ES

COMISIÓN EUROPEA

Bruselas, 4.11.2010
COM(2010) 609 final

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

Un enfoque global de la protección de los datos personales en la Unión Europea

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

Un enfoque global de la protección de los datos personales en la Unión Europea

1. NUEVOS RETOS EN MATERIA DE PROTECCIÓN DE LOS DATOS PERSONALES

La Directiva relativa a la protección de datos de 1995[1] estableció un hito en la historia de la protección de los datos personales en la Unión Europea. Consagra dos de las más antiguas ambiciones del proceso de integración europea: por una parte, la protección de los derechos y libertades fundamentales de las personas, en particular, del derecho fundamental a la protección de datos, y, por otra parte, la realización del mercado interior, es decir, en este caso, la libre circulación de datos personales.

Quince años más tarde, este doble objetivo sigue teniendo vigencia y los principios consagrados en la Directiva siguen siendo válidos. **Sin embargo, la rapidez de la evolución tecnológica y la globalización han modificado profundamente nuestro medio y han lanzado nuevos retos en materia de protección de los datos personales.**

En la actualidad, 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 podría plantear 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. Un reciente estudio ha confirmado que 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 en línea[2].

Paralelamente, **los métodos de recogida de los datos personales son cada vez más complicados y se detectan con más dificultad**. Por ejemplo, la utilización de herramientas sofisticadas permite a los agentes económicos localizar mejor a las personas, mediante el registro de su comportamiento. 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 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

---

1 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 de 23.11.1995, p. 31).

2 Véase *Study on the economic benefits of privacy enhancing technologies*, London Economics, julio de 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf), p. 14.

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 plantean inevitablemente la cuestión de si la legislación de la Unión Europea en materia de protección de datos es capaz de hacer frente plena y eficazmente a estos retos.

Para responder a esta cuestión, la Comisión inició un examen del marco jurídico actual, con una conferencia de alto nivel en mayo de 2009, seguida de una consulta pública hasta finales de 2009[3]. También se iniciaron varios estudios[4].

Los resultados obtenidos confirman 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 cuya resolución supone retos específicos. Se trata, en especial, de lo siguiente:

- *Abordar el impacto de las nuevas tecnologías*

Las respuestas recibidas a las consultas, tanto de particulares como de organizaciones, confirman la 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. Se ha respondido parcialmente a esta necesidad por medio de la Directiva 2002/58/CE (la llamada «Directiva sobre la privacidad y las comunicaciones electrónicas»)[5], que especifica y completa la Directiva general relativa a la protección de datos en el sector de las comunicaciones electrónicas[6].

---

3 Véanse las respuestas a la consulta pública organizada por la Comisión: http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm. A lo largo de 2010 tuvieron lugar consultas más específicas de las partes interesadas. La Vicepresidenta Viviane Reding también presidió una reunión de alto nivel con las partes involucradas, que se celebró el 5 de octubre de 2010 en Bruselas. Por otra parte, la Comisión consultó al Grupo de Trabajo del Artículo 29, que aportó una amplia contribución a la consulta de 2009 (documento WP 168) y adoptó en julio de 2010 un dictamen específico sobre el principio de responsabilidad (documento WP 173).

4 Además del *Study on the economic benefits of privacy enhancing technologies* (véase la nota a pie de página n° 2), véase también el *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, enero de 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf). También está en curso un estudio sobre un análisis de impacto para el futuro marco jurídico de la UE en materia de protección de datos.

5 Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

6 La Directiva 95/46/CE sobre protección de datos establece las normas de protección de datos para todos los actos legislativos de la UE, incluida la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas (modificada por la Directiva 2009/136/CE - DO L 337, de 18.12.2009, p. 11). La Directiva sobre la privacidad y las comunicaciones electrónicas se aplica al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones. Traduce los principios fijados en la Directiva sobre

- *Reforzar la dimensión de mercado interior de la protección de datos*

Una de las preocupaciones recurrentes de las partes involucradas, y en particular de las empresas multinacionales, es la insuficiente 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. Estas empresas han destacado 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.

- *Hacer frente a la globalización y mejorar las transferencias internacionales de datos*

Algunas partes involucradas destacaron que 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, numerosas organizaciones consideraron que los regímenes actuales no son plenamente satisfactorios y que deben revisarse y racionalizarse para simplificar las transferencias y hacerlas menos pesadas.

- *Consolidar las disposiciones institucionales para la aplicación efectiva de las normas sobre protección de datos*

Existe un consenso entre las partes involucradas 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. Algunas organizaciones pidieron también una mayor transparencia de los trabajos del Grupo de Trabajo del Artículo 29 (*véase el apartado 2.5*), y la clarificación de su misión y poderes.

- *Mejorar la coherencia del marco jurídico que regula la protección de datos*

En la consulta pública, todas las partes involucradas destacaron la necesidad de disponer de 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[7].

Los retos previamente mencionados **requieren que la UE elabore 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**. El Tratado de Lisboa dotó a la Unión de medios suplementarios para afrontar estos retos: la Carta de los Derechos Fundamentales de la UE - cuyo artículo 8 reconoce un derecho autónomo a la protección de los datos personales - es en adelante jurídicamente vinculante, y se ha creado una nueva base jurídica[8], que permite la elaboración de una normativa de la Unión global y coherente en materia de protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos. Esta nueva base jurídica autoriza, en particular, a la Unión

---

protección de datos en normas específicas para el sector de las comunicaciones electrónicas. La Directiva 95/46/CE se aplica a los servicios de comunicaciones electrónicas que no sean de carácter público.

7 En contribuciones separadas realizadas tras el fin de la consulta pública, Europol y Eurojust abogaron por tener en cuenta las especificidades de su trabajo relativo a la coordinación de la aplicación de la ley y la prevención de la delincuencia.

8 Véase el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE).

a regular la protección de datos por medio de un único instrumento jurídico, en particular, en los ámbitos de la cooperación policial y la cooperación judicial en materia penal. La Política Exterior y de Seguridad Común sólo está cubierta parcialmente por el artículo 16 TFUE, dado que una decisión del Consejo, con una base jurídica distinta, debe establecer normas específicas aplicables a los tratamientos de datos efectuados por los Estados miembros en este ámbito[9].

Basándose en estas nuevas posibilidades jurídicas, la Comisión concederá la más alta prioridad al respeto del derecho fundamental a la protección de datos 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. En este contexto, procede tener en cuenta plenamente otros derechos fundamentales pertinentes consagrados en la Carta, y otros objetivos enunciados en los Tratados, a la hora de garantizar el derecho fundamental a la protección de los datos personales.

La presente Comunicación tiene por objeto definir el enfoque que permitirá 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 siga garantizando un elevado nivel de protección de los ciudadanos respecto al tratamiento de estos datos en todos estos ámbitos. La Unión seguirá siendo así una fuerza motriz en la promoción de normas estrictas de protección de datos en todo el mundo.

2. OBJETIVOS ESENCIALES DEL ENFOQUE GLOBAL DE LA PROTECCIÓN DE DATOS

2.1. Reforzar los derechos de las personas

2.1.1. Garantizar a las personas una protección adecuada en cualesquiera circunstancias

El objetivo de las normas establecidas en los actuales instrumentos europeos de protección de datos consiste en **proteger los derechos fundamentales de las personas físicas y en particular su derecho a la protección de los datos personales**, de acuerdo con la Carta de los Derechos Fundamentales de la UE[10].

El concepto de «datos personales» es uno de los conceptos clave de la protección de las personas por los instrumentos europeos en vigor en el ámbito de la protección de datos, y es la causa de la imposición de las obligaciones que incumben a los responsables y encargados del tratamiento[11]. La definición del término «datos personales» engloba el conjunto de la información relativa a una persona identificada o identificable, directa o indirectamente. Para determinar si una persona es identificable, «hay que considerar el conjunto de los medios que

---

9 Véase el artículo 16, apartado 2, último párrafo, del TFUE y el artículo 39 del Tratado de la Unión Europea (TUE).

10 Véanse las sentencias del Tribunal de Justicia en los asuntos C-101/01, Bodil Lindqvist, Rec. 2003, p. I-1297, 96, 97, y C-275/06, Productores de Música de España (Promusicae) contra Telefónica de España SAU, Rec. 2008 p. I-271. Véase también la jurisprudencia del Tribunal Europeo de Derechos Humanos, por ejemplo en los siguientes asuntos: S. y Marper contra el Reino Unido, sentencia de 4.12.2008 (nº 30562/04 y 30566/04); y Rotaru contra Rumania, sentencia de 4.5.2000 (nº 28341/95), apartado 55, TEDH 2000-V.

11 Véanse las definiciones de los términos «responsable del tratamiento» y «encargado del tratamiento» en el artículo 2, letras d) y e), de la Directiva 95/46/CE.

puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona»[12]. Este enfoque, deliberadamente elegido por el legislador, presenta la ventaja de ser flexible, lo que permite aplicarlo a distintos casos y evoluciones que afectan a los derechos fundamentales, incluidos los que no eran previsibles en el momento de la aprobación de la Directiva.
No obstante, una consecuencia de este enfoque amplio y flexible es que hay numerosos casos en los que no está claro, al aplicar la Directiva, qué enfoque adoptar: el derecho a la protección de datos de las personas, o el cumplimiento de las obligaciones impuestas por la Directiva a los responsables del tratamiento[13].

Algunas situaciones que implican el tratamiento de información específica requerirían la aprobación de medidas suplementarias en el marco del Derecho de la Unión. Tales medidas ya existen en algunos casos. Por ejemplo, la conservación de datos en un terminal (por ejemplo, un teléfono móvil) sólo se autoriza si la persona ha dado su consentimiento. Esta cuestión también deberá abordarse a escala de la Unión por lo que se refiere, por ejemplo, a los datos codificados, los datos de localización, las tecnologías de extracción de datos que permiten relacionar datos que emanan de fuentes diferentes, o siempre que sea necesario garantizar la confidencialidad y la integridad de los sistemas de información[14].

Todas las cuestiones mencionadas exigen un examen detallado.

La Comisión estudiará **la manera de garantizar una aplicación coherente de las normas de protección de datos, habida cuenta de las repercusiones de las nuevas tecnologías en los derechos y libertades de las personas, y habida cuenta del objetivo consistente en garantizar la libre circulación de datos personales en el mercado interior**.

2.1.2. Aumentar la transparencia para los interesados

La transparencia es una condición fundamental indispensable para permitir a las personas efectuar un control sobre sus propios datos y para garantizar la protección efectiva de los datos personales. Es pues primordial que los responsables del tratamiento **informen** a los ciudadanos **correcta y claramente, con toda transparencia**, para que sepan quién recogerá y tratará sus datos, de qué manera, por qué motivos y durante cuánto tiempo, y cuáles son sus derechos a efectos de acceder, rectificar o suprimir sus datos. Las disposiciones aplicables relativas a la información que debe comunicarse al interesado[15] son insuficientes.

La transparencia se basa en elementos fundamentales, como **un acceso fácil a la información, que debe ser fácil de entender, y la utilización de un lenguaje claro y sencillo**. Eso es particularmente importante en un medio en línea donde, muy a menudo, las declaraciones de confidencialidad carecen de claridad, son difícilmente accesibles, poco transparentes[16], y no se ajustan siempre plenamente a las normas vigentes. Un ejemplo podría

---

12 Véase el considerando 26 de la Directiva 95/46/CE.

13 Véase, por ejemplo, el caso de las direcciones IP, examinado en el Dictamen 4/2007 del Grupo de Trabajo del Artículo 29 sobre el concepto de datos personales (documento WP 136).

14 Véase, por ejemplo, la sentencia del Tribunal constitucional federal alemán (*Bundesverfassungsgericht*) de 27 de febrero de 2008, 1 BvR 370/07.

15 Véanse los artículos 10 y 11 de la Directiva 95/46/CE.

16 Un sondeo de Eurobarómetro realizado en 2009 reveló que cerca de la mitad de las personas encuestadas consideraban que las declaraciones de confidencialidad que figuran en los sitios web eran poco claras o muy poco claras (véase el Flash Eurobarómetro n° 282: http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

ser la publicidad en línea basada en el comportamiento, en la que la multiplicidad de participantes y la complejidad tecnológica son tales que los individuos difícilmente pueden determinar si se recogen datos personales, por quién y con qué fin.

En este contexto, los **niños** merecen una protección particular, ya que pueden ser menos conscientes de los riesgos, consecuencias y derechos vinculados al tratamiento de datos personales[17].

La Comisión estudiará las siguientes acciones:

- introducir, en el marco jurídico, un **principio general que imponga el tratamiento transparente** de los datos personales;

- introducir **obligaciones específicas** para los responsables del tratamiento relativas al tipo de información que debe comunicarse y a las **modalidades** de su comunicación, incluso por lo que se refiere a los **niños**;

- elaborar uno o más **modelos normalizados europeos** («**declaraciones de confidencialidad»**) que deberán utilizar los responsables del tratamiento.

También es importante que los ciudadanos sean informados cuando los datos que les conciernan sean objeto de destrucción, accidental o ilícita, pérdida, alteración, o acceso por personas no autorizadas o revelación a tales personas. La reciente revisión de la Directiva sobre la privacidad y las comunicaciones electrónicas instauró una **notificación obligatoria de las violaciones de datos,** que no obstante, sólo es aplicable en el sector de las telecomunicaciones. Dado que el riesgo de las violaciones de datos existe también en otros sectores (por ejemplo, el sector financiero), la Comisión examinará las modalidades de ampliar a otros sectores la obligación de notificar las violaciones de datos personales, de acuerdo con la declaración que presentó al Parlamento Europeo en 2009 en el contexto de la reforma del marco normativo para las comunicaciones electrónicas[18]. Este examen no afectará a las disposiciones de la Directiva sobre la privacidad y las comunicaciones electrónicas, que debe transponerse en el Derecho nacional a más tardar el 25 de mayo de 2011[19]. Deberá garantizarse la adopción de un enfoque sistemático y coherente a este respecto.

---

17 Véase el estudio cualitativo sobre Mayor seguridad para los niños en Internet, por lo que se refiere a los niños de 9 y 10 años y de 12 a 14 años, que reveló que los niños tienden a subestimar los riesgos vinculados a la utilización de Internet y a minimizar las consecuencias de sus comportamientos de riesgo (disponible en la siguiente dirección: http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

18 «La Comisión toma nota de la voluntad del Parlamento Europeo de que la obligación de notificar las violaciones relativas a datos personales no se limiten al sector de las comunicaciones electrónicas, sino que se aplique también a entidades como los proveedores de servicios de la Sociedad de la Información […]. Por ello, la Comisión iniciará en breve los trabajos preparatorios necesarios, incluida la consulta de las partes interesadas, con miras a presentar, en su caso, propuestas en este ámbito a más tardar en 2011 […]», que se puede consultar en la siguiente dirección: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//EN. Véase también el considerando 59 de la Directiva 2009/136/CE que modifica la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas: «Este interés de los usuarios por ser informados no se limita, obviamente, al sector de las comunicaciones electrónicas, por lo que deben introducirse, a escala comunitaria y con carácter prioritario, requisitos de notificación explícitos y obligatorios en todos los sectores.»

19 Véase el artículo 4 de la Directiva 2009/136/CE.

La Comisión:

- examinará las modalidades de la introducción, en el marco jurídico global, de una obligación **de notificación general de las violaciones de datos personales**, indicando los destinatarios de este tipo de notificaciones y los criterios a que se supeditaría la obligación de notificar.

2.1.3. Reforzar el control sobre los propios datos

Para garantizar que los ciudadanos gocen de un elevado nivel de protección de datos, deben cumplirse dos condiciones previas: **el tratamiento de los datos por los responsables del tratamiento debe limitarse únicamente a su propósito (principio de minimización de los datos)** y los interesados deben conservar un **control efectivo sobre sus propios datos**. Según el artículo 8, apartado 2, de la Carta, «Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación». Los individuos deberían siempre poder acceder a sus datos, rectificarlos, suprimirlos o bloquearlos, salvo que existan motivos legítimos previstos por la ley. Estos derechos ya están consagrados en el marco jurídico actual. No obstante, las condiciones de su ejercicio no están armonizadas, y por tanto este ejercicio es más fácil en unos Estados miembros que en otros. Esta cuestión es especialmente difícil en el medio en línea, donde los datos a menudo se conservan sin que se haya informado previamente al interesado o sin que éste haya dado su consentimiento.

El ejemplo de las redes sociales es especialmente esclarecedor a este respecto, ya que presenta grandes dificultades para que los individuos puedan ejercer un control efectivo sobre los datos que les conciernen. La Comisión ha recibido varias denuncias de personas que no siempre han podido recuperar datos personales de los prestadores de servicios en línea, como fotos, y a quienes se ha impedido por tanto ejercer su derecho de acceso, rectificación y supresión.

Por tanto, estos derechos deben hacerse más explícitos, claros y, eventualmente, reforzarse.

Por tanto, la Comisión estudiará los medios que permitan:

- reforzar el **principio de la minimización de datos**;

- **mejorar las condiciones** de un verdadero **ejercicio de los derechos de acceso, rectificación, supresión y bloqueo** (por ejemplo, fijando plazos de respuesta a las solicitudes de las personas en cuestión, autorizando el ejercicio de estos derechos por vía electrónica o instaurando la gratuidad como principio del ejercicio del derecho de acceso);

- clarificar el llamado «**derecho a ser olvidado**», es decir, el derecho de las personas a que sus datos no se traten y se supriman cuando dejan de ser necesarios con fines legítimos. Se trata, por ejemplo, del caso en que la persona retira su consentimiento al tratamiento de datos, o del caso en que haya expirado el plazo de conservación de los datos;

- completar el abanico de los derechos de los interesados garantizando la «**portabilidad de los datos**», es decir, confiriendo a los individuos el derecho explícito a retirar sus datos (por ejemplo, fotografías o listas de amigos) de una aplicación o de un servicio, de modo que los datos retirados puedan transferirse a otra aplicación u otro servicio, siempre que ello sea técnicamente posible, sin que los responsables del tratamiento lo obstaculicen.

2.1.4. Sensibilización

Si la transparencia es esencial, es también indispensable sensibilizar más a la opinión pública, en particular a los jóvenes, respecto de los riesgos vinculados al tratamiento de los datos personales y respecto de sus derechos. Un sondeo de Eurobarómetro realizado en 2008 puso

de manifiesto que la gran mayoría de los habitantes de los Estados miembros de la UE consideran más bien escaso el nivel de sensibilización de sus conciudadanos respecto de la protección de los datos personales[20]. Por tanto, una serie de agentes (las autoridades nacionales, en particular las responsables de la protección de datos y los organismos de formación, así como los responsables del tratamiento y las asociaciones de la sociedad civil) deberían fomentar y promover las acciones de sensibilización. Estas acciones deberían consistir entre otras cosas en medidas no legislativas tales como campañas de sensibilización en la prensa escrita y los medios de comunicación electrónicos, y la publicación de información clara en sitios web, que describan con concreción los derechos de los interesados y las responsabilidades de los responsables del tratamiento.

La Comisión estudiará:

- la posibilidad de **cofinanciar acciones de sensibilización respecto de la protección de datos** con ayuda del presupuesto de la Unión;

- la necesidad y la oportunidad de incluir en el marco jurídico **una obligación de realizar acciones de sensibilización** en este ámbito.

2.1.5. Garantizar un consentimiento informado y libre

Cuando se exige un consentimiento informado, las normas vigentes prevén que el consentimiento de la persona sobre el tratamiento de sus datos personales debería ser una «manifestación de voluntad, libre, específica e informada» por la que acepta este tratamiento[21]. Ahora bien, actualmente, estas condiciones son objeto de distintas interpretaciones en los Estados miembros, desde de la obligación general de obtener un consentimiento escrito hasta la aceptación de un consentimiento implícito.

Además, en el medio en línea - vista la opacidad de las políticas de confidencialidad - las personas tienen a menudo más dificultades para informarse de sus derechos y dar un consentimiento informado. Esto es tanto más complejo debido a que, en algunos casos, no está claro lo que constituye un consentimiento libre, específico e informado respecto del tratamiento de datos, como en el ámbito de la publicidad en línea basada en el comportamiento, donde se considera a veces, pero no siempre, que los parámetros del navegador del internauta expresan su consentimiento.

Conviene pues clarificar las condiciones del consentimiento del interesado, con el fin de garantizar que se concede siempre con conocimiento de causa, y de garantizar que el interesado es plenamente consciente de que da su autorización y respecto a qué tratamiento, de conformidad con lo dispuesto en el artículo 8 de la Carta de los Derechos Fundamentales de la UE. La claridad de los conceptos clave puede también favorecer las iniciativas de autorregulación destinadas a desarrollar soluciones prácticas conformes al Derecho de la Unión.

La Comisión estudiará los medios de **clarificar y reforzar las normas en materia de consentimiento**.

---

[20] Véase el Flash Eurobarómetro n° 225 – Protección de datos en la Unión Europea http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

[21] Véase el artículo 2, letra h), de la Directiva 95/46/CE.

2.1.6. Proteger los datos sensibles

El tratamiento de los datos sensibles, es decir, los datos que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad, está prohibido por regla general, con excepciones limitadas bajo algunas condiciones y garantías[22]. Sin embargo, habida cuenta de las evoluciones tecnológicas y en el ámbito social, es necesario revisar las disposiciones existentes relativas a los datos sensibles, con el fin de determinar si convendría someter otras categorías de datos a esta normativa y precisar aún más las condiciones aplicables a su tratamiento. Esto afecta, por ejemplo, a los datos genéticos, que actualmente no se mencionan expresamente como una categoría de datos sensibles.

La Comisión estudiará las siguientes acciones:

- determinar si otras categorías de datos deberían considerarse «**sensibles»**, por ejemplo, los datos **genéticos**;

- precisar aún más y **armonizar las condiciones** que deben cumplirse para realizar el tratamiento de determinadas categorías de datos sensibles.

2.1.7. Reforzar la eficacia de las vías de recurso y las sanciones

Para garantizar la aplicación de las normas de protección de datos, es esencial disponer de una **normativa eficaz en materia de vías de recurso y sanciones**. Numerosos son los casos en que una violación de estas normas en detrimento de una persona afecta también a un gran número de otras personas que se encuentran en una situación similar.

Por tanto, la Comisión iniciará las siguientes acciones:

- estudiar la posibilidad de **ampliar el poder de recurrir a los órganos jurisdiccionales nacionales** a las autoridades encargadas de la protección de datos y a las asociaciones de la sociedad civil, así como a **otras asociaciones que representen los intereses de las personas interesadas**;

- evaluar la necesidad de **endurecer las disposiciones vigentes en materia de sanciones**, por ejemplo previendo expresamente sanciones penales para las violaciones de las normas de protección de datos, con el fin de reforzar su eficacia.

2.2. Profundizar en la dimensión de mercado interior

2.2.1. Aumentar la seguridad jurídica y garantizar condiciones iguales a los responsables del tratamiento

La protección de datos en la UE tiene **una sólida dimensión de mercado interior**, es decir, la necesidad de garantizar la libre circulación de datos personales entre los Estados miembros en el mercado interior. Por consiguiente, la armonización realizada por la Directiva de las legislaciones nacionales relativas a la protección de datos no se limita a una armonización mínima, sino que efectúa una armonización generalmente completa[23].

---

22 Véase el artículo 8 de la Directiva 95/46/CE.

23 Sentencia del Tribunal de Justicia en el asunto C-101/01, Bodil Lindqvist, Rec. 2003, p. I-1297, apartados 96 y 97.

Al mismo tiempo, la Directiva otorga a los Estados miembros un margen de maniobra en algunos ámbitos y les autoriza a mantener o introducir regímenes especiales para situaciones específicas[24]. Estos elementos, junto con el hecho de que los Estados miembros aplican a veces incorrectamente la Directiva, son la causa de **divergencias entre las legislaciones nacionales que transponen la Directiva, que contradicen uno de sus objetivos principales, a saber, garantizar la libre circulación de datos en el mercado interior**. Esto sucede en numerosos sectores y contextos, por ejemplo, en el tratamiento de datos personales en el contexto profesional o con fines de salud pública. La falta de armonización es uno de los principales problemas recurrentes puestos de relieve por las partes involucradas, en particular los agentes económicos, ya que implica costes suplementarios y una sobrecarga administrativa. Es el caso, en particular, de los responsables del tratamiento establecidos en varios Estados miembros y que deben cumplir requisitos y prácticas distintos en cada uno de ellos. Además, las aplicaciones divergentes de la Directiva por los Estados miembros crean una inseguridad jurídica no sólo para los responsables del tratamiento, sino también para los interesados, creando el riesgo de distorsionar el objetivo de un nivel equivalente de protección que se supone que la Directiva debe alcanzar y garantizar.

La Comisión estudiará los medios de alcanzar una **mayor armonización de las normas de protección de datos en la UE**.

2.2.2. Reducir la carga administrativa

La igualdad de condiciones reducirá la necesidad de ajustarse a exigencias nacionales divergentes, lo que reducirá considerablemente la carga administrativa soportada por los responsables del tratamiento. Otra manera concreta de reducir para éstos la carga administrativa y los costes sería **revisar y simplificar el actual sistema de notificación**[25]. La mayoría de los responsables del tratamiento están de acuerdo en que la obligación general de notificar todas las operaciones de tratamiento a las autoridades encargadas de la protección de datos es bastante pesada y no aporta, en sí, un verdadero valor añadido desde el punto de vista de la protección de los datos personales. Por otra parte, se trata de un ámbito en el que la Directiva deja un margen de maniobra a los Estados miembros, que son libres para decidir posibles exenciones y simplificaciones, así como los procedimientos que deben seguirse.

La armonización y la simplificación del sistema permitirían reducir los costes y la carga administrativa, en particular para las empresas multinacionales establecidas en varios Estados miembros.

La Comisión estudiará los distintos medios para **simplificar y armonizar el actual sistema de notificación**, incluida la posible elaboración de un **formulario de registro uniforme válido en toda la Unión.**

2.2.3. Clarificar las normas relativas a la legislación aplicable y al Estado miembro responsable

El primer informe de la Comisión sobre la aplicación de la Directiva sobre protección de datos destacaba, ya en 2003[26], que la aplicación de la disposición relativa al Derecho

[24] *Ibidem*, apartado 97. Véase también el considerando 9 de la Directiva 95/46/CE.

[25] Véase el artículo 18 de la Directiva 95/46/CE.

[26] Informe de la Comisión - Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE) - COM(2003) 265.

aplicable[27] era «deficiente en varios casos, lo que puede provocar que surja el tipo de conflicto jurídico que este artículo pretende evitar». La situación no ha mejorado desde entonces, a resultas de lo cual los responsables del tratamiento y las autoridades de control de la protección de datos no saben siempre claramente cuál es el Estado miembro responsable y cuál es la legislación aplicable cuando hay varios Estados miembros implicados. Tal es el caso, en particular, cuando el responsable del tratamiento está sujeto a diferentes requisitos en distintos Estados miembros, cuando una empresa multinacional está establecida en varios Estados miembros, o cuando el responsable del tratamiento no está establecido en la Unión, pero presta sus servicios a residentes de la UE.

La complejidad también crece debido a la globalización y a los progresos tecnológicos: los responsables del tratamiento ejercen su actividad cada vez más en varios Estados miembros y jurisdicciones, prestando servicios y asistencia las 24 horas. Internet permite a los responsables del tratamiento establecidos fuera del Espacio Económico Europeo (EEE)[28] prestar más fácilmente servicios a distancia y tratar en línea los datos personales. Por ello, a menudo resulta difícil determinar la ubicación de estos datos y el equipo utilizado (por ejemplo, en las aplicaciones y servicios de la «computación en nube»).

Sin embargo, la Comisión considera que, aunque el tratamiento de los datos personales se confíe a un responsable establecido en un tercer país, los interesados deben poder beneficiarse de la protección a que tienen derecho en virtud de la Carta de los Derechos Fundamentales de la Unión Europea y de la legislación de la UE en materia de protección de datos.

La Comisión examinará la manera en que pueden **revisarse y clarificarse las disposiciones existentes sobre el Derecho aplicable**, y en particular los criterios actuales de determinación del Derecho aplicable, con el fin de mejorar la seguridad jurídica, clarificar cuál es el Estado miembro responsable de la aplicación de las normas de protección de datos y, en definitiva, garantizar el mismo nivel de protección a todos los interesados de la UE, independientemente del lugar de establecimiento del responsable del tratamiento.

2.2.4. Reforzar la responsabilidad de los responsables del tratamiento

La simplificación administrativa **no debería traducirse en una reducción general del nivel de responsabilidad de los responsables del tratamiento respecto a la protección de datos**. La Comisión considera, por el contrario, que sus obligaciones deberían definirse más claramente en el marco jurídico, en particular, por lo que se refiere a los mecanismos de control interno y la cooperación con las autoridades de control de la protección de datos. Además, convendría velar por que este nivel de responsabilidad se aplique también a los responsables del tratamiento que están sujetos al secreto profesional (por ejemplo, los abogados) y en los casos cada vez más corrientes en los que el responsable confía el tratamiento a otra entidad (por ejemplo, encargados del tratamiento).

La Comisión estudiará pues los medios de **garantizar que los responsables del tratamiento establezcan políticas y mecanismos eficaces para garantizar el respeto de las normas en materia de protección de datos**. De esta manera, tendrá en cuenta el debate actual sobre la posible introducción de un principio de «rendición de cuentas» (*accountability)*[29]. No se

---

27 Véase el artículo 4 de la Directiva 95/46/CE.

28 El Espacio Económico Europeo incluye Noruega, Liechtenstein e Islandia.

29 Véase, en particular, el dictamen n° 3/2010 del Grupo de Trabajo del Artículo 29, adoptado el 13 de julio de 2010.

trataría de aumentar la carga administrativa que pesa sobre los responsables del tratamiento, puesto que estas medidas tendrían más bien por objeto establecer garantías y mecanismos de protección más eficaces, reduciendo y simplificando al mismo tiempo algunos trámites administrativos, como las notificaciones (*véase el apartado 2.2.2*).

La promoción de la utilización de las tecnologías de protección del derecho a la intimidad (PET), como ya se destacó en la Comunicación de la Comisión de 2007 a este respecto, así como del principio de privacidad desde el diseño (*Privacy by Design*), podría desempeñar un papel importante a este respecto, incluso para garantizar la seguridad de los datos[30].

La Comisión examinará las medidas siguientes destinadas a reforzar la responsabilidad de los responsables del tratamiento:

– hacer obligatoria la designación de un **responsable de la protección de datos** independiente, y armonizar las normas relativas a sus tareas y competencias[31], evitando al mismo tiempo imponer cargas administrativas indebidas, en particular a las pequeñas empresas y las microempresas;

– introducir en el marco jurídico la obligación, para los responsables del tratamiento, de realizar un **análisis de impacto respecto a la protección de datos** en casos específicos, por ejemplo, cuando se tratan datos sensibles o cuando el tipo de tratamiento implica riesgos específicos, en particular en caso de utilización de tecnologías, mecanismos o procedimientos específicos, como la elaboración de perfiles o la videovigilancia;

– proseguir la promoción de la utilización de las PET y de las posibilidades de aplicación concreta del concepto de «privacidad desde el diseño».

2.2.5. Fomentar las iniciativas en materia de autorregulación y examinar la posibilidad de instaurar regímenes europeos de certificación

La Comisión sigue opinando que las **iniciativas en materia de autorregulación** adoptadas por los responsables del tratamiento pueden **contribuir a una mejor aplicación de las normas relativas a la protección de datos**. Las disposiciones actuales de la Directiva sobre protección de datos relativas a la autorregulación, es decir, la posibilidad de elaborar códigos de conducta[32], apenas se han utilizado hasta ahora y las partes involucradas del sector privado no las consideran satisfactorias.

Además, la Comisión examinará la posibilidad de crear **regímenes europeos de certificación (por ejemplo, «distintivos de protección de la intimidad»)** para los procesos, tecnologías,

---

30 Por lo que respecta a las PET, véase lo siguiente: Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET) - COM(2007) 228. El principio de «privacidad a través del diseño» significa que la protección de la intimidad y los datos personales se tiene en cuenta a lo largo de todo el ciclo de vida de las tecnologías, desde su concepción hasta su despliegue, utilización y eliminación final. Este principio figura, en particular, en la Comunicación de la Comisión «Una Agenda Digital para Europa» COM(2010) 245.

31 La posibilidad actual del responsable del tratamiento de designar a un responsable de la protección de datos para velar, de forma independiente, por el respeto de las normas nacionales y de la UE en materia de protección de datos y para ayudar a las personas interesadas, ya se ha utilizado en varios Estados miembros (véase, por ejemplo, el *Beauftragter für den Datenschutz* en Alemania y el *correspondant informatique et libertés (CIL)* en Francia).

32 Véase el artículo 27 de la Directiva 95/46/CE.

productos y servicios que sean conformes a las normas de protección de la intimidad[33]. Esta medida no sólo proporcionaría una orientación a las personas que utilizan estas tecnologías, productos o servicios, sino que sería importante en cuanto a la responsabilidad del responsable del tratamiento, pues ayudaría a probar que ha cumplido efectivamente sus obligaciones (*véase el apartado 2.2.4*). Por supuesto, habría que **garantizar la fiabilidad de tales distintivos de protección de la intimidad**, así como su compatibilidad con las obligaciones legales y las normas técnicas internacionales.

La Comisión:

- examinará los medios de **fomentar más las iniciativas en materia de autorregulación**, en particular, la promoción activa de los códigos de conducta;

- estudiará la viabilidad de la instaurar **regímenes europeos de certificación** en el ámbito de la protección de la intimidad y los datos.

2.3. Revisar las normas de protección de datos en los ámbitos de la cooperación policial y judicial en materia penal

La Directiva sobre protección de datos se aplica a todas las actividades de tratamiento de datos personales en los Estados miembros, tanto en el sector público como en el privado. Sin embargo, no se aplica al «tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario», como las actividades en los ámbitos de la cooperación policial y judicial en materia penal[34]. No obstante, el Tratado de Lisboa ha suprimido la antigua «estructura en pilares» de la UE y ha introducido una nueva base jurídica amplia para la protección de los datos personales en todas las políticas de la Unión[35]. En este contexto, y a la vista de la Carta de los Derechos Fundamentales de la UE, las Comunicaciones de la Comisión sobre el Programa de Estocolmo y el Plan de acción por el que se aplica el programa de Estocolmo[36] subrayaron la necesidad de contar con un «sistema general de protección» y de «reforzar la posición de la UE en cuanto a la protección de los datos personales en el contexto de todas las políticas de la UE, incluida la represión policial y la prevención de la delincuencia».

El instrumento de la UE aplicable en materia de protección de los datos personales en los ámbitos de la cooperación policial y judicial en materia penal es la **Decisión Marco 2008/977/JAI**[37]. Esta última constituye un importante avance en un ámbito donde la necesidad de normas comunes para la protección de datos era acuciante. No obstante, es preciso seguir trabajando a este respecto.

La Decisión Marco sólo se aplica al intercambio transfronterizo de datos personales en la UE y no a las operaciones de tratamiento nacionales efectuadas en los Estados miembros.

---

33 A este respecto, véase también la Comunicación sobre las PET citada en la nota a pie de página n° 30.

34 Véase el artículo 3, apartado 2, primer guión, de la Directiva 95/46/CE.

35 Véase el artículo 16 del TFUE.

36 Véase COM(2009) 262, de 10.6.2009, y COM(2010) 171, de 20.4.2010.

37 Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (DO L 350, de 30.12.2008, p. 60). La Decisión marco sólo prevé una armonización mínima de las normas de protección de datos.

Esta distinción es difícil de establecer en la práctica y puede complicar la aplicación efectiva de la Decisión Marco[38].

Asimismo, **la Decisión Marco contiene una excepción demasiado amplia al principio de limitación de la finalidad**. Otra de sus deficiencias es la ausencia de disposiciones que prevean una diferenciación de las distintas categorías de datos en función de su grado de exactitud o fiabilidad, y en particular una diferenciación de los datos basados en hechos de los basados en opiniones o valoraciones personales[39], así como una diferenciación de las distintas categorías de interesados (delincuentes, sospechosos, víctimas, testigos, etc.), combinada con garantías específicas para los datos relativos a personas no sospechosas[40].

Además, **la Decisión Marco no sustituye a los diversos instrumentos legislativos de carácter sectorial adoptados a escala de la UE en el ámbito de la cooperación policial y judicial en materia penal**[41], en particular, los que regulan el funcionamiento de Europol, Eurojust, el Sistema de Información de Schengen (SIS) y el Sistema de Información Aduanero (SIA)[42], que prevén regímenes especiales de protección de datos o que suelen remitirse a los instrumentos de protección de datos del Consejo de Europa. Por lo que se refiere a las actividades en el marco de la cooperación policial y judicial, todos los Estados miembros suscribieron la Recomendación del Consejo de Europa n° R (87) 15, que establece los principios del Convenio n° 108 para el sector policial. No obstante, esta Recomendación no constituye un instrumento jurídicamente vinculante.

Esta situación puede afectar directamente a las posibilidades de las personas de ejercer sus derechos en materia de protección de datos en estos ámbitos (por ejemplo, el derecho a saber qué datos personales se tratan y se intercambian, por quién y con qué fines, y el de conocer las condiciones de ejercicio de estos derechos, tal como el derecho de acceso a los datos que les conciernen).

El objetivo consistente en establecer un sistema global y coherente en la UE y respecto a los terceros países implica pues **la necesidad de considerar la posibilidad de una revisión de las normas actuales de protección de datos en los ámbitos de la cooperación policial y judicial en materia penal.** La Comisión destaca que el concepto de un régimen global de protección de datos no excluye la adopción de normas específicas para los sectores policial y judicial dentro del marco general, habida cuenta de la naturaleza específica de estos ámbitos, como indica la Declaración 21 adjunta al Tratado de Lisboa. Esto implica, por ejemplo, la necesidad de examinar en qué medida el ejercicio por una persona de determinados derechos en materia de protección de datos puede, en un caso específico, comprometer la prevención, la

---

38 Esta distinción no existe en los instrumentos pertinentes del Consejo de Europa como el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (CETS n° 108), su Protocolo adicional relativo a las autoridades de control y a la transferencia de datos (ETS nº 181), y la Recomendación nº R (87) 15 del Comité de Ministros por la que se regula el uso de datos personales en el ámbito policial, adoptada por el Consejo de Europa el 17 de septiembre de 1987.

39 Tal como lo exige el Principio 3.2 de la Recomendación n° R (87) 15.

40 Contrariamente al Principio 2 de la Recomendación n° R (87) 15 y a sus informes de evaluación.

41 Véase la presentación general de estos instrumentos en la Comunicación de la Comisión «Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia» - COM(2010) 385.

42 Los instrumentos correspondientes establecieron unas autoridades de control comunes con el fin de garantizar el control de la protección de datos, además de los poderes de control generales conferidos por el Reglamento (CE) n° 45/2001 al Supervisor Europeo de Protección de Datos (SEPD) sobre las instituciones, órganos, oficinas y agencias de la Unión.

investigación, la detección o la persecución de infracciones penales, o la aplicación de sanciones penales.

La Comisión, en particular:

- examinará la oportunidad de **ampliar la aplicación de las normas generales de protección de datos a los ámbitos de la cooperación policial y judicial en materia penal**, incluso para el tratamiento a nivel nacional, previendo al mismo tiempo si es preciso **limitaciones** armonizadas a algunos derechos de las personas en materia de protección de datos, por ejemplo por lo que se refiere al derecho de acceso o al principio de transparencia;

- examinará la necesidad de introducir **disposiciones específicas y armonizadas** en el nuevo marco general que regula la protección de datos, por ejemplo por lo que se refiere al tratamiento de los **datos genéticos** a efectos del Derecho penal o la distinción que debe establecerse entre las distintas categorías de interesados (testigos, sospechosos, etc.) en los ámbitos de la cooperación policial y la cooperación judicial en materia penal;

- iniciará, en 2011, una **consulta** de todas las partes interesadas sobre la mejor manera de **revisar los sistemas de control actuales en los ámbitos de la cooperación policial y la cooperación judicial en materia penal**, con el fin de garantizar el ejercicio de un control eficaz y coherente de la protección de datos en el conjunto las instituciones, órganos, oficinas y agencias de la Unión;

- evaluará la necesidad de **alinear**, a largo plazo, las **distintas normas sectoriales, adoptadas en la UE para la cooperación policial y judicial en materia penal y contenidas en instrumentos específicos,** con el nuevo marco jurídico general de la protección de datos.

2.4. La dimensión mundial de la protección de datos

2.4.1. Clarificar y simplificar las normas aplicables a las transferencias internacionales de datos

La transferencia de datos personales fuera de la UE y del espacio EEE está supeditada, en particular, a la **«comprobación de la existencia de un nivel de protección adecuado».** En la actualidad, la adecuación de un país tercero, es decir, la comprobación de que un país tercero garantiza un nivel de protección considerado adecuado por la UE, puede ser determinada por la Comisión y por los Estados miembros.

Cuando la Comisión considera adecuado el nivel de protección garantizado por un tercer país, los datos personales pueden circular libremente desde los veintisiete Estados miembros de la UE y los tres países miembros del EEE hacia ese tercer país, sin que sea necesaria ninguna otra garantía. Sin embargo, las condiciones exactas que deben cumplirse para que la Comisión reconozca el carácter adecuado del nivel de protección no están actualmente definidas de una manera suficientemente precisa en la Directiva sobre protección de datos. Además, la Decisión Marco no prevé la adopción de este tipo de decisión por la Comisión.

En algunos Estados miembros, el carácter adecuado del nivel de protección es evaluado en primer lugar por el responsable del tratamiento, que transfiere datos personales a un tercer país, a veces en el marco del control *a posteriori* efectuado por la autoridad de control en materia de protección de datos. Esta situación puede dar lugar a enfoques diferentes de la apreciación del nivel de protección garantizado por los terceros países u organizaciones internacionales y, por consiguiente, **implica el riesgo de que el nivel de protección de los interesados previsto en un tercer país se juzgue diferentemente de un Estado miembro a**

otro. Asimismo, los instrumentos jurídicos existentes no establecen condiciones precisas y armonizadas en cuanto a las transferencias que pueden considerarse legítimas. Por ello, las prácticas varían de un Estado miembro a otro.

Además, por lo que se refiere a las transferencias hacia terceros países que no garantizan un nivel de protección adecuado, las cláusulas modelo actuales de la Comisión para la transferencia de datos personales a los responsables del tratamiento[43] y a los encargados del tratamiento[44] no están concebidas para situaciones extracontractuales y no pueden, por ejemplo, aplicarse a transferencias entre Administraciones públicas.

Además, los acuerdos internacionales celebrados por la UE o sus Estados miembros exigen a menudo la inserción de cláusulas específicas o principios relativos a la protección de datos. Esto puede dar lugar a textos distintos con disposiciones y derechos incoherentes y, por consiguiente, que se presten a interpretaciones divergentes, en detrimento del interesado. Por consiguiente, la Comisión anunció que trabajaría en los elementos esenciales relativos a la protección de los datos personales en los acuerdos celebrados entre la Unión y terceros países a efectos de la aplicación de la ley[45].

Otros medios que se han desarrollado en forma de autorregulación, como los códigos de conducta internos de algunas empresas (normas vinculantes para las empresas)[46], pueden también constituir una herramienta útil para las transferencias legítimas de datos personales entre las empresas de un mismo grupo. No obstante, las partes involucradas han sugerido que este mecanismo puede mejorarse y facilitarse su aplicación.

Habida cuenta de los problemas puestos de relieve, **es preciso mejorar, en general, los mecanismos existentes de transferencia internacional de datos personales**, garantizando al mismo tiempo un nivel adecuado de protección de estos datos en caso de transferencia o tratamiento fuera de la UE o el EEE.

---

43 Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE (DO L 181 de 4.7.2001, p. 19); Decisión 2002/16/CE de la Comisión, de 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE (DO L 6 de 10.1.2002, p. 52); Decisión 2004/915/CE de la Comisión, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países (DO L 385 de 29.12.2004, p. 74).

44 Decisión 2010/87/CE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo (DO L 39 de 12.2.2010, p. 5).

45 Plan de acción por el que se aplica el programa de Estocolmo (véase la nota a pie de página n° 36).

46 Por «normas vinculantes para las empresas» se entienden los códigos de buenas prácticas basados en las normas europeas de protección de datos, que las multinacionales elaboran y siguen voluntariamente para garantizar un nivel adecuado de protección de los datos personales transferidos entre empresas que forman parte de un mismo grupo y que están vinculadas por las mismas normas internas. Véase: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

La Comisión se propone examinar los medios para:

- **mejorar y racionalizar los procedimientos actuales** de transferencia internacional de datos, incluidos los instrumentos jurídicamente vinculantes y las «normas vinculantes para las empresas», con el fin de lograr un **enfoque de la UE más uniforme y más coherente** respecto a los terceros países y las organizaciones internacionales;

- **clarificar su procedimiento de evaluación del carácter adecuado del nivel de protección** garantizado en un tercer país o una organización internacional y precisar los **criterios y condiciones** aplicables;

- definir los **elementos esenciales en materia de protección de datos** que deberían utilizarse en todos los tipos de acuerdos internacionales celebrados por la **UE**.

2.4.2. Promover principios universales

El tratamiento de datos es un proceso a escala mundial y requiere la elaboración de normas universales para la protección de las personas por lo que respecta al tratamiento de los datos personales.

El marco jurídico de la UE sobre esta cuestión ha servido a menudo de **referencia a los terceros países para regular la protección de datos**. Su incidencia y sus efectos, tanto dentro como fuera de la Unión, han revestido la mayor importancia. La **Unión Europea debe pues seguir desempeñando un papel motriz en la elaboración y la promoción de las normas jurídicas y técnicas internacionales en el ámbito de la protección de los datos personales,** sobre la base de los instrumentos pertinentes de la UE y los otros instrumentos europeos relativos a la protección de datos. Eso es especialmente importante en el marco de la política de ampliación de la UE.

Por lo que se refiere a las normas técnicas internacionales elaboradas por los organismos de normalización, la Comisión considera que una coherencia entre el futuro marco jurídico y estas normas será esencial para garantizar una aplicación sistemática y práctica de las normas de protección de datos por los responsables del tratamiento.

La Comisión tiene intención de:

- seguir **promoviendo la elaboración de normas jurídicas y técnicas de alto nivel en materia de protección de datos** en los terceros países y a nivel internacional;

- esforzarse en defender el **principio de reciprocidad de la protección** en las acciones internacionales de la Unión y, en particular, por lo que se refiere a las personas cuyos datos se exportan de la UE hacia terceros países;

- **reforzar su cooperación, a tal efecto, con los terceros países y las organizaciones internacionales**, como la OCDE, el Consejo de Europa, las Naciones Unidas, y otras organizaciones regionales;

- **seguir de cerca la elaboración de las normas técnicas internacionales por los organismos de normalización** como el CEN y la ISO, con el fin de garantizar que completan adecuadamente las normas jurídicas y respetan efectivamente a nivel operativo las exigencias esenciales en materia de protección de datos.

2.5. Reforzar el marco institucional para una mejor aplicación de las normas de protección de datos

La aplicación y el control de la aplicación de los principios y normas en materia de protección de datos son indispensables para garantizar el respeto de los derechos de los interesados.

En este contexto, **el papel de las autoridades encargadas de la protección de datos es esencial** para el control de la aplicación de las normas de protección de datos. Estas autoridades son guardianas independientes de los derechos y libertades fundamentales de las personas respecto al tratamiento de los datos personales. Por esta razón, la Comisión considera que su papel debería reforzarse, en particular vista la reciente jurisprudencia del Tribunal de Justicia de la Unión Europea acerca de su independencia[47], y que deberían dotarse de los poderes y recursos necesarios para realizar correctamente sus tareas tanto a nivel nacional como cuando cooperan entre sí.

Al mismo tiempo, la Comisión considera que las **autoridades de protección de datos deberían reforzar su cooperación y coordinar mejor sus actividades**, en particular cuando encuentran problemas que revisten, por su naturaleza, una dimensión transfronteriza. Este es especialmente el caso cuando algunas empresas multinacionales están establecidas en varios Estados miembros y ejercen sus actividades en cada uno de estos Estados, o cuando se requiere un control coordinado con el Supervisor Europeo de Protección de Datos (SEPD)[48].

A este respecto, **el Grupo de Trabajo del Artículo 29 puede desempeñar un papel importante**[49], ya que tiene por tarea, además de su función consultiva[50], contribuir a la aplicación uniforme de las normas de protección de datos de la UE a nivel nacional. Sin embargo, la aplicación y la interpretación divergentes de las normas de la UE por las autoridades de protección de datos, incluso aunque los retos en este ámbito sean los mismos en toda la Unión, exigen un refuerzo del papel de este Grupo de Trabajo en la coordinación de las posiciones de las autoridades de protección de datos, con el fin de garantizar una aplicación más uniforme a nivel nacional y, por consiguiente, un nivel equivalente de protección de datos.

---

47 Sentencia del Tribunal de Justicia, de 9 de marzo de 2010, en el asunto C-518/07, Comisión contra Alemania.

48 Este es actualmente el caso de los grandes sistemas informáticos, por ejemplo el SIS II (véase el artículo 46 del Reglamento (CE) n° 1987/2006 - DO L 318 de 28.12.2006, p. 4) y el VIS (véase artículo 43 del Reglamento (CE) n° 767/2008 - DO L 218 de 13.8.2008, p. 60).

49 El Grupo de Trabajo del Artículo 29 es un órgano consultivo compuesto por un representante de las autoridades de control de los Estados miembros, el Supervisor Europeo de Protección de Datos (SEPD) y la Comisión (sin derecho de voto), que también realiza las funciones de secretaría. Véase: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

50 El Grupo de Trabajo del Artículo 29 tiene por misión asesorar a la Comisión sobre el nivel de protección en la UE y en los terceros países, así como sobre cualquier otra medida relativa al tratamiento de los datos personales.

La Comisión examinará los medios para:

- **reforzar, clarificar y armonizar el estatuto y los poderes de las autoridades nacionales de protección de datos** en el nuevo marco jurídico, incluida la plena aplicación del concepto de «total independencia»[51];

- **mejorar la cooperación y la coordinación entre las autoridades de protección de datos**;

- garantizar una aplicación más coherente de las normas de la UE en materia de protección de datos en todo el mercado interior, en particular, **reforzando el papel de los supervisores nacionales de protección de datos, coordinando mejor su trabajo a través del Grupo de Trabajo del Artículo 29 (que debería convertirse en un órgano más transparente), o creando un mecanismo destinado a garantizar la coherencia en el mercado interior bajo la autoridad de la Comisión Europea**.

3. CONCLUSIÓN: PERSPECTIVA FUTURA

Al igual que la tecnología, la forma en que nuestros datos personales se utilizan y comparten en nuestra sociedad está en evolución constante. El reto que esto plantea a los legisladores es el de establecer un marco legislativo que resista al tiempo. Al final del proceso de reforma, las normas europeas de protección de datos deberían seguir asegurando un elevado nivel de protección y garantizando la seguridad jurídica a las personas, a las Administraciones públicas y a las empresas en el mercado interior, durante varias generaciones. Independientemente de la complejidad de la situación o de la sofisticación de la tecnología, es esencial que las normas que deben aplicar las autoridades nacionales y que deben cumplir las empresas y los responsables del desarrollo de tecnologías, estén claramente definidas. Del mismo modo, las personas deben tener claros los derechos de que gozan.

El enfoque global previsto por la Comisión para abordar los problemas y alcanzar los objetivos esenciales puestos de relieve en la presente Comunicación servirá de base para los debates posteriores con las otras instituciones europeas y otras partes interesadas, y se traducirá a continuación en propuestas y medidas concretas de carácter legislativo y no legislativo. A tal efecto, la Comisión desearía recibir información sobre las cuestiones que se plantean en la presente Comunicación.

Sobre esta base, tras la elaboración de un análisis de impacto y teniendo en cuenta la Carta de los Derechos Fundamentales de la UE, la Comisión **presentará en 2011 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. Paralelamente, se adoptarán medidas no legislativas, como la promoción de la autorregulación y el examen de la viabilidad de los distintivos europeos de protección de la intimidad.

Como segundo paso, la Comisión **evaluará la necesidad de adaptar otros instrumentos jurídicos** al nuevo marco general de protección de datos. Esto afecta, en primer lugar, al Reglamento (CE) n° 45/2001, cuyas disposiciones deberán ser objeto de una adaptación.

[51] Véase la sentencia del Tribunal de Justicia, de 9 de marzo de 2010, en el asunto C-518/07, Comisión contra Alemania.

Convendrá también, en una fase posterior, examinar atentamente el impacto en otros instrumentos sectoriales.

La Comisión seguirá también controlando la adecuada aplicación del Derecho de la Unión en este ámbito, prosiguiendo una **política activa de represión de las infracciones** cuando las normas de la UE en materia de protección de datos no se apliquen correctamente. En efecto, la actual revisión de los instrumentos pertinentes no afecta en modo alguno a la obligación de los Estados miembros de aplicar y controlar la correcta aplicación de los instrumentos jurídicos existentes en materia de protección de los datos personales[52].

Un nivel elevado y uniforme de protección de datos en la UE será la mejor manera de defender y promover a escala mundial las normas europeas de protección de datos.

[52] Entre estos instrumentos figura la Decisión Marco 2008/977/JAI del Consejo: los Estados miembros deberán adoptar las medidas necesarias para cumplir las disposiciones de esta Decisión Marco antes del 27 de noviembre de 2010.