

# Interacciones judiciales en aplicación de la Carta de Derechos Fundamentales de la Unión Europea

## El derecho a la protección de datos y la privacidad

"E-LEARNING NATIONAL ACTIVE CHARTERTRAINING (E-NACT)"<sup>1</sup>

### Índice

1. La cultura europea de protección de datos.....	2
2. La Reforma de Protección de Datos de 2016: el RGPD y la fuerza vinculante de la Directiva .....	3
3. Principios generales sobre tratamiento de datos.....	4
4. Principales novedades del RGPD .....	6
5. Breve glosario de técnicas de interacción judicial .....	12

---

<sup>1</sup> Elaborado sobre la base del *Handbook on the Techniques of Judicial Interactions in the Application of the EU Charter. Data protection and privacy*, en el marco del Proyecto **E-LEARNING NATIONAL ACTIVE CHARTERTRAINING (E-NACT)**. Traducción a cargo de María Camila Medina. Publicación elaborada con el apoyo financiero del Programa de Justicia de la Unión Europea. Los contenidos de esta publicación son de la sola responsabilidad de sus autores, y en ningún caso reflejan la visión de la Comisión Europea.

## 1. La cultura europea de protección de datos

A través del caso *Schrems (2014)*, el Tribunal de Justicia de la Unión Europea (TJUE) dio un gran impulso a la protección de datos personales como está consagrado en la Carta de Derechos Fundamentales (en adelante, Carta), al afirmar la primacía del modelo europeo de protección de datos personales sobre otros sistemas jurídicos con menor protección<sup>2</sup>.

La relevancia de la cuestión prejudicial como técnica de diálogo judicial ha resultado fundamental en este caso, especialmente como un mecanismo capaz de activar el uso de la Carta. Esta ha sido aplicada no solo para aumentar la protección de datos a nivel constitucional, sino también como un mecanismo de control recíproco para promover el respeto del Estado de Derecho en los órganos de la Unión Europea y de los Estados parte.

El TJUE sostuvo que la existencia de una decisión de la Comisión que establece un nivel adecuado de protección de los datos personales transferidos, garantizados por terceros países, no puede eliminar o incluso reducir los poderes de las autoridades nacionales de control previstos en la Carta de los Derechos Fundamentales de la Unión Europea y en la Directiva. Sobre el particular, el Tribunal hizo énfasis en que el derecho a la protección de datos personales está garantizado por la Carta, y que esta encomienda su protección a las autoridades nacionales

En particular, la sentencia encontró que el Acuerdo de Puerto Seguro se ajustaba al nivel de adecuación requerido por la Directiva de Protección de Datos para el procesamiento de datos que resulten de la transferencia de datos a terceros países.

El Tribunal observó que el Acuerdo de Puerto Seguro (ahora reemplazado por el *Escudo para la privacidad*) se aplicaba únicamente a las empresas de Estados Unidos que se adhirieron a él, de modo que las autoridades públicas de Estados Unidos no estaban sujetas a este. Por otra parte, observó que las exigencias de seguridad nacional, interés público y cumplimiento de la ley prevalecían sobre el esquema de puerto seguro, de modo que las empresas de Estados Unidos no estaban obligadas a aplicar las normas de protección establecidas por dicho régimen en caso de conflicto. Así pues, el esquema de Puerto Seguro de Estados Unidos permitía la interferencia de las autoridades públicas en los derechos fundamentales de las personas como están consagrados en la Carta, y la decisión de adecuación de la Comisión no se refería a la existencia, en Estados Unidos, de reglas dirigidas a limitar algún tipo de interferencia o existencia de protección

---

<sup>2</sup>Ver *Maximilian Schrems v Data Protection Commissioner*, Case C-362/14, 6 October 2015, ECLI:EU:C:2015:650.

judicial efectiva contra estas, sino solo a la adecuación formal al esquema de Puerto Seguro.

En cuanto a un nivel de protección esencialmente equivalente a los derechos y libertades fundamentales garantizado dentro de la UE, el TJUÉ sostuvo que, conforme a la legislación de la UE, la legislación no se limita a lo que es estrictamente necesario cuando autoriza, de forma generalizada, el almacenamiento de todos los datos personales transferidos de la UE a los Estados Unidos sin ninguna diferenciación, limitación o excepción a la luz del objetivo perseguido y sin que se establezca un criterio objetivo para determinar los límites del acceso de los poderes públicos a los datos y de su uso posterior. El Tribunal agregó que se debe considerar que la legislación que permite a las autoridades públicas tener acceso de manera generalizada al contenido de las comunicaciones electrónicas compromete la esencia del Derecho fundamental al respeto a la vida privada.

Asimismo, el Tribunal observó que la legislación que no contempla la posibilidad de que un individuo pueda acudir a recursos judiciales para tener acceso a los datos personales relacionados con él, o para obtener la rectificación o eliminación de tales datos, compromete la esencia del derecho fundamental a la protección judicial efectiva, y que la existencia de dicha posibilidad guarda una relación intrínseca con la existencia del Estado de Derecho.

Desde esta perspectiva, la ampliación del alcance territorial del Reglamento General de Protección de Datos (art. 3), leído en conexión con los requisitos más estrictos establecidos para la transferencia de datos a terceros países (arts. 45-49), son esfuerzos significativos para mejorar la legislación de protección de datos de la UE a nivel mundial, dando por sentada la importancia de la Carta.

## **2. La Reforma de Protección de Datos de 2016: el RGPD y la fuerza vinculante de la Directiva**

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD), entró en vigor en mayo de 2018. Estas normas buscan proteger a todos los ciudadanos de la UE de la violación de la privacidad y los datos en un mundo cada vez más permeado por estos, al tiempo que crea un marco más claro y coherente para los negocios, aunque el RGPD se refiera como beneficiarios a todos los individuos, sin importar su nacionalidad o lugar de residencia (art. 1). Los nuevos derechos de los ciudadanos incluyen el consentimiento claro y afirmativo para el tratamiento de sus datos, así como el derecho a recibir

información clara y comprensible sobre el mismo; el derecho al olvido: un ciudadano puede solicitar que se borren sus datos; el derecho a transferir datos a otro proveedor de servicios (por ejemplo, cuando se cambia de una red social a otra); y el derecho a saber cuándo los datos han sido hackeados. Las nuevas reglas se aplican a todas las compañías que operan en la UE, incluso si están situadas fuera de la UE. Además, será posible imponer medidas correctivas, como amonestaciones y órdenes, o multas a las empresas que incumplan la ley.

La Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo entró en vigor en mayo de 2018. La directiva protege el derecho fundamental de los ciudadanos a la protección de datos cuando los datos personales sean utilizados por las autoridades policiales. Esto garantiza que los datos personales de las víctimas, testigos y sospechosos de delitos estén debidamente protegidos y facilita la cooperación transfronteriza en la lucha contra la delincuencia y el terrorismo<sup>3</sup>.

### 3. Principios generales sobre tratamiento de datos

#### *Legalidad, equidad y transparencia*

De acuerdo al principio de legalidad, el tratamiento de datos solo es legítimo si está justificado por la ley y puede tener lugar si está amparado por una autorización legal o por el consentimiento del interesado.

Se debe permitir a los individuos entender cómo se están manejando sus datos, en lo que respecta a la identidad del responsable, el propósito del procesamiento, así como los riesgos, reglas, salvaguardas y derechos en relación con las actividades de procesamiento y cómo pueden ejercer esos derechos.

La transparencia también es un principio relacionado con el procesamiento de datos personales. Debe ser transparente para las personas físicas que sus datos personales sean recopilados, utilizados, consultados o tratados de otro modo y en qué medida los datos personales son o serán procesados. Los fines específicos para los que los datos personales serán procesados deben ser explícitos, legítimos y determinados al momento de la recolección de la información personal. Además, se requiere que toda información y comunicación relacionada con el

---

<sup>3</sup> Fichas temáticas sobre la Unión Europea, disponibles en <http://www.europarl.europa.eu/factsheets/es/sheet/157/personal-data-protection>

procesamiento de esos datos personales sean de fácil acceso y comprensión, utilizando un lenguaje claro y sencillo.

Las personas físicas deben conocer los riesgos, normas, garantías y derechos relacionados con el procesamiento de datos personales, así como la manera de ejercer sus derechos en relación con el procesamiento. Estas son obligaciones del responsable de los datos.

Dicha información podrá proporcionarse en formato electrónico, por ejemplo, cuando se dirige al público, a través de un sitio web. Dado que los niños merecen protección específica, cualquier información y comunicación, donde el procesamiento está dirigido a un niño, debe estar en un lenguaje tan claro y sencillo que el niño pueda entenderlo fácilmente<sup>4</sup>.

Al respecto, debe prestarse la mayor parte de la atención al principio de limitación del propósito, según el cual los datos personales se deben recopilar para fines específicos, explícitos y legítimos, y no podrán procesarse de una manera incompatible con dichos propósitos. Un tratamiento posterior cuyo fin sea el interés público, o la investigación científica o histórica, o para fines estadísticos no se considerarán incompatibles con los fines iniciales, siempre no se consideren incompatibles con el propósito inicial, y siempre que los Estados miembros proporcionen las garantías adecuadas.

### *Responsabilidad*

El RGPD incluye el principio general de responsabilidad en el Artículo 5 (2), que impone la responsabilidad de la conformidad del procesamiento de datos con el RGPD y la obligación de mantener un registro del procesamiento de datos, así como la carga de la prueba del cumplimiento para el responsable.

### *Minimización de datos*

El procesamiento de los datos personales se restringirá a un uso adecuado, pertinente y limitado a lo necesario en relación con los fines para los que son tratados (rec 39RGPD), buscando la reducción de la recopilación de datos al nivel más bajo posible para lograr los propósitos de tratamiento.

### *Exactitud*

Este principio significa que se deben tomar todas las medidas razonables para garantizar que los datos estén actualizados, sean correctos, borrados o rectificadas<sup>5</sup>.

### *Integridad y confidencialidad*

---

<sup>4</sup>RGPD: rec 13, 39, 58, 60, 71, 78, 100, 121; Arts 5(1)(a), 12(1), 13(2), 14(2), 26(1), 40(2)(a), 41(2)(c), 42(3), 43(2)(d), 53(1), 88(2).

<sup>5</sup>RGPD: rec 39; Arts 5(1)(d), 18(1)(a).

La integridad y la confidencialidad son principios relacionados con el tratamiento de datos personales que a menudo se tratan juntos. En particular, se espera que los datos personales se traten de una manera que garantice su adecuada seguridad, incluyendo la protección contra tratamientos sin autorización o ilegales, y contra pérdida accidental, destrucción o daño. Esto se asegura mediante medidas técnicas y organizativas adecuadas. El responsable y el encargado deberán adoptar e implementar medidas técnicas y organizativas adecuadas para tal efecto.

El principio de confidencialidad tiene como objetivo la prevención del acceso no autorizado o el uso de datos personales, y de los equipos para el tratamiento. La legislación de los Estados miembros debe garantizar que las personas autorizadas para procesar los datos personales se comprometan con la confidencialidad o tengan una apropiada obligación legal de confidencialidad. Además, el responsable de protección de datos estará obligado al secreto o la confidencialidad en relación con el desempeño de sus tareas, de conformidad con la legislación de la Unión o del Estado miembro<sup>6</sup>.

## 4. Principales novedades del RGPD

### 4.1 Alcance del RGPD

#### *ALCANCE MATERIAL*

El RGPD es aplicable a cualquier tratamiento de datos personales de personas físicas. El reglamento será relevante para las empresas tan pronto como se lleve a cabo cualquier tratamiento de datos. El alcance (material) se interpreta de manera mucho más amplia para garantizar un mayor nivel de protección para las personas en relación con la protección prevista en el art. 7 de la CFR.

“Tratamiento” significa cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, según el Artículo 4 No. 2 del RGPD. Básicamente, cualquier operación de datos será considerada como tratamiento. Los ejemplos incluyen la recogida, registro, organización, estructuración y supresión o de datos.

El Artículo 2 Sec. 2 del RGPD establece cuatro excepciones en cuanto al alcance de aplicación material, de modo que no se aplica en las áreas fuera del alcance de la Ley de la Unión (a), de la política de seguridad (lit. b), de la relacionada con persecución criminal (lit. d), y de la actividad puramente personal o doméstica (c).

#### *ALCANCE TERRITORIAL*

---

<sup>6</sup>RGPD: rec 39, 49, 75, 83, 85, 162-163; Arts 5(1)(f), 28(3)(b), 32(1)(b), 38(5), 76.

Aunque el RGPD es un reglamento europeo, su alcance territorial se extiende más allá de las fronteras europeas. Dado el carácter no físico de los datos y el objetivo de garantizar el libre flujo de los mismos, la aplicación transnacional garantizará la privacidad integral de los individuos y condiciones de competencia justa en el mercado interior de la UE. Asimismo, se evitará el fenómeno del *forum shopping* (foro más conveniente): debido a las diferentes normas de protección de datos dentro de los Estados miembros de la UE, las empresas podían elegir su lugar de negocios de acuerdo con el nivel nacional más bajo de estándares de protección de datos (entre otros factores). Así, la legislación de la UE prescribe un ámbito territorial particularmente amplio.

Desde una perspectiva territorial, el RGPD no diferencia entre responsable o encargado y establece el mismo ámbito territorial para ambos. Principalmente, el RGPD se aplica en las siguientes dos situaciones:

- cuando el tratamiento de los datos personales se realiza en el contexto de las actividades de un establecimiento del responsable o encargado dentro de la UE; o
- cuando el procesamiento de los datos de individuos dentro de la UE se realiza mediante un responsable o encargado no establecido en la UE.

Sin embargo, el RGPD puede aplicar cuando ni el responsable, ni el encargado están establecidos en la UE. De acuerdo con este principio, la ley aplicable depende del lugar donde se ofreció la ejecución relevante del contrato. Incluso, la nacionalidad de los clientes no es relevante, en siempre que estén en la UE.

El RGPD establece un núcleo de temas tales como: el establecimiento, así como el ejercicio efectivo y real de la actividad a través de acuerdos estables; el principio de establecimiento, según el cual la elección del derecho aplicable depende del lugar donde se establezca una entidad; régimen estable, que significa que no importa si la entidad relevante es una sucursal o filial de una compañía con personalidad jurídica; estabilidad, que debe determinarse en relación con la naturaleza específica de la actividad.

La expresión "en el contexto de las actividades" debe interpretarse en el sentido de que tiene que haber una conexión entre la actividad económica del establecimiento y el tratamiento de datos, pero no es necesario que el establecimiento lleve a cabo algún tratamiento de datos.

Recientes decisiones judiciales también ilustran la aplicación extraterritorial de la ley de protección de datos. En el caso *Google Spain*, decidido en mayo de 2014, el TJUE sostuvo que debido a que las actividades de las filiales europeas de Google estaban estrechamente vinculadas al funcionamiento del motor de búsqueda de la empresa matriz de Google en Estados Unidos, el motor de búsqueda estaba sujeto a las normas de protección de datos de la UE. Además, en *Schrems*, decidido en octubre de 2015, el Tribunal invalidó el esquema de

Puerto Seguro entre la UE y EE. UU. porque no garantizaba una protección adecuada y efectiva contra el acceso a los datos por parte de las autoridades públicas de Estados Unidos con respecto a los datos personales que se habían transferido a Estados Unidos<sup>7</sup>.

#### **4.2. Transferencia de datos a terceros países**

Las transferencias de datos transfronterizas tienen que cumplir con las garantías proporcionadas por el RGPD, sobre la base de un doble enfoque: las transferencias de datos deben cumplir, no solo con la legalidad del tratamiento, sino también con las disposiciones específicas establecidas en los art. 44-49. Esto incluye también las transferencias posteriores.

La primera disposición establecida por el RGPD es la decisión de adecuación adoptada por la Comisión, de acuerdo con los requisitos mencionados en el art. 45. En ausencia de una decisión de adecuación, las reglas aplicables son las siguientes: el consentimiento explícitamente relacionado con la transferencia propuesta (Art. 49); garantías adecuadas, como las cláusulas contractuales estándar aprobadas por la Comisión o por las autoridades de control (art. 46); normas corporativas vinculantes aprobadas por la autoridad de control competente (art. 47).

Si no se aplican salvaguardas apropiadas o cláusulas contractuales estándar, el RGPD prevé excepciones para situaciones específicas - además del caso de consentimiento explícito- como, por ejemplo, la ejecución de un contrato; razones de interés público; el tratamiento necesario para el dereclamaciones legales (art. 49).

La novedad más importante delRGPD es que la falta de cumplimiento con los estándares establecidos en los art. 44-49 conllevan la aplicación de multas que ascienden a EUR 20,000,000.00 o hasta el 4% del total de la facturación anual mundial (Art. 83 RGPD).

#### **4.3 Categorías especiales de datos**

El legislador de la UE prohíbe el procesamiento de datos para categorías especiales (Art. 9 RGPD). Dichas categorías especiales son: 1) datos que revelan el origen racial o étnico, opiniones políticas, religiosas o creencias filosóficas, o afiliación sindical, 2) datos genéticos, 3) datos biométricos con el único propósito de identificar a una persona física, 4) datos relativos a la salud o 5) datos relativos a la vida sexual u orientación sexual de una persona natural. El tratamiento de estos datos está prohibido.

---

<sup>7</sup> D. Cooper – C. Kuner, 'Data protection law and Internatoional Dispute Resolution', Collected Course of the Hague Academy of International Law, Vol. 382, 2017, p. 71.



El tratamiento de estos datos está permitido cuando el procesamiento se lleve a cabo en materia de empleo o seguridad social; cuando sea necesario para proteger intereses vitales; cuando el interesado los ha hecho manifiestamente públicos; cuando el tratamiento sea necesario por razones de considerable interés público; cuando sea necesario por razones de interés público en el área de la salud pública o para medicina predictiva u ocupacional; cuando sea necesario para satisfacer el interés público.

En lo que respecta a los datos genéticos, los datos biométricos y los datos relativos a la salud, los Estados miembros podrán introducir más limitaciones.

El RGPD introduce por primera vez el concepto de:

#### *Datos biométricos*

Los datos biométricos son una categoría especial de datos personales, resultado de un procesamiento técnico relativo a las características físicas, psicológicas o de comportamiento de una persona, que permiten confirmar su única identificación como persona natural.

Los datos biométricos constituyen una de las categorías de datos especiales. Por su naturaleza particularmente sensible con relación a los derechos y libertades fundamentales, merecen una protección específica, ya que el contexto de su tratamiento podría crear riesgos significativos. En principio, su tratamiento está prohibido, salvo que se encuentre permitido por el Reglamento, la Directiva o por una ley más estricta del Estado parte. También es fundamental que el tratamiento sea estrictamente necesario y que a él se apliquen las garantías adecuadas para los derechos y libertades los datos del sujeto.

#### *Datos genéticos*

Estos datos también se encuentran dentro de las categorías especiales de datos para las que el RGPD (art. 9) y la Directiva (art. 10) prevén normas especiales para su tratamiento. Específicamente, los datos genéticos, así como otras categorías especiales de datos, se deben tratar para propósitos relativos a la salud, solo para el beneficio de las personas físicas y de la sociedad como un todo considerado, o para servir al interés público, o para efectos de investigación científica, histórica o estadística.

### **4.4 Consentimiento**

El consentimiento ya no tiene la misma relevancia que tuvo bajo la Directiva 46/95/EC, pues ahora solo es una de las normas sobre tratamiento de datos. A pesar de su relevancia, se ha incluido entre otras justificaciones para el tratamiento de datos. En particular, debido al hecho de que el consentimiento se debe dar libremente, en casos de clara desigualdad entre la persona interesada y el responsable. Por ejemplo, el RGPD prohíbe el consentimiento como condición

para la ejecución de un contrato. El interesado puede retirar su consentimiento en cualquier momento (Art. 7 (3)).

En cuanto al consentimiento de los niños, el RGPD contiene una novedad al establecer la edad mínima de 16 años para su validez y permite el de los titulares de la patria potestad de los niños menores de esta edad.

Entre las otras normas del tratamiento lícito, este podrá estar basado en aquel que es (Art. 6, b) necesario para la ejecución de un contrato del cual el interesado es parte; (Art. 6, c) necesario para el cumplimiento de las obligaciones legales de las que está sujeto el controlador; (Art. 6, d) necesario para proteger el interés vital del interesado; (Art. 6, e) el cumplimiento de una misión realizada en interés público; (Art. 6, f) necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.

Si el consentimiento se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo (Art 7 (2)RGPD).

A pesar de que el RGPD no contiene requisitos formales como el consentimiento, en comparación con la Directiva, este contiene condiciones más estrictas para obtener el consentimiento de la persona interesada. La forma escrita es deseable, aunque no es obligatoria. En particular, si el consentimiento se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud del consentimiento se presentará de manera tal que se diferencie de las otras materias, en una forma inteligible y de fácil acceso, usando un lenguaje claro y sencillo.

#### **4.5 Mecanismo de competencia de la autoridad de control principal**

El mecanismo de competencia de la autoridad de control principal (“*one stop shop*”) previsto en el Art. 56 del RGPD supone, como regla general, que las organizaciones que lleven a cabo actividades de tratamiento de datos transfronterizo solo deberán comparecer ante una autoridad de control en el futuro.

#### **4.6 Automatización de la toma de decisiones**

Respecto de las técnicas “de elaboración de perfiles” – que incluyen cualquier forma de tratamiento automático de datos personales consistentes en su uso para evaluar ciertos aspectos personales relacionados con las personas físicas, en particular, para analizar o predecir aspectos relacionados con su actuación en el trabajo, su situación económica, su salud, sus preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos- el RGPD prevé una particular forma de protección de los datos del interesado en caso de procesos automatizados. De hecho, de acuerdo con el art. 22 RGPD, todo interesado tendrá

derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Hay excepciones previstas en caso de que una decisión automatizada sea necesaria para la celebración o ejecución de un contrato entre el interesado y un responsable del tratamiento; si está autorizada por el Derecho de la Unión o por el de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; o si está basado en el consentimiento explícito del interesado. En todo caso, estas excepciones no se aplican a las categorías especiales de datos previstas en el art. 9.

#### ***4.7 Portabilidad de datos***

El interesado tendrá el derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, así como tendrá derecho a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los facilitó. Este derecho aplicará cuando el interesado haya proporcionado sus datos con su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato; o en caso de que el tratamiento se realice por medios automatizados. Esto también incluye el derecho del interesado a que sus datos sean transmitidos directamente de un responsable a otro, cuando sea técnicamente posible. Sin embargo, lo anterior no aplicará para el tratamiento necesario para el desarrollo de una misión desarrollada con base en el interés público o en ejercicio de poderes públicos conferidos al responsable.

Los derechos y libertades de otros, así como el derecho a borrar los datos del interesado no se verán comprometidos con el ejercicio de la portabilidad.

El límite intrínseco de este derecho – cuyo propósito es asegurar la libre competencia entre proveedores de servicios- es que aplicará solo cuando el tratamiento este basado en el consentimiento del interesado. Sin embargo, el art. 23 del RGPD concede una amplia competencia a los Estados miembro para limitar los derechos del interesado.

#### ***4.8 Medidas organizativas***

El RGPD establece medidas organizativas específicas para los responsables y encargados, de las cuales deriva su responsabilidad legal de cumplir con las obligaciones que surgen del GDRP Este aspecto se discutirá en la sección de las obligaciones de los responsables y encargados.

#### ***4.9 Comité Europeo de Protección de Datos***

El art. 68 del RGPD crea un Comité Europeo de Protección de Datos que reemplaza el Grupo de Trabajo previsto en el art. 29 de la Directiva de Protección de Datos.

#### 4.10 Sanciones

El RGPD ha hecho más estrictos los recursos y sanciones por la violación del derecho a los datos personales. De manera particular, las multas administrativas han sido diseñadas por la UE en aras de desincentivar las violaciones por parte de los responsables, al afectar sus activos comerciales o empresas.

### 5. Breve glosario de técnicas de interacción judicial

La mayoría de las siguientes técnicas de interacción judicial se han descrito en el contexto del proyecto ACCIONES (*Active Charter Training Through Interaction Of National Experiences*), un proyecto bajo la coordinación del Centro de Cooperación Judicial del IUE, finalizado el 31 de octubre 2017<sup>8</sup>. De aquí en adelante, proporcionaremos una descripción general de las técnicas de interacción judicial más comunes.

#### A) TÉCNICAS DE INTERPRETACIÓN

##### **Interpretación conforme**

Tradicionalmente, los jueces nacionales deben interpretar el derecho interno de conformidad con su constitución. Además, también están obligados a interpretar el derecho interno de tal manera que no incumplan las obligaciones del derecho de la UE y de la Convención Europea de Derechos Humanos. Estos deberes son resultado del principio de primacía del derecho de la UE sobre el derecho interno, y de las obligaciones de las Altas Partes Contratantes para asegurar que el Convenio sea implementado en el ordenamiento interno. De acuerdo con la doctrina de la interpretación conforme, un juez nacional debe elegir entre todas las posibles formas de interpretación de una norma de derecho interno, aquella que no entre en conflicto con el derecho de la Unión o con el Convenio. En particular, en la medida que el derecho de la Unión se encuentre involucrado, la interpretación conforme es una técnica que en ocasiones permite a los jueces nacionales superar la falta de implementación de la legislación de la UE por el legislador nacional, limitando eventualmente las implicaciones de una falta de efecto horizontal sobre ciertas fuentes secundarias del derecho de la UE (especialmente, directivas). En aras de realizar una interpretación conforme con el

---

<sup>8</sup>Al respecto, consultar la base de datos disponible en: <http://judcoop.eui.eu/data/?p=data>.

derecho de la UE, los jueces nacionales deben analizar el derecho interno disponible (en conjunto) para alcanzar el propósito de la norma de la UE.

### ***Razonamiento comparado***

También puede ser útil revisar las aproximaciones que tienen los legisladores de otros Estados o Tribunales extranjeros a problemas o preguntas jurídicas similares. Así pues, esta técnica puede ofrecer soluciones adoptadas por otros jueces nacionales que se han enfrentado a la aplicación de la misma norma de derecho de la UE o del Convenio, o cuando el Estado actúa dentro del margen de apreciación/discrecionalidad. El juez nacional que quiera utilizar esta técnica de comparación tendrá que 1) elegir una decisión extranjera que pueda ser útil para solucionar sus propios casos; 2) adoptar una solución aplicada en un contexto distinto al de su ordenamiento jurídico.

## **B) RELACIÓN ENTRE NORMAS LEGALES**

### ***Inaplicación***

Probablemente esta técnica es la que implica el mayor grado de intervención del derecho supranacional/internacional en el ordenamiento jurídico interno de los Estados Miembros, en la medida que requiere que los jueces nacionales dejen de lado las normas internas en conflicto con el derecho de la UE, la Convención Europea sobre Derechos Humanos o el derecho internacional. Así las cosas, esto presupone un juicio de incompatibilidad entre la norma nacional y las normas supranacionales/internacionales relevantes. Determinar la incompatibilidad de una norma nacional con una de nivel europeo que podría conllevar a la inaplicación de la norma nacional no conlleva a su invalidez. Simplemente impide su aplicación en casos específicos. Las consecuencias de la inaplicación en la vida de la norma interna inaplicada no están reguladas por el derecho internacional/supranacional, los cuales dejan un margen al derecho nacional para resolver este problema.

## **C) INTERACCIÓN ENTRE DERECHOS (NACIONAL/UE)**

### ***Test de proporcionalidad***

Esta técnica requiere que los jueces nacionales valoren si la medida de derecho interno que interfiere con una norma supranacional/internacional (que garantiza un derecho fundamental a nivel europeo) persigue un fin legítimo, si realmente contribuye a alcanzar este fin y si la medida es la menos restrictiva para alcanzarlo. Esta técnica es posible solo en el caso de derechos fundamentales que pueden ser limitados, y con el propósito de ponderar la garantía de derechos fundamentales contra los poderes públicos o entre distintas garantías de derechos fundamentales.

## **D) RELACIÓN ENTRE CORTES**

### ***Cuestión prejudicial***

El art. 267 del TFUE prevé un mecanismo de cooperación directa entre los jueces nacionales y el TJEU. Este permite a cualquier corte nacional elevar preguntas sobre la interpretación o validez del derecho de la UE ante el TJEU. En principio, las cortes cuyas decisiones no tengan recursos a nivel interno deberán elevar una cuestión prejudicial en caso de dudas sobre la interpretación o validez de una norma de la UE, mientras otros tribunales están obligados a elevar la cuestión solo cuando consideren que la norma de derecho de la UE aplicable su caso no es válida.

## E) APROXIMACIÓN DEFERENTE

### *Margen de apreciación*

Con el fin de preservar la autonomía de regulación y la identidad constitucional de los Estados miembro, el CEDH les deja cierto margen de discreción para implementar las obligaciones del Convenio. Esto es particularmente cierto respecto de derechos fundamentales en dos hipótesis. Primero, cuando no hay consenso europeo en cuanto a la interpretación y aplicación de un derecho. Segundo, cuando los derechos deben ponderarse con otros, en cuyo caso la elección de la ponderación adecuada está a cargo del Estado. La doctrina del margen de apreciación implica que la aplicación del CEDH no sea necesariamente uniforme entre todos los Estado parte, mientras que, en principio, la aplicación de la Carta de Derechos Fundamentales está menos interesada en las particularidades internas y promueve el cumplimiento incondicional de los estándares uniformes de protección consagrados en esta (el TJUE dijo expresamente en *Melloni* que “la primacía, unidad y efectividad del derecho de la UE” no debería verse comprometido por la adopción de estándares nacionales).

### *Autolimitación de los jueces*

Es una aproximación procesal o sustancial al ejercicio de la revisión judicial. Como doctrina de procedimiento, este principio de autolimitación insta a los jueces a abstenerse de decidir cuestiones legales, y especialmente constitucionales, a menos que la decisión sea necesaria para resolver una controversia concreta. Como un principio sustancial, insta a los jueces a considerar cuestiones constitucionales para otorgar una deferencia sustancial a los puntos de vista de las ramas del gobierno e invalidar sus acciones solo cuando hayan violado claramente los límites constitucionales<sup>9</sup>

### *Protección equivalente*

Esta doctrina se ha desarrollado para regular la relación entre el Tribunal de Justicia de la Unión Europea y la Corte Europea de Derechos Humanos. Es una técnica de interacción horizontal, que tiene como fin asegurar que la protección de derechos fundamentales por el derecho de la UE pueda considerarse equivalente

---

<sup>9</sup> Al respecto, ver <https://www.britannica.com/topic/judicial-restraint>.

a la protección de estos bajo el sistema de la Convención, teniendo como única excepción para refutar esta doctrina, que la protección bajo la Convención sea manifiestamente deficiente (caso *Bosphorus*).

Concretamente, el apartado 3 del art. 52 tiene por objeto garantizar la coherencia necesaria entre la Carta y el CEDH estableciendo la regla de que, en la medida en que los derechos en la presente Carta también correspondan a los derechos garantizados por el CEDH, el significado y alcance de esos derechos, incluidas las limitaciones autorizadas, son las mismas que las establecidas por el CEDH. Esto significa, en particular, que el legislador, al fijar limitaciones a estos derechos, deba respetar las mismas normas establecidas por el régimen preciso de limitaciones contemplado en el CEDH, que se aplican por consiguiente a los derechos contemplados por este apartado, sin que ello afecte a la autonomía del Derecho de la Unión y del TJUE<sup>10</sup>.

---

<sup>10</sup>Ver explicaciones relativas a la Carta de Derechos Fundamentales, Art. 52. Explanations relating to the Charter of Fundamental Rights, Art. 52-Alcance e interpretación, Diario Oficial de la Unión Europea C 303/17 - 14.12.2007, available at <https://fra.europa.eu/en/charterpedia/article/52-scope-and-interpretation-rights-andprinciples>