposición entre Estados miembros o intercambiados entre Estados miembros e instituciones u organismos de la UE (véase el artículo 1, apartado 2).

tratamiento de datos personales que no haya sido objeto de intercambio queda actualmente fuera del ámbito de aplicación de las disposiciones de la UE que regulan ese tratamiento y salvaguardan el derecho fundamental a la protección de datos. Además, en algunos casos, esto crea una dificultad práctica a la policía y otras autoridades, para quienes no siempre está claro si el tratamiento de datos ha de ser exclusivamente nacional o internacional, o si los datos nacionales pueden ser objeto de un intercambio internacional subsiguiente[28].

Por consiguiente, el nuevo marco reformado de protección de datos de la UE trata de garantizar un nivel elevado y sistemático de protección de los datos que **fomente la confianza mutua entre la policía y las autoridades judiciales de los distintos Estados miembros, contribuyendo con ello a mejorar la libre circulación de datos y la cooperación efectiva entre la policía y las autoridades judiciales**.

Con el fin de asegurar un alto nivel de protección de los datos personales en el ámbito de la cooperación policial y judicial en materia penal y de facilitar los intercambios de datos personales entre la policía y las autoridades judiciales de los Estados miembros, la Comisión propone, como parte del paquete de reforma de la protección de datos, una Directiva que:

- **aplique los principios generales de la protección de datos** a la cooperación policial y judicial en materia penal, siempre en total respeto de la naturaleza específica de cada uno de estos ámbitos[29];

- establezca **condiciones y criterios mínimos armonizados para toda posible limitación de las reglas generales**; esto se refiere específicamente a los derechos de los ciudadanos a ser informados cuando la policía y las autoridades judiciales manejen sus datos o accedan a ellos; esas limitaciones son necesarias para la prevención, investigación, detección o enjuiciamiento efectivos de los delitos;

- establezca **normas específicas adaptadas a la naturaleza característica de las actividades de los organismos con funciones coercitivas, incluida una distinción entre las distintas categorías de interesados**, cuyos derechos pueden variar (como los testigos y los sospechosos).

5. PROTECCIÓN DE LOS DATOS EN UN CONTEXTO DE GLOBALIZACIÓN

La protección de los derechos de los ciudadanos debe extenderse a la transferencia de datos personales de la UE a terceros países y a toda actividad que se dirija a los ciudadanos de los Estados miembros y en el marco de la cual sus datos sean utilizados o analizados por proveedores de servicios de terceros países. Esto significa que las normas de protección de datos de la UE deben aplicarse con independencia de la ubicación geográfica de una empresa o de su centro de tratamiento de datos.

[28] Este extremo fue confirmado por varios Estados miembros en su respuesta al cuestionario de la Comisión para el Informe de aplicación de la Decisión Marco (COM(2012)12).

[29] Véase la Declaración nº 21 relativa a la protección de datos de carácter personal en el ámbito de la cooperación judicial en materia penal y de la cooperación policial, aneja al Acta Final de la Conferencia Gubernamental que adoptó el Tratado de Lisboa.

En el contexto de globalización actual, los datos personales se transfieren a través de un creciente número de fronteras virtuales y geográficas, y se conservan en servidores ubicados en numerosos países. Aumenta el número de empresas que ofrecen a sus clientes servicios de computación en nube que les permiten consultar y conservar los datos guardados en servidores remotos. Estos factores exigen una mejora de los actuales mecanismos de transferencia de datos a terceros países que incluya decisiones de adecuación (es decir, decisiones que certifiquen la adecuación de las normas de protección de datos de terceros países), amén de las garantías apropiadas, como cláusulas contractuales tipo o normas corporativas vinculantes[30], para garantizar un alto nivel de protección de los datos en las operaciones internacionales de tratamiento de datos y de facilitar el flujo transfronterizo de datos.

Normas corporativas vinculantes

Un grupo de sociedades necesita transferir periódicamente datos personales desde sus filiales en la UE a las radicadas en terceros países. El grupo desearía introducir una serie de normas corporativas vinculantes (NCV) que permitan cumplir el Derecho de la UE, limitando, al mismo tiempo, los requisitos administrativos de cada transferencia. En la práctica, las normas corporativas vinculantes aseguran la aplicación de un único conjunto de normas a todo el grupo en lugar de varios contratos internos.

De acuerdo con las prácticas vigentes acordadas por el Grupo de trabajo del artículo 29, para reconocer que las normas vinculantes de una sociedad ofrecen garantías suficientes se necesita un examen pormenorizado por parte de tres autoridades responsables de la protección de datos (una «principal» y dos «examinadoras»), que puede complementarse con las observaciones de otros responsables. Además, la legislación de muchos Estados miembros exige autorizaciones nacionales adicionales para las transferencias efectuadas con arreglo a las normas corporativas vinculantes, lo que hace de su adopción un proceso muy engorroso, costoso, largo y complejo.

A partir de la reforma de la protección de datos:

- este proceso se simplificará y racionalizará;

- las normas corporativas vinculantes serán validadas por una única autoridad responsable de protección de datos, con mecanismos para asegurar la pronta participación de las demás autoridades de protección de datos pertinentes;

- una vez una autoridad haya aprobado una norma corporativa vinculante, esta será válida para toda la UE sin necesidad de autorizaciones adicionales a nivel nacional.

Los retos que plantea la globalización requieren herramientas y mecanismos flexibles, especialmente para las empresas activas en todo el mundo, que garanticen al mismo tiempo la protección sin fisuras jurídicas de los datos personales. La Comisión propone las medidas siguientes:

30 Por normas corporativas vinculantes se entienden los códigos de buenas prácticas basados en las normas de protección de datos europeas y aprobados al menos por una autoridad de control de la protección de datos, que las entidades elaboran de manera voluntaria y suscriben a fin de asegurar las salvaguardias necesarias para determinadas categorías de transferencias de datos personales entre empresas que forman parte del mismo grupo de sociedades y están vinculadas por esas normas. No están explícitamente reguladas por la Directiva 95/46/CE pero han surgido como práctica entre las autoridades nacionales de control de la protección de datos, con el apoyo del Grupo de trabajo del artículo 29.

- adopción de **normas claras** que determinen en qué supuestos se aplica **el Derecho de la UE a los responsables del tratamiento de datos establecidos en terceros países** y que, en particular, especifiquen que siempre que se ofrezcan bienes y servicios a ciudadanos de la UE, o cuando se proceda a algún control de su comportamiento, **serán de aplicación las normas europeas**;

- toda **decisión de adecuación** que la Comisión adopte, incluso en el ámbito de la cooperación policial y la justicia penal, se basará en criterios explícitos y claros;

- la circulación legítima de datos a terceros países se facilitará reforzando y simplificando **las normas sobre transferencias internacionales** de datos a los países no cubiertos por ninguna decisión de adecuación, y sobre todo racionalizando ciertas herramientas (como por ejemplo las **normas corporativas vinculantes**) y generalizando su uso, de forma que puedan aplicarse a los **responsables del tratamiento de datos** y dentro de los **grupos de sociedades**, lo que reflejará mejor el número de empresas que llevan a cabo actividades de tratamiento de datos, especialmente mediante computación en nube;

- apertura de un **diálogo** y, cuando así proceda, **negociaciones** con terceros países –especialmente los socios estratégicos de la UE y los países de la Política Europea de Vecindad– y con las organizaciones internacionales pertinentes (como el Consejo de Europa, la Organización para la Cooperación y el Desarrollo Económico, las Naciones Unidas) a fin de **promover la adopción de unas normas de protección de datos exigentes e interoperables** en todo el mundo.

6. CONCLUSIÓN

La reforma de la protección de datos de la UE pretende configurar un **marco moderno, sólido, coherente y global de protección de datos para la Unión Europea** que reforzará el derecho fundamental de los ciudadanos a la protección de sus datos. Se respetarán otros derechos como la libertad de expresión e información, los derechos del niño, el derecho a la actividad empresarial, el derecho a un juicio justo y el secreto profesional (por ejemplo, para la abogacía), así como el estatuto jurídico de las iglesias conforme a la legislación de los Estados miembros.

La reforma beneficiará en primer lugar a los particulares, ya que consolidará sus derechos a la protección de datos y aumentará su confianza en el entorno digital. Además, la reforma simplificará considerablemente el marco jurídico tanto para las empresas como para el sector público, intervención que se espera estimule el desarrollo de la economía digital dentro de la UE y allende sus fronteras, conforme a los objetivos de la estrategia Europa 2020 y a la Agenda Digital para Europa. Por último, la reforma aumentará la confianza entre las autoridades con funciones coercitivas con el fin de facilitar el intercambio de datos y la cooperación en la lucha contra la delincuencia grave, asegurando al mismo tiempo un alto nivel de protección a los ciudadanos.

La Comisión Europea trabajará en estrecha colaboración con el Parlamento Europeo y el Consejo para garantizar la obtención de un acuerdo acerca del nuevo marco de protección de datos de la UE antes de que concluya 2012. A lo largo de todo este proceso de aprobación e incluso después, especialmente en el contexto de la

aplicación de los nuevos instrumentos legales, la Comisión mantendrá un **diálogo intenso y transparente con todas las partes**, con la participación de representantes del sector privado y público. Entre ellos figurarán representantes de la policía y la judicatura, organizaciones de la sociedad civil, además de autoridades y expertos en materia de protección de datos y de las agencias especializadas de la UE como Eurojust, Europol y la Agencia Europea de Seguridad de las Redes y de la Información.

En un contexto de constante desarrollo de las tecnologías y de cambio en las costumbres sociales, ese diálogo reviste una importancia crucial para disponer de la información necesaria para asegurar un alto nivel de protección de los datos personales, el crecimiento y la competitividad de la industria de la UE, la eficacia de la administración pública (incluida la policía y el poder judicial) y un bajo volumen de cargas administrativas.