EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

19 December 2019

Directrices del SEPD para la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales

edps.europa.eu

Índice

I. El objetivo de las presentes Directrices y cómo utilizarlas

Los **derechos fundamentales,** consagrados en la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «**la Carta**»), forman parte de los **valores fundamentales** de la Unión Europea,que también se recogen en el Tratado de la Unión Europea (en lo sucesivo, «el TUE»)[1]. Entre estos derechos, se encuentran los derechos fundamentales a la intimidad y a la protección de los datos personales, consagrados en los artículos 7 y 8 de la Carta. Estos derechos fundamentales deben ser respetados en todo momento por parte de las instituciones y organismos de la UE, inclusive a la hora de diseñar y aplicar nuevas políticas o al adoptar cualquier medida legislativa nueva. Existen otras normas sobre derechos fundamentales que también desempeñan un papel muy influyente en el ordenamiento jurídico de la UE,en particular los establecidos en el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades (en lo sucesivo, **el** «**CEDH**»)[2].

Las **condiciones de las posibles limitaciones** al ejercicio de los derechos fundamentales son una de lascaracterísticas más importantes de la Carta, puesto que determinan **en qué medida es posible ejercer efectivamente los derechos**[3].

La **necesidad** y la **proporcionalidad** de una medida legislativa que implique una limitación de los derechos fundamentales a la intimidad y a la protección de los datos personales son un **doble requisito**esencial que debe cumplir cualquier medida propuesta que implique el tratamiento de datos personales.No obstante, el hecho de garantizar que **la protección de datos** se convierta en una **parte integral en la elaboración de políticas de la UE** requiere no solo la comprensión de los principios expresados en el marco jurídico y en la jurisprudencia pertinente, sino también un **enfoque práctico y creativo** de lassoluciones a problemas complejos, con prioridades políticas que a menudo chocan entre sí[4].

El **Tribunal de Justicia de la Unión Europea** (en lo sucesivo, «el TJUE») ha reconocido que la legislación de la UE a menudo debe cumplir **varios objetivos de interés público** que a veces pueden ser contradictorios y que exigen un **justo equilibrio** entre los distintos derechos fundamentalesprotegidos por el ordenamiento jurídico de la UE[5]. Así, entre estos derechos e intereses, consagrados en la Carta,

---

[1] El artículo 2 del TUE establece que «La Unión se fundamenta en los valores de respeto de la **dignidad humana, libertad, democracia, igualdad, Estado de derecho y respeto de los derechos humanos, incluidos los derechos de las personaspertenecientes a minorías**». Además, el artículo 6, apartado 1, del TUE reconoce los **derechos, libertades y principios recogidos en la Carta**, que tiene el mismo valor jurídico que los tratados (la negrita es nuestra).

[2] El artículo 6, apartado 3, del TUE establece que «Los derechos fundamentales que garantiza el Convenio Europeo para laProtección de los Derechos Humanos y de las Libertades Fundamentales y los que son fruto de las **tradiciones constitucionales comunes a los Estados miembros** formarán parte del **Derecho de la Unión como principios generales**.» (la negrita es nuestra).

[3] El artículo 52, apartado 1, de la Carta establece que «Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Solo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechosy libertades de los demás».

[4] Véase **la publicación «*EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience*»**, del 4 de junio de 2014, disponible en: https://edps.europa.eu/data-protection/our-work/publications/papers/edps-advisor-eu-institutions-policy-and-legislation_en.

[5] Asunto C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU*, ECLI:EU:C:2008:54,apartado 68. En los asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB*, el Abogado General Saugmandsgaard Øe explicó en sus conclusiones, ECLI:EU:C:2016:572 apartado 247, que «*esta exigencia de proporcionalidad en el seno de unasociedad democrática —o proporcionalidad "stricto sensu"— se deriva a la vez del artículo 15, apartado 1, de la Directiva 2002/58, del artículo 52, apartado 1, de la Carta y de una reiterada jurisprudencia. Según esta reiterada jurisprudencia, una medida que menoscabe derechos fundamentales sólo puede considerarse proporcionada si las desventajas ocasionadas* ***no son desproporcionadas*** *con respecto a los objetivos perseguidos.*» (la negrita es nuestra). En el apartado 248 tambiénseñaló que la exigencia de proporcionalidad en este caso concreto de retención de gran cantidad de datos «*abre así un debate sobre los queremos valores que deben prevalecer en una sociedad democrática y, en definitiva, sobre el tipo de sociedad en el que vivir.*».

se pueden incluir: el derecho a la vida (artículo 2) y a la integridad de la persona (artículo 3); el derecho a la libertad y la seguridad (artículo 6); la libertad de expresión (artículo 11); la libertad de empresa (artículo 16); el derecho a la propiedad, incluida la propiedad intelectual (artículo 17); y el derecho de acceso a losdocumentos (artículo 42).

Las presentes Directrices pretenden servir de **ayuda a la hora de evaluar la conformidad** de las medidas propuestas respecto de la legislación de la UE sobre protección de datos. Se han elaborado para equipar mejor a los responsables políticos y legislativos de la UE encargados de **preparar o examinarlas medidas que implican el tratamiento de datos personales** y limitan los derechos a la protección de los datos personales y a la intimidad. Su objetivo es ayudar a los responsables políticos y a los legisladores, una vez identificadas las medidas que tienen un impacto en la protección de datos y las prioridades y objetivos que subyacen tras estas medidas, así como encontrar soluciones que minimicenel conflicto entre estas prioridades y que sean proporcionales.

El SEPD subraya la responsabilidad del legislador a la hora de evaluar la proporcionalidad de una medida. Así, las presentes Directrices no pretenden ni pueden proporcionar una evaluación definitiva sobre si una medida específica propuesta puede considerarse proporcional.Más bien, ofrecen una **metodología práctica, paso a paso**, para evaluar la proporcionalidad de las nuevas medidas legislativas, con explicaciones y ejemplos concretos. Responden a las solicitudes de las instituciones de la UE de orientación sobre los requisitos particulares derivados del artículo 52, apartado 1, de la Carta.

Las presentes Directrices **complementan** el conjunto de herramientas del SEPD *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit* («Conjunto de herramientas sobre la evaluar la necesidad de medidas que limiten el derecho fundamental a la protección de los datos personales», en lo sucesivo, «**el Manual sobre la Necesidad**»)[6] y profundizan, con respecto a los derechos a la intimidad y a la protección de los datos personales[7], las directrices existentes elaboradas por la Comisión Europea, el Consejo de la UE y la Agencia de los Derechos Fundamentales de la Unión Europea (en losucesivo, «la FRA»), sobre las limitaciones de los derechos fundamentales en general, en relación, por ejemplo, con las evaluaciones de impacto y los controles de compatibilidad[8].

---

[6] SEPD, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*,11 de abril de 2017, disponible en:

https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.

[7] En las presentes Directrices, a menudo se hace referencia a la «protección de datos» para referirse tanto al derecho a **la intimidad** como a la **protección de los datos personales**. No obstante, señalamos que se trata de derechos distintos. Sobre la diferencia entre ambos, véase: https://edps.europa.eu/data-protection/data-protection_en.

[8] Véase la **Herramienta n.º 28** de la Comisión Europea sobre **Derechos fundamentales y derechos humanos, que forma parte del manual «Caja de herramientas para la mejora de la legislación»**, disponible en https://ec.europa.eu/info/files/better-regulation-toolbox-28_en,
y el análisis en mayor profundidad que se incluye en el **documento de trabajo de los servicios de la Comisión**, «***Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments***», SEC (2011) 567 final (Directrices Operativas relativas a la consideración de los derechos fundamentales en las evaluaciones de impacto de la [SEC(2011) 567 final de 6.5.2011), disponible en http://ec.europa.eu/smart-regulation/impact/key_docs/docs/sec_2011_0567_en.pdf.
Véanse también «***Council Guidelines on methodological steps to be taken to check fundamental rights compatibility at the Council preparatory bodies***» (**(Directrices del Consejo sobre las medidas metodológicas que se han de tomar para verificar la compatibilidadde los derechos fundamentales en los órganos preparatorios)**, 5377/15, 20 de enero de 2015, disponibles en https://www.consilium.europa.eu/media/30209/qc0214079enn.pdf ,
y el **Manual de la FRA «Aplicación de la Carta de los Derechos Fundamentales de la Unión Europea en la elaboraciónde normas y políticas de ámbito nacional. Directrices»**, mayo de 2018, disponible en http://fra.europa.eu/en/publication/2018/national-guidance-application-eu-charter.
Estos documentos abarcan todos los derechos fundamentales, por lo que también hacen referencia a varios ejemplos de jurisprudencia del TJUE relativos a los derechos consagrados en los artículos 7 y 8 de la Carta.

El objetivo de las presentes Directrices es profundizar en las cuestiones relativas al impacto sobre los derechos fundamentales a la intimidad y a la protección de los datos personales, y ofrecer ejemplos pertinentes al respecto, ampliando y complementando, en particular, **la Herramienta n.º28** del **Manual «Caja de herramientas para la mejora de la legislación»** de la Comisión y las «**Orientaciones operativas para tener en cuenta los derechos fundamentales en las evaluaciones de impacto de la Comisión» (*Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments*)**.

El SEPD observa que, en los últimos años, la protección de los datos personales ha ido ganando peso yse reconoce cada vez más como una dimensión que debe tener en cuenta el legislador en todos los ámbitos políticos y gran parte de las iniciativas de la Comisión. Esto no solo se debe a una mayor concienciación de la población, sino al **enorme incremento de la capacidad de procesamiento de datos** (que hasta hacepoco parecían inofensivos) **con capacidad para afectar de manera significativa a la vida de todos ycada uno de los ciudadanos**.

Para facilitar los esfuerzos de la Comisión para tener en cuenta esta dimensión clave, **de forma proactiva**, **ya en el momento de la preparación de la Evaluación del Impacto**, también se hacereferencia, en la parte operativa de las presentes directrices, a la **terminología de la metodología de Evaluación del Impacto de la Comisión** (es decir: ***Motores; Causas; Definición del problema; Impacto***).

A la vista de las complejidades y especificidades de este ejercicio, el SEPD **está comprometido y dispuesto a ayudar a los servicios de la Comisión, incluso contribuyendo a las tareas de Evaluación del Impacto**, para proporcionar una fuente de información valiosa relativa a la protección de datos como derecho fundamental.

Se podrá contactar con la Unidad de Política y Consulta del SEPD para cualquier pregunta sobre las presentes orientaciones y sobre cómo evaluar el impacto de los actos legislativos sobre los derechos fundamentales a la intimidad y a la protección de los datos personales. Para ello, se podrá contactar a través de la dirección de correo electrónico operativa de la Unidad de Política y Consulta: POLICY- CONSULT@edps.europa.eu.

Es importante destacar que la **necesidad y la proporcionalidad**, si bien es cierto que están estrechamente vinculadas entre sí (son dos condiciones que debe cumplir la legislación), implican **dos evaluaciones diferentes**. Esto se pone de manifiesto en la sección III de las presentes Directrices, en laque se presenta la lista de comprobación práctica paso a paso de la proporcionalidad, con la que se ofrece la primera visión holística del **flujo de trabajo global.**

Las Directrices constan de una **introducción**, que expone su contenido y finalidad, un **análisis jurídico** del criterio de proporcionalidad aplicado al tratamiento de datos personales y una **lista de comprobación práctica, paso a paso**, para evaluar la proporcionalidad de las nuevas medidas legislativas. La lista de comprobación es la parte

fundamental de las presentes Directrices y puede usarsede forma independiente.

Las Directrices se basan en la **jurisprudencia**[9] del TJUE, del Tribunal Europeo de Derechos Humanos(en lo sucesivo, «el TEDH»), en los dictámenes del SEPD y del Grupo de Trabajo del Artículo 29 (en lo sucesivo, «el GT29»), así como en las directrices del Comité Europeo de Protección de Datos (en adelante, «el CEPD»).

Junto con el **Manual sobre la necesidad**, con las presentes Directrices pretendemos proporcionar **un enfoque común para la evaluación de la necesidad y la proporcionalidad** de las medidas legislativascon respecto al derecho a la intimidad y a la protección de los datos personales.

II. Análisis jurídico: la evaluación de la proporcionalidad aplicada al derecho a la protección de datos personales

1. **La evaluación de la proporcionalidad** a la hora de valorar la legalidad de cualquier medidapropuesta que implique el tratamiento de datos personales

El artículo 8 de la Carta consagra el **derecho fundamental a la protección de los datos personales**. Este **no es un derecho absoluto** y **puede limitarse**, siempre que las limitaciones cumplan los requisitosprevistos en el artículo 52, apartado 1, de la Carta. El mismo análisis se aplica al **derecho al respetode la vida privada** consagrado en el artículo 7 de la Carta[10].

Para ser legal, cualquier limitación del ejercicio de los derechos fundamentales protegidos por la Cartadebe cumplir los **siguientes criterios**, establecidos en el artículo 52, apartado 1, de la Carta:

- debe estar **prevista por ley**;

---

[9] Para una visión general de la **jurisprudencia** pertinente del TJUE y del TEDH, véase: **FRA, *Manual de legislación europea en materia de protección de datos***, edición de 2018, disponible en: http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law.
Véase también «*Factsheet - Personal data protection*», publicado en noviembre de 2018 por el TEDH a través de la Unidad dePrensa, disponible en: https://www.echr.coe.int/Documents/FS_Data_ENG.pdf.

[10] En los asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke y Hartmut Eifert*, la Abogada General Sharpstonexplicó en sus conclusiones, ECLI:EU:C:2010:353, apartado 73, que «*Como varios de los derechos clásicos del CEDH,el derecho a la intimidad **no es un derecho absoluto**. El artículo 8, apartado 2, del CEDH reconoce expresamente la posibilidad de excepciones a ese derecho, al igual que el artículo 9 del Convenio n.º 108 respecto al derecho a la protección de los datos personales. El artículo 52 de la Carta establece, asimismo (en términos generales) criterios similares que, en caso de cumplirse, permiten excepciones (o limitaciones) a los derechos de la Carta.*» (la negrita es nuestra). Este enfoque se vio confirmado por la sentencia del TJUE, ECLI:EU:C:2010:662, apartados 48-50.
Sobre el derecho a la protección de datos personales como «no absoluto», véase el considerando 4 del Reglamento (UE) 2016/679 (el «Reglamento General de Protección de Datos», en lo sucesivo, «el RGPD»): «*El tratamiento de datos personalesdebe estar concebido para servir a la humanidad. El **derecho a la protección de los datos personales no es un derecho absoluto** sino que debe considerarse **en relación con su función en la sociedad** y mantener el **equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.***» (la negrita es nuestra).
Sobre la diferencia entre los **derechos absolutos** (como la prohibición de la tortura y de las penas o tratos inhumanos o degradantes consagrada en el artículo 4 de la Carta) y los **derechos sujetos a limitaciones** (como el derecho a la intimidad y a la protección de los datos personales), véase el documento de trabajo de los servicios de la Comisión «*Operational Guidanceon taking account of Fundamental Rights in Commission Impact Assessments*» (Directrices operativas para tener en cuenta los derechos fundamentales en las evaluaciones de impacto de la Comisión Europea), SEC (2011) 567 final, página 9, y el manual dela FRA «Aplicación de la Carta de los Derechos Fundamentales de la Unión Europea en la elaboración de normas y políticas de ámbito nacional. Directrices», mayo de 2018, página 70.
Una consecuencia importante de esta distinción es que **los derechos absolutos no pueden limitarse y, por tanto, no están sujetos a un equilibrio con otros derechos o intereses**. Por consiguiente, en los casos en que el **derecho a la intimidad concurre con** (va en la misma línea que) **un derecho absoluto** (por ejemplo, el derecho a no ser sometido a torturas), **ambosderechos (concurrentes) no estarán sujetos a un equilibrio** con otros derechos o intereses (por ejemplo, la seguridad nacional).

- debe **respetar la esencia** de los derechos;
- debe **responder realmente a objetivos de interés general** reconocidos por la Unióno a la necesidad de proteger los derechos y libertades de los demás;
- debe ser **necesaria**, el tema que aborda el Manual sobre la Necesidad; y
- debe ser **proporcional**, que es el objetivo de las presentes Directrices.

Esta lista de **macrocriterios** establece el **orden** necesario para la **evaluación de** la legalidad de unalimitación del ejercicio de un derecho fundamental.

1. En primer lugar, debe examinarse si la ley que establece una limitación es **accesible y previsible**[11]**.** Si no se cumple este requisito, la medida será ilegal y no será necesario seguir analizándola[12].

---

[11] En virtud del artículo 52, apartado 3, de la Carta, «*En la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán iguales a los que les confiere dicho Convenio. Esta disposición no impide que el Derecho de la Unión conceda una protección más extensa*». En cuanto al concepto de «**previsto por la ley**», en virtud del artículo 52, apartado 1, de la Carta, deben utilizarse los criterios desarrollados por el TEDH, tal como se sugiere envarias conclusiones de los abogados generales del TJUE: véanse, por ejemplo, las conclusiones en los asuntos acumulados C-203/15y C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:572, apartados 137-154, y en el asunto C-70/10, *Scarlet Extended*, ECLI:EU:C:2011:255, apartados 88-114. Por consiguiente, se puede hacer referencia, entre otras, a la sentencia del TEDH en el asunto *Weber y Saravia contra Alemania*, apartado 84: «*El Tribunal de Justicia reitera que la expresión "conforme a la ley" en el sentido del artículo 8, apartado 2,* [del CEDH] *exige, en primer lugar, que la medida impugnada tenga algún fundamento en el derecho interno; también se refiere a la calidad de la ley en cuestión, exigiendo que sea accesible a la persona afectada, que deberá, además, poder prever sus consecuencias para sí misma, y deberá ser compatible con el Estado de derecho*».
Véase también el considerando 41 del RGPD: «*dicha base jurídica o medida legislativa deberá ser **clara** y **precisa** y su aplicación **previsible para sus destinatarios**, de conformidad con la jurisprudencia del Tribunal de Justicia de la Unión Europea [...] y del Tribunal Europeo de Derechos Humanos.*» (la negrita es nuestra).

- Sobre la noción de «**previsibilidad**» en el contexto de la **interceptación de comunicaciones,** véase el asunto del TEDH, *Zakharov c. Rusia*, apartado 229: «*El Tribunal de Justicia ha establecido en repetidas ocasiones que la referencia a la "previsibilidad" en el contexto de la interceptación de las comunicaciones no puede ser la misma que en muchos otros ámbitos. La previsibilidad en el contexto especial de las medidas secretas de vigilancia, como la interceptación de las comunicaciones,no puede significar que una persona deba ser capaz de prever cuándo es probable que las autoridades intercepten sus comunicaciones para poder adaptar su conducta en consecuencia. Sin embargo, especialmente cuando un poder conferido al ejecutivo se ejerce en secreto, los riesgos de arbitrariedad son evidentes. Por tanto, es esencial contar con normas claras y detalladas sobre la interceptación de las conversaciones telefónicas, particularmente porque la tecnología disponible para su uso es cada vez más sofisticada. El derecho interno debe ser lo suficientemente claro como para ofrecer a los ciudadanos una indicación adecuada de las circunstancias y condiciones en las que las autoridades públicas están facultadas para recurrir a tales medidas*» (el subrayado es nuestro). En el mismo sentido, más recientemente, véase *Big Brother Watch y otros contra Reino Unido*, TEDH, 13 de septiembre de 2018, apartado 306.
- Véase también el asunto *Shimovolos contra Rusia,* TEDH, 21 de junio de 2011.

[12] Véase el asunto del TEDH *Benedik contra Eslovenia*, apartado 132: «*el Tribunal de Justicia considera que la ley en la que se basóla medida impugnada, es decir, la obtención por parte de la policía de la información del abonado asociada a la dirección IP dinámica en cuestión [...], y la forma en que fue aplicada por los tribunales nacionales **carecían de claridad** y no ofrecían suficientes garantías contra la injerencia arbitraria en los derechos previstos en el artículo 8. En tales circunstancias, el Tribunalconsidera que la injerencia en el derecho del demandante al respeto de su vida privada **no fue "conforme a la ley"** como exigeel artículo 8, apartado 2, del Convenio. Por consiguiente, el Tribunal de Justicia **no necesita examinar si la medida impugnada tenía una finalidad legítima y era proporcionada***» (la negrita es nuestra).
Véanse también los asuntos *Rechnungshof (C-465/00) contra Österreichischer Rundfunk y otros y Christa Neukomm (C- 138/01) y Joseph Lauermann (C-139/01) contra Österreichischer Rundfunk*, ECLI:EU:C:2003:294, apartados 77-80; conclusiones del Abogado General en el Dictamen 1/15 del PNR Canadá, ECLI:EU:C:2017:592**,** apartados 191-192: «*Por lo que respecta a la conservación de los datos personales, es preciso señalar que la normativa en cuestión debe, entre otras cosas, seguir satisfaciendo criterios objetivos que establezcan una relación entre los datos personales que deben conservarsey el objetivo perseguido (véanse, en este sentido, las sentencias de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650,apartado 93, y de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros, C-203/15 y C-698/15,*

2. En segundo lugar, si la medida hubiera superado la prueba de la calidad del derecho de conformidad con el punto 1 anterior, deberá examinarse si se respeta la **esencia del derecho**, es decir, si el derecho queda **vacío** de hecho de su contenido básico y si la persona no puede ejercerlo. Si la esencia del derecho se viera afectada, la medida sería ilegal y no sería necesario seguir evaluando su compatibilidad con las normas previstas en el artículo 52, apartado 1, de la Carta[13].

3. En tercer lugar, deberá evaluarse si la medida cumple un **objetivo de interés general**. El objetivode interés general proporciona el **contexto** en el que se puede evaluar la necesidad de la medida.Como se explica en el Manual sobre la Necesidad, es importante identificar el objetivo de interésgeneral con suficiente detalle para poder evaluar si la medida es necesaria.

4. El siguiente paso consiste en evaluar la **necesidad** de una medida legislativa propuesta que conlleve el tratamiento de datos personales (evaluación de la necesidad)[14].

5. Si se cumple esta evaluación, se evaluará la **proporcionalidad** de la medida prevista (prueba de proporcionalidad). El concepto de proporcionalidad es un concepto jurídico bien desarrollado en la legislación de la UE. Es un **principio general del Derecho de la UE** que exige que *«el contenido y la forma de la acción de la Unión **no excedan de lo necesario para alcanzar los objetivos** de los*

---

*EU:C:2016:970, apartado 110). Por lo que se refiere a la utilización, por parte de una autoridad, de datos personales legítimamente conservados, cabe recordar que el Tribunal de Justicia ha declarado que la normativa de la UE no puede limitarse a exigir que el acceso a tales datos tenga por objeto uno de los objetivos perseguidos por dicha normativa, sino quedebe establecer también **las condiciones de fondo y de procedimiento que rigen dicha utilización** (véase, por analogía, la sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros, C-203/15 y C-698/15, EU:C:2016:970, apartados 117y 118, y la jurisprudencia citada)».*

[13] Aunque no abunda la jurisprudencia en cuanto a las condiciones en las que se ve afectada**la esencia** de un derecho, cabe afirmar que este sería el caso **si la limitación fuera tan lejos que se vacía el derecho de sus elementos esenciales** y, por tanto, se impide el ejercicio del derecho.

- En el asunto **C-362/14**, *Schrems*, ECLI:EU:C:2015:650, apartados 94 y 95, el TJUE consideró que **la esencia del derecho alrespeto de la vida privada y el derecho a un recurso** efectivo estaban afectados: «*la legislación que permite a las autoridadespúblicas acceder de forma generalizada al contenido de las comunicaciones electrónicas debe considerarse que comprometela esencia del derecho fundamental al respeto de la vida privada, garantizado por el artículo 7 de la Carta [...]. Asimismo, una legislación que **no prevea la posibilidad de que una persona interponga una acción judicial** para tener acceso a los datos personales que le conciernen, o para obtener su rectificación o supresión, **no respeta la esencia del derecho fundamental a la tutela judicial efectiva**, consagrado en el artículo 47 de la Carta*» (apartados 94 y 95) (la negrita es nuestra). El Tribunal no prosiguió con la evaluación de la necesidad de tal limitación, sino que **invalidó**, también por otros motivos, la **Decisión de la Comisión** sobre la adecuación de los principios de puerto seguro.

- En los asuntos acumulados **C-293/12 y C-594/12**, *Digital Rights*, ECLI:EU:C:2014:238, apartado 39, el TJUE consideró quela **esencia del derecho *al respeto de la vida privada* no se veía afectada**, ya que la Directiva de conservación de datos **no permitía conocer *el contenido de las comunicaciones electrónicas*** (sino solo los «metadatos»).
Asimismo, el TJUE consideró que la **esencia del derecho a la protección de los *datos personales*** no se veía afectada porquela Directiva de Conservación de Datos establece la **norma básica de que deben adoptarse medidas organizativas y técnicas adecuadas contra la destrucción, pérdida o alteración accidental o ilícita de los datos conservados** (apartados 39 y 40). Solo tras la apreciación de que la esencia del derecho fundamental en juego no se veía comprometida, el Tribunal de Justicia procedió a examinar **la necesidad** de la medida.

- En los asuntos acumulados **C-203/15 y C-698/15**, *Tele2 Sverige AB,* ECLI:EU:C:2016:970, apartado 123, el Tribunal estableció que la **privación de la revisión**, por parte de una autoridad independiente, del cumplimiento del nivel de proteccióngarantizado por el Derecho de la UE podría **afectar también a la esencia del derecho a la protección de los datos personales**,ya que así lo exige expresamente el artículo 8, apartado 3, de la Carta y «*Si no fuera así, las personas cuyos datos personalesfueran conservados se verían privadas del derecho, garantizado en el artículo 8, apartados 1 y 3, de la Carta, a presentar ante las autoridades nacionales de control una reclamación solicitando la protección de sus datos*».

[14] Para nuestro análisis de la **prueba de la necesidad**, véase el Manual sobre la necesidad del SEPD, disponible en: https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en.

tratados»[15] (la negrita es nuestra). Se «construye» sobre las tradiciones constitucionales de variosestados miembros[16].

Según el artículo 52, apartado 1, de la Carta, «*Sólo se podrán introducir limitaciones* [al ejercicio de los derechos fundamentales]*, respetando el principio de proporcionalidad, cuando sean necesarias* [...]». Según reiterada jurisprudencia del TJUE, «*el principio de proporcionalidad exige que los actos de las instituciones de la UE sean apropiados para alcanzar los objetivos legítimos perseguidos por la legislación de que se trate y no excedan los límites de lo que es apropiado y necesario para alcanzar dichos objetivos*»[17]. De ahí que la **proporcionalidad en sentido amplio** (tal como la denomina el TJUE)abarque **tanto la necesidad como la adecuación (proporcionalidad en sentido estricto)** de una medida, es decir, la medida en que existe un vínculo lógico entre la medida y el objetivo (legítimo) perseguido[18].

Para que una medida respete el principio de proporcionalidad consagrado en el artículo 52, apartado 1, de la Carta, **las ventajas resultantes de la medida no deben ser superadas por las desventajas** que la medida provoca con respecto al ejercicio de los derechos fundamentales. Por lo tanto, *«**restringea las autoridades** en el ejercicio de sus facultades al exigir **un equilibrio** entre los **medios** utilizados yel **objetivo previsto (o el resultado alcanzado)**»*[19].

De hecho, en la sentencia sobre *Derechos Digitales*[20], el TJUE ha dictaminado que el **poder discrecional del legislador** se reduce al restringir los derechos fundamentales: «*cuando se trata de injerencias en los derechos fundamentales, el alcance de la facultad de apreciación del legislador de la UE puede resultar limitado, en función de una serie de factores,* entre los que figuran, en particular, el ámbito afectado, el carácter del derecho en cuestión garantizado por la Carta, la naturaleza y la gravedad de la injerencia, así como la finalidad de ésta [21]». Respondiendo en esencia a la

---

15 Véase el artículo 5, apartado 4, del TUE.

16 El principio fue desarrollado; y (iii) proporcionalidad *stricto sensu*. Véase a este respecto: C. Bagger Tranberg, *Proportionality* por el TJUE en el asunto *Internationale Handelsgesellschaft*, **C-11/70,** ECLI:EU:C:1970:114. Al igual que en el derecho administrativo alemán, también en el ámbito de la UE, la prueba para establecer la necesidad y la proporcionalidad de una medida consta de tres pasos: (i) adecuación; (ii) necesidad*and data protection in the case law of the European Court of Justice*, International Data Privacy Law, 2011, Vol. 1, núm. 4, página 240.

17 Asunto C-62/14, *Gauweiler (OMT)*, ECLI:EU:C:2015:400, apartado 67. Véase también asunto C-331/88, *Fedesa y otros*, ECLI:EU:C:1990:391, apartado 13: *«En lo que respecta a la evaluación de la proporcionalidad, el principio de proporcionalidad,que es uno de los principios generales del derecho comunitario, exige que las medidas adoptadas por las instituciones comunitarias no sobrepasen los límites de lo que resulta apropiado y necesario para alcanzar los objetivos legítimamente perseguidos por la legislación en cuestión; cuando haya que elegir entre varias medidas apropiadas, deberá recurrirse a la menos gravosa, y los inconvenientes causados no deberán ser desproporcionados con respecto a los objetivos perseguidos*».

18 Como posible ejemplo de **proporcionalidad en sentido amplio**, que abarca tanto la evaluación de la necesidad como la dela proporcionalidad, véase asunto C-594/12, *Digital Rights*, donde la necesidad (apartado 65: «*De lo anterior se desprende que la Directiva 2006/24 no establece normas claras y precisas sobre el alcance de la injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta. Por consiguiente, debe considerarse que la Directiva 2006/24 supone una injerencia amplia y especialmente grave en dichos derechos fundamentales del ordenamiento jurídico de la UE, sin que tal injerencia esté precisamente delimitada por disposiciones que garanticen que se limita efectivamente a lo **estrictamente necesario***») y la proporcionalidad (apartado 69: *«Habida cuenta de todas las consideraciones anteriores, procede declarar que, al adoptar la Directiva 2006/24, el legislador de la Unión Europea ha rebasado los límites impuestos por el respeto del principio de **proporcionalidad** de conformidad con los artículos 7, 8 y 52, apartado 1, de la Carta»*) se abordan claramente por el TJUE. En otras palabras, el TJUE concluye sobre la proporcionalidad *tras* haber analizado la necesidad.

19 K. Lenaerts, P. Van Nuffel, *European Union Law*, Sweet y Maxwell, 3.ª edición, Londres, 2011, p. 141 (asunto C-343/09, *Afton Chemical*, apartado 45; asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke y Hartmut Eifert*, ECLI:EU:C:2010:662, apartado 74; asuntos C-581/10 y C-629/10, *Nelson y otros*, apartado 71; asunto C-283/11, *Sky Österreich*, apartado50; y asunto C-101/12, *Schaible*, apartado 29).

20 Asuntos acumulados C-293/12 y C-594/12, ECLI:EU:C:2014:238.

21 Asuntos acumulados C-293/12 y C-594/12, ECLI:EU:C:2014:238. apartado 47.

pregunta «¿Cuál es **el alcance de la discrecionalidad (reducida) del legislador de la UE**?», declaró el TJUE: «*La normativa de la Unión de que se trate **debe** establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión y establezcan unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos respecto de tales datos* »[22] (la negrita es nuestra).

Este último elemento (el equilibrio que debe alcanzarse) describe **la proporcionalidad *stricto sensu*** y constituye la prueba de proporcionalidad que es objeto de las presentes Directrices. Debe distinguirse claramente de la necesidad (véase la sección III), tanto desde un punto de vista conceptual como práctico.

2. Aclaraciones sobre **la relación** entre proporcionalidad y necesidad

Tal y como se establece en el Manual sobre la Necesidad, «***La necesidad implica que se requiere unaevaluación combinada, basada en hechos, sobre la eficacia de la medida para el objetivo perseguido y sobre si resulta menos intrusiva en comparación con otras opciones para lograr el mismo objetivo***». La evaluación de la necesidad debe considerarse como **el primer paso** que debe cumplir una medida propuesta que implique el tratamiento de datos personales. Si el proyecto de medida **no supera** la evaluación de la necesidad, **no será necesario** analizar su proporcionalidad. No deberá proponerse una medida que no se demuestre que es necesaria a menos que se hubiera modificado para cumplir el requisito de necesidad: en otras palabras, **la necesidad es una condición previa a la proporcionalidad**[23].

Así, las presentes Directrices se basan en el supuesto de que solo una medida que se demuestre que es necesaria debe evaluarse con arreglo a la evaluación de la proporcionalidad. Como se menciona en el Manual sobre la Necesidad, en algunos casos recientes, el TJUE no procedió a evaluar la proporcionalidad tras considerar que las limitaciones a los derechos de los artículos 7 y 8 de la Carta **no** eran estrictamente necesarias[24].

Sin embargo, una vez que se considera que una medida legislativa es **necesaria**, debe analizarse en función de su **proporcionalidad**. **Una evaluación de la proporcionalidad implica, por lo general, evaluar qué «salvaguardias» deben acompañar a una medida** (por ejemplo, sobre la vigilancia) para reducir

---

[22] Asuntos acumulados C-293/12 y C-594/12, ECLI:EU:C:2014:238, apartado 54.

- Véase también el **Dictamen 5/2015 del SEPD, Segundo Dictamen sobre la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave (***Opinion 5/2015 - Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime***)**, páginas 6-7: «*En el marco de la realización deuna **evaluación de proporcionalidad**, la **medida en que la facultad de apreciación del legislador de la UE puede resultar limitada** depende de una serie de factores, entre los que se encuentran, en particular: el ámbito de que se trate, la naturaleza de los derechos en cuestión, la naturaleza y la gravedad de la injerencia y el objeto perseguido por la misma. El Tribunal insistió en que estas limitaciones y salvaguardias son aún más importantes cuando los datos personales se someten a un tratamiento automatizado y cuando existe un riesgo significativo de acceso ilícito a los mismos*». El dictamen del SEPD está disponible en https://edps.europa.eu/sites/edp/files/publication/15-09-24_pnr_en.pdf.

[23] En los asuntos acumulados **C-465/00, C-138/01 y C-139/01**, *Rechnungshof*, ECLI:EU:C:2003:294, apartado 91, el TJUE sostuvo que «*Si los órganos jurisdiccionales nacionales llegan a la conclusión de que la legislación nacional controvertida es **incompatible** con el artículo 8 del Convenio, dicha legislación **tampoco puede cumplir el requisito de proporcionalidad*** previsto en los artículos 6, apartado 1, letra c), y apartado 7, letras c) o e), de la Directiva 95/46» (la negrita es nuestra).

[24] En los asuntos acumulados **C-293/12 y C-594/12**, *Digital Rights*, ECLI:EU:C:2014:238, el TJUE afirmó en primer lugar que la proporcionalidad está conformada por los pasos de adecuación y necesidad (apartado 46). A continuación, estableció que la limitación con los derechos protegidos en los artículos 7 y 8 de la Carta **no era necesaria** (apartado 65) y, por tanto, concluyó que las limitaciones no resultaban proporcionales (apartado 69).

- Del mismo modo, en el asunto **C-362/14**, *Schrems*, ECLI:EU:C:2015:650, apartados 92 y 93, el TJUE analizó la necesidad y consideró quela Decisión de puerto seguro no era válida, sin hacer **ninguna referencia a la proporcionalidad** antes de llegara esta conclusión (apartado 98).

los riesgos que plantea la medida prevista para los derechos y libertades fundamentales de las personasafectadas, a un nivel «aceptable» /proporcional.

Otro factor que debe tenerse en cuenta en la evaluación de la proporcionalidad de una medida propuestaes **la eficacia de las medidas existentes** por encima de la propuesta[25]. Si ya existen medidas para un propósito similar o idéntico, su eficacia debe evaluarse de forma sistemática como parte de la evaluación de la proporcionalidad. Sin esa evaluación de la eficacia de las medidas existentes que persiguen un objetivo similar o el mismo, no se puede considerar que se haya realizado debidamente la evaluación de la proporcionalidad de una nueva medida.

3. **Conclusión**: la proporcionalidad en la normativa de protección de datos. Un concepto «basado en hechos»que requiere una evaluación caso por caso por parte del legislador de la UE

La «aparición de un requisito de proporcionalidad» se ha considerado «**uno de los avances más sorprendentes** de la última década en la legislación europea sobre privacidad de datos»[26].

El principio de proporcionalidad se ha incorporado en el artículo 5, apartado 1, del **Convenio 108 modernizado**[27], que establece lo siguiente: «*El tratamiento de datos deberá ser* ***proporcional*** *en relación con la finalidad legítima perseguida y reflejar en todas las fases del tratamiento un* ***justo equilibrio*** *entre todos los intereses afectados, públicos o privados, y los derechos y libertades en juego*»(la negrita es nuestra).

En el núcleo de la noción de proporcionalidad subyace el concepto de un **ejercicio de una ponderación**:el balance de la **intensidad de la interferencia** frente a la **importancia** («legitimidad», utilizando la expresión de la jurisprudencia) del objetivo alcanzado **en el contexto dado**.

Una evaluación bien realizada requiere la identificación expresa, y la estructuración en un marco coherente, de los diferentes elementos de los que depende la ponderación, para que sea completa y precisa.

Por consiguiente, la **claridad de la medida** que restringe los derechos fundamentales a la privacidad y/o a la protección de datos es una condición previa para la identificación de la intensidad de la interferencia. Esta última, a su vez, es necesaria para verificar si el impacto sobre estos derechos fundamentales es «proporcional a la finalidad» (es decir, al objetivo perseguido por la legislación evaluada).

Tal y como afirma el TJUE, es fundamental señalar que la proporcionalidad es una valoración ***in concreto*** (caso por caso) :

«En virtud del principio de ***proporcionalidad****, incumbe al órgano jurisdiccional remitente tomar en consideración* ***todas las circunstancias del asunto del que conoce****, en particular, la duración de la infracción de las normas que desarrollan la Directiva 95/46, así como la importancia, para los afectados, de la tutela de los datos difundidos.»*[28] (la negrita es nuestra).

---

25 Véase WP29, Dictamen 01/2014 sobre la aplicación de los conceptos de necesidad y proporcionalidad y la protección dedatos en el sector de los organismos con funciones coercitivas, 27 de febrero de 2014, página 9, disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf.

26 Lee A. Bygrave, *Data Privacy Law. An International Perspective*, Oxford University Press, 2014, página 147.

27 Consejo de Europa, **Convenio modernizado para la protección de las personas con respecto al tratamiento automatizado de datos personales,** texto consolidado, disponible (en inglés) en: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000016807c65bf.

28 TJUE, asunto C-101/01, *Linqvist*, ECLI:EU:C:2003:596, apartado 89.

En otras palabras, el análisis de la proporcionalidad es siempre **contextual**[29]: como se explica con másdetalle en las presentes Directrices, este análisis no puede tener lugar sin identificar en primer lugar el contexto de la medida que se examina (por ejemplo, *¿Comparte el responsable del tratamiento la información sobre la persona en cuestión o proporciona acceso a ella? ¿Con quién y con qué fin?*).

La parte dispositiva de las Directrices ofrece orientación al respecto. Al igual que la metodología de evaluación del impacto de la Comisión en lo que respecta a las cuestiones de protección de datos, las directrices sobre la proporcionalidad tienen como objetivo esencial **ayudar al legislador a plantear el conjunto de preguntas adecuadas**, teniendo en cuenta las cuestiones más relevantes y recurrentes en materia de protección de datos. La siguiente lista de comprobación de las presentes Directrices (una herramienta analítica de cuatro pasos) también tiene como objetivo estimular el razonamiento pragmático, lo que permite alcanzar políticas innovadoras *ex ante* y ayuda en el seguimiento y la evaluación *ex post* de las medidas.

III. Lista de control para evaluar la proporcionalidad de nuevas medidaslegislativas

1. Descripción general del flujo de trabajo

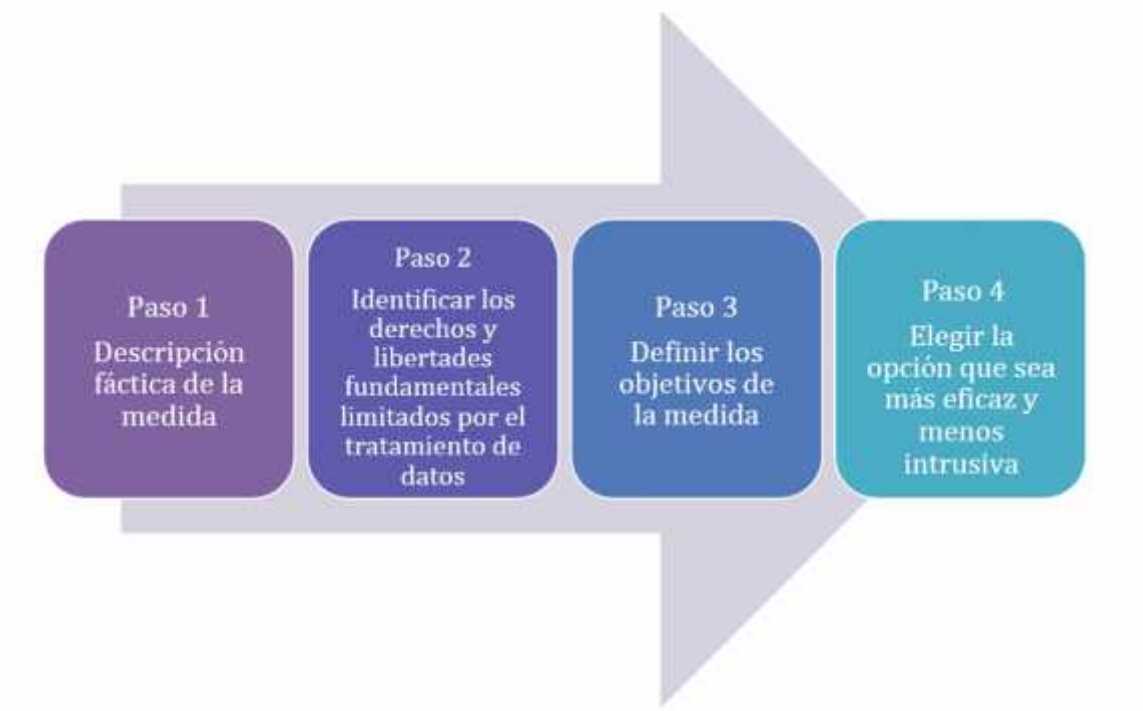
La evaluación global de la necesidad y la proporcionalidad **(visión sinóptica**) es la siguiente:

Prueba 1: en lo que respecta a la necesidad (evaluación de la necesidad), los pasos recomendados enel Manual sobre la Necesidad de necesidad son[30]:

- El **paso 1** es preliminar: requiere **una descripción fáctica detallada** de la medida propuesta yde su finalidad, antes de cualquier evaluación.
- El **paso 2** ayudará a identificar si la medida propuesta representa **una limitación** de los derechos a la protección de datos personales o al respeto de la vida privada (también llamado derecho a la intimidad), y posiblemente también de otros derechos.
- El **paso 3** considera el **objetivo de la medida** con respecto al cual debe evaluarse la necesidadde una medida.
- El **paso 4** orienta **sobre los aspectos específicos que deben abordarse** al realizar la evaluaciónde la necesidad, en particular que la medida debe ser **eficaz** y **lo menos intrusiva posible.**

29 Véase, por ejemplo, TEDH, *M.K. c. Francia,* apartado 46: «*El Tribunal considera que el Estado demandado* ***se ha extralimitadoen su margen de apreciación en este asunto****, ya que la normativa sobre la conservación en la base de datos impugnada de las huellas dactilares de las personas sospechosas de haber cometido delitos pero no condenadas,* ***tal como se aplica a la demandante en el presente caso****, no establece un justo equilibrio entre los intereses públicos y privados en juego. Por consiguiente, la conservación de los datos debe considerarse una* ***injerencia desproporcionada*** *en el derecho del demandanteal respeto de su vida privada y no puede considerarse necesaria en una sociedad democrática*» (la negrita es nuestra).

30 Véase la página 9 del Manual sobre la Necesidad del SEPD.



Si la evaluación de la medida lleva a la conclusión de que una medida cumple el requisito de necesidad**(prueba 1**), dicha medida podrá evaluarse siguiendo los siguientes pasos de la evaluación de la proporcionalidad **(prueba 2**).

En otras palabras, en el marco de la **prueba 2** reconsideraremos la medida evaluada como necesaria (loque significa que se trata de la medida efectiva menos intrusiva disponible para alcanzar el objetivo perseguido) y evaluaremos si la limitación (interferencia) que provoca es proporcional al objetivo quese pretende alcanzar.

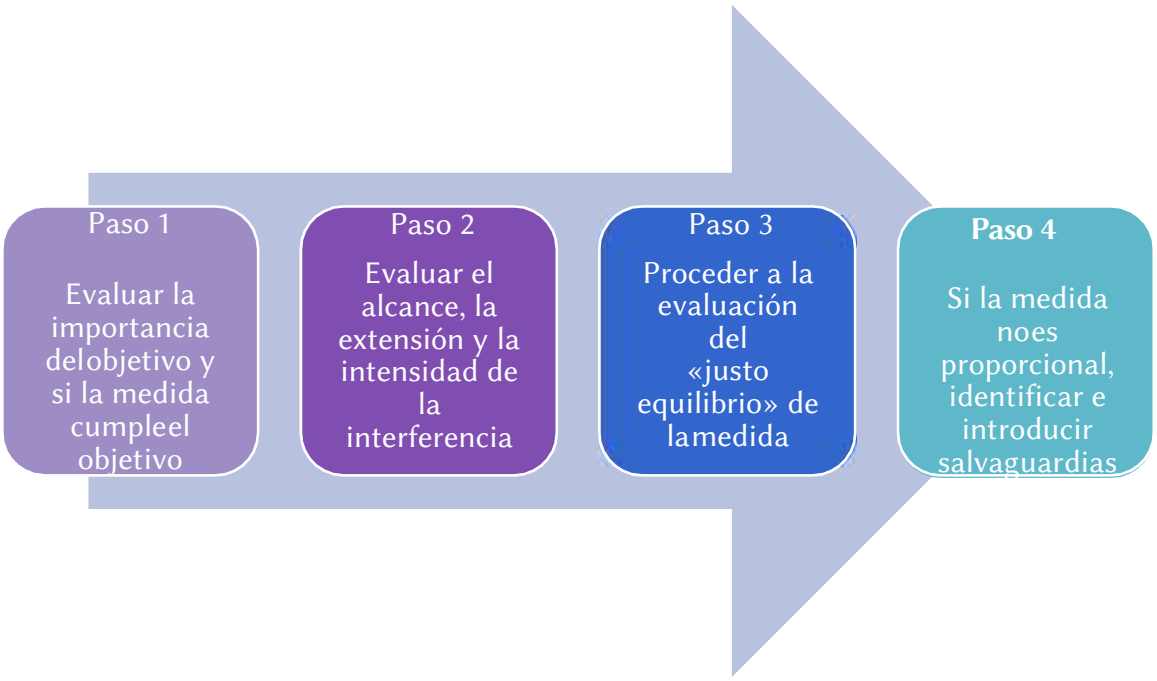
Prueba 2: en lo que respecta a la proporcionalidad (prueba de proporcionalidad), los pasos son:

- **Paso 1** (o 5 del flujo de trabajo global combinado): evaluar **la importancia** («**legitimidad**») **del objetivo** (identificado en el paso 3 de las Herramientas de Necesidad) y **si** la medida propuesta cumpliría este objetivo y aborda la cuestión identificada en la definición del problema(«cumple **realmente**») **y en qué medida** [esto sería «la ventaja/beneficio»].

- **Paso 2** (o 6 del flujo de trabajo global combinado): evaluar **el alcance, la extensión y la intensidad** de la interferencia (identificada en el paso 2 del Manual sobre la Necesidad) en términos de **impacto** sobre los derechos fundamentales a la privacidad y a la protección de datos [esto sería «la desventaja/el coste»].

- **Paso 3** (o 7 del flujo de trabajo global combinado): proceder a la **evaluación del equilibrio justo (*ventaja/desventaja*; *beneficio/coste*)** de la medida.

- **Paso 4** (u 8 del flujo de trabajo global combinado): **tomar una decisión («sí/no») sobre la medida**. Si el resultado es «no», teniendo en cuenta todos los factores que determinaron la evaluación como desproporcionada, identificarán e introducirán (si fuera posible) salvaguardias que puedan hacer que la medida sea proporcional.



2. Descripción de las etapas de la evaluación de la proporcionalidad

Paso 1: evaluar la importancia («legitimidad») del objetivo y si la medida propuesta cumpliría este objetivo y en qué medida (eficacia y eficiencia)

Una descripción detallada de la **finalidad** de la medida prevista no solo es un **requisito previo** para la evaluación de la proporcionalidad, sino que también ayuda a demostrar el cumplimiento del primer requisito del artículo 52, apartado 1, de la Carta, es decir, *la calidad de la ley*[31].

[31] Como se indica en las conclusiones del Abogado General Mengozzi, ECLI:EU:C:2016:656, apartado 193 sobre el proyecto de Acuerdo entre Canadá y la Unión Europea sobre la transferencia y el tratamiento de datos del registro de nombres de los pasajeros: «*Según la jurisprudencia del TEDH, dicha expresión exige, en lo sustancial, que la medida en cuestión sea* ***accesible*** *y* ***suficientemente previsible, est****o es, dicho de otro modo, que utilice términos lo bastante claros para indicar a todos de forma suficiente en qué circunstancias y en qué condiciones habilita a los poderes públicos a recurrir a medidas que afecten a sus derechos protegidos por el CEDH.*» (la negrita es nuestra).

- En los asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB*, el Abogado General Saugmandsgaard Øe profundiza en sus conclusiones, ECLI:EU:C:2016:572, apartados 139-140, que: «*Según dicha jurisprudencia, la expresión "prevista por la ley" implica que la base legal sea suficientemente accesible y previsible, es decir,* ***que se enuncie con la suficiente precisión como para permitir al individuo, buscando si es preciso asesoramiento jurídico adecuado, que ajuste su conducta a Derecho****. Dicha base legal debeasimismo proporcionar una protección adecuada frente a la arbitrariedad y, en consecuencia, definir con la suficiente nitidez la amplitud y los modos de ejercer la facultad conferida a las autoridades competentes (principio de la primacía del Derecho). […] Pues bien, considero necesario, por las razones que expondré seguidamente, que se atribuya a la expresión «prevista por la ley» utilizada en el artículo 52, apartado 1, de la Carta un alcance similar al que dicha expresión tiene en el contexto del CEDH.*».
A este respecto, véase también TEDH, *Catt c. Reino Unido*, 24 de enero de 2019, apartado 6 del voto concurrente del juez Koskelo al cual se sumó el juez Felici: «***los principios generales de la ley de protección de datos****, como los que exigen*

En la práctica, si la ley no **define de forma clara y específica el objetivo** en juego, es imposible realizaruna evaluación *ex ante* de la importancia del objetivo y de la eficacia de la medida para alcanzarlo.

Es importante tener en cuenta que tanto la **medida** como sus **objetivos** deberían haberse **identificado** ya en los pasos 1 y 3 de la evaluación de la necesidad (prueba 1). En este paso, volveremos a plantear estos objetivos para establecer, aún *ex ante* pero en esta ocasión *in concreto*, su **importancia** y en qué medida se **cumplirán de forma efectiva** con la medida.

> En referencia a la terminología utilizada por la evaluación de impacto de la Comisión, lo que se plantea aquí es la eficacia *(¿La medida propuesta es la más adecuada para alcanzar los objetivos?*)y la eficiencia *(rentabilidad*) de la medida (la opción política identificada) para cumplir el objetivo(es decir, para **resolver las cuestiones identificadas en la Definición del Problema**).

Las medidas deben responder **a las necesidades** (es decir, a los objetivos de interés general reconocidospor la Unión Europea o a la necesidad de proteger los derechos y libertades de los demás) **claramenteidentificadas en el Análisis del Problema**. Tal y como afirma el TJUE, la **medida**, para ser proporcional, debe «cumplir realmente» el **objetivo**[32]. Asimismo, el objetivo debe reflejar las necesidades señaladas en el análisis del problema.

A la hora de evaluar la eficacia de la medida, el legislador siempre debe comprobar en primer lugar la eficacia de las **medidas ya existentes**[33]. En otras palabras, antes de proponer y adoptar nuevas medidas,el legislador debe considerar si la «medida existente» se **aplica** en

---

que los datos que se van a tratar deben ser adecuados, pertinentes y no excesivos en relación con dicha finalidad, ***se diluyen, posiblemente hasta el punto de resultar irrelevantes en la práctica, cuando la propia finalidad queda sin ninguna definición o limitación significativa*****».** (la negrita es nuestra).

[32] En los asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB,* ECLI:EU:C:2016:970, apartado 94: «*Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones al ejercicio de esos derechos y libertades cuando sean necesarias y* ***respondan efectivamente*** *a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.*» (la negrita es nuestra).

[33] En el Dictamen 01/2014 sobre la aplicación de los conceptos de necesidad y proporcionalidad y la protección de datos en elsector de los organismos con funciones coercitivas (disponible en https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf), el WP29 afirma: « *cualquiera que sea la manera en que se lleve a cabo esta evaluación, debería explicarse con pruebas por qué las medidas existentes ya no son suficientes para satisfacer esta necesidad.*».

En el **Dictamen 06/2016 sobre el segundo paquete de fronteras inteligentes de la UE**, 21 de septiembre de 2016 (página 3)(disponible en:https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_en.pdf), el SEPD señaló que «*La necesidad y proporcionalidad del SES* [el Sistema de Entradas y Salidas] *deben evaluarse tanto de forma general, teniendo* ***en cuenta los sistemas informáticos a gran escala que ya existen en la UE****, como de forma específica, en el caso concreto de aquellos nacionales de terceros países que visitan legalmente la UE.*».

- En el **Dictamen 3/2017 sobre la Propuesta de Sistema Europeo de Información y Autorización de Viajes (SEIAV)**, 6 de marzo de 2017 (disponible en: https://edps.europa.eu/sites/edp/files/publication/17-03-070_etias_opinion_en.pdf), el SEPD lo ha declarado claramente (página 8): «*Una evaluación del impacto del SEIAV sobre la privacidad y la protección de datos debería hacer un* ***balance de todas las medidas adoptadas a nivel de la UE para los objetivos de migración y seguridad y analizar en profundidad su aplicación concreta, su eficacia y su impacto sobre los derechos fundamentales de las personas antes de crear nuevos sistemas que impliquen el tratamiento de datos personales****. Este análisis también debe tener en cuenta el ámbito político en el que se aplican estas medidas y el papel respectivo de los principales agentes implicados*».

- Véase el **Dictamen 5/2015 del SEPD sobre la propuesta de Directiva relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves,** (página 15): «*La propuesta no proporciona una evaluación exhaustiva de la capacidad de los instrumentos existentes actualespara lograr la finalidad del sistema PNR de la UE*».

la práctica, y si la **ampliación y/o la profundización** de esta medida ya resolvería satisfactoriamente el problema identificado en el Análisis del Problema. Sin una evaluación sistemática de la eficacia de las medidas existentes que persiguen un objetivo similar o el mismo, no se puede considerar que la evaluación de la proporcionalidad de una nueva medida se haya realizado de forma debida. En el caso de una medida preexistente, la eficacia debe considerarse, durante el ejercicio de la ponderación, no entérminos absolutos sino en términos de **valor añadido** de la medida.

Orientación (cómo proceder)

- **Las necesidades** deben estar suficientemente descritas en el análisis del problema para permitiruna clara comprensión de *lo que* motivó exactamente la iniciativa de una propuesta legislativa.El legislador debe disponer de información completa y precisa sobre los **problemas que hay que resolver** (los **Elementos Subyacentes** del problema) y sobre las opciones disponibles.

- En particular, en lo que respecta al problema que debe abordarse **(Definición del Problema**), el legislador debe ser consciente del **nivel de urgencia del interés público** (por ejemplo, la seguridad pública) que debe abordarse y **referirse claramente al mismo** en la medida (especificando, por ejemplo, que la medida está destinada a abordar una amenaza temporal de alto nivel). Esto podría reducirse a la siguiente pregunta: «¿Estamos en presencia de una *necesidad social apremiante* para restringir el derecho (a la intimidad y/o a la protección de datos)?»[34].

- La referencia al **nivel de amenaza**, como se ha mencionado anteriormente, y el seguimiento/actualización de este elemento subyacente permite al legislador levantar la medidade restricción de los derechos a la intimidad y a la protección de los datos personales una vez que este nivel disminuya. También es clave contar un sistema de supervisión independiente, para evitar que la medida temporal se convierta en permanente.

- Es importante verificar si el **objetivo concreto** de la medida **refleja** estas necesidades. Esto podría reducirse a la siguiente pregunta: «¿Corresponde la finalidad prevista a esta necesidad?»[utilizando la terminología de la Evaluación del Impacto, «*¿La medida resuelve el Problema teniendo en cuenta su impacto/sus consecuencias*?»] La respuesta afirmativa a esta pregunta evitaría la extralimitación de la función legislativa (es decir, una medida que no aborda realmente el problema[35] sino un propósito diferente).

---

[34] Por ejemplo, véase la sentencia del TEDH en el asunto *Weber y Saravia contra Alemania*, apartado 112: «*En opinión del demandante, estos amplios poderes de control* ***no se correspondían con una necesidad apremiante*** *de la sociedad de dicha vigilancia. Ya no existe la amenaza de un ataque armado contra la República Federal de Alemania por parte de un Estado extranjero que posea armas nucleares, como había ocurrido durante la Guerra Fría. Tampoco había ningún otro peligro actualcomparable que pudiera evitarse. En particular, el tráfico de drogas, la falsificación de dinero y el blanqueo de capitales o lospresuntos peligros derivados de la delincuencia organizada no constituían un peligro para la seguridad pública suficiente parajustificar una injerencia tan intensa en las telecomunicaciones de los particulares. El hecho de que la interceptación se limitaraa los contenidos de "relevancia para el servicio de inteligencia*" ("*nachrichtendienstliche Relevanz"), como consecuencia de la decisión del Tribunal Constitucional Federal, no era suficiente para limitar de forma efectiva los poderes de control del Servicio Federal de Inteligencia*» (la negrita es nuestra).
Sobre la necesidad social apremiante, véase la aclaración realizada por el **Dictamen 01/2014 del WP29 sobre la aplicación de losconceptos de necesidad y proporcionalidad y la protección de datos en el sector de los organismos con funciones coercitivas**, WP211, 27 de febrero de 2014,páginas 7 y 8. Véase también la lista de factores a tener en cuenta, señalada en las páginas 9-11. El dictamen está disponibleen: https://ec.europa.eu/justice/article-29/documentation/opinion- recommendation/files/2014/wp211_en.pdf.

[35] Véase el documento «***Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice***» (Documento de reflexión sobre la interoperabilidad de los sistemas de información en el espacio de libertad,seguridad y justicia), 17 de noviembre de 2017 (disponible en:

- Verificar que el **propósito (**el **objetivo)** consagrado en la propuesta de legislación está en consonancia con la **necesidad de regulación pública/social** que se abordará (el daño al que puede estar expuesta la sociedad en ausencia de la medida, por ejemplo, la delincuencia comúngeneralizada o los delitos específicos de guante blanco).

Recordamos que, según la evaluación del impacto de la Comisión, los **objetivos** deben ser «**SMART»**, siglas en inglés que corresponden a: **específicos** (lo suficientemente precisos y concretos); **medibles** (definir un estado futuro deseado en términos medibles, por ejemplo, disminución de los delitos estimada en un ...%); **alcanzables**; **realistas**; y **delimitados en el tiempo** (relacionados con una fecha o periodo de tiempo fijo en el que deben lograrse losresultados). Estos requisitos, que son comunes a la metodología de mejora de la legislación,son especialmente importantes, como demostrarán los ejemplos, en caso de que la legislación restrinja o afecte de otro modo a la protección de los datos personales.

- Evaluar la **importancia** del objetivo (¿se trata de proteger un valor constitucional o un derechofundamental?[36]).

- Evaluar la **eficacia y la eficiencia** de la medida para cumplir el objetivo mencionado.

---

https://edps.europa.eu/sites/edp/files/publication/17-11-6_opinion_interoperability_en.pdf), donde el SEPD observó que la Comisión «*también debería establecer claramente **para qué fines específicos** se tratarían las categorías de datos personales enel contexto de sus futuras iniciativas sobre interoperabilidad. Esto permitirá un debate adecuado sobre la interoperabilidad desde la perspectiva de los derechos fundament*ales». (página 3).

De forma similar, véase el **Dictamen 4/2018 del SEPD sobre las propuestas de dos Reglamentos por los que se estableceun marco de interoperabilidad entre los sistemas de información a gran escala de la UE**, 16 de abril de 2018, disponible en https://edps.europa.eu/sites/edp/files/publication/2018-04-16_interoperability_opinion_en.pdf.

«*41. El SEPD subraya que "combatir la migración irregular y garantizar un nivel elevado de seguridad" es una descripción muy amplia de los fines (por otro lado, legítimos)* [página 12]. *Señala que el artículo 20 exige la adopción de una ley nacionalque los defina con más detalle. Sin embargo, le gustaría recordar que el Tribunal de Justicia de la Unión Europea ("TJUE"), en su sentencia sobre los derechos digitales en Irlanda (apartado 61), sostuvo que la Directiva 2006/24 no establecía* "ningún criterio objetivo para determinar los límites del acceso de las autoridades nacionales competentes a los datos y su posterior utilización con fines de prevención, detección o persecución penal de los delitos", *al limitarse a referirse* "de manera generala la delincuencia grave, tal como la define cada estado miembro en su legislación nacional*". El Tribunal también consideró que la finalidad del acceso y la utilización de los datos no se* "limitaba estrictamente al propósito de prevenir y detectar delitosgraves definidos con precisión o de llevar a cabo acciones penales relacionadas con los mismos*".*

*42. **El SEPD considera que los fines de la lucha contra la migración irregular y la contribución a un nivel elevado de seguridad en el contexto del artículo 20 son demasiado amplios y no cumplen los requisitos de estar "estrictamente restringidos" y "definidos con precisión" en las propuestas, como exige el Tribunal. Por consiguiente, recomienda definirlos mejor en las propuestas**. Por ejemplo, la "migración irregular" podría referirse a las condiciones de entrada y estancia establecidas en el artículo 6 del Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo. Por lo que respectaa la seguridad, el SEPD recomienda centrarse en las infracciones penales que puedan amenazar especialmente un alto nivel deseguridad; por ejemplo, haciendo referencia a los delitos enumerados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI si son punibles con arreglo a la legislación nacional con una pena privativa de libertad o una orden de detenciónpor un período máximo de al menos tres años*».

36 Para una **visión general de los derechos, libertades y principios garantizados por la Carta**, véase el anexo II, página 28,del documento de trabajo de los servicios de la Comisión «Directrices operativas para tener en cuenta los derechos fundamentales en las evaluaciones de impacto de la Comisión», SEC (2011) 567 final.

Ejemplos relevantes

Como ilustración de esta **metodología**, en particular, **deconstruimos** en los cuatro recuadros grises queofrecen ejemplos para cada uno de los cuatro pasos las sentencias del TJUE en los asuntos *Tele2* y *Ministerio Fiscal,* las Conclusiones del Abogado General y el Dictamen 1/15 del TJUE en el caso del Registrode Nombres de Pasajeros UE-Canadá (en lo sucesivo, «el PNR») y la sentencia del TJUE en el asunto *Bevándorlási és Állampolgársági Hivatal.*

EJEMPLO 1: Tele2 Sverige AB (TJUE, C-203/15, ECLI:EU:C:2016:970)

El Tribunal **describió los objetivos** de la medida examinada (en breve, una obligación relativa a la conservaciónde los datos de tráfico y de localización) de la siguiente manera: «El a*rtículo 15, apartado 1, primera frase, de la Directiva 2002/58 establece que los* ***objetivos*** *perseguidos por las medidas legislativas que contempla, que suponen una excepción al principio de confidencialidad de las comunicaciones y de los datos de tráfico correspondientes, deben ser para «proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas », o uno de los otros objetivos especificados en* ***el artículo 13, apartado 1*** *, de la Directiva 95/46, al que se refiere la primera frase del artículo 15, apartado 1, de la Directiva 2002/58 (...). Esta* ***lista de objetivos es exhaustiva****, como se desprende del artículo 15, apartado 1, segunda frase, de la Directiva 2002/58, que establece que las medidas legislativas deben estar justificadas por*

«los motivos previstos» en el artículo 15, apartado 1, primera frase, de dicha Directiva. En consecuencia, los estados miembros ***no pueden adoptar tales medidas para fines distintos de los*** *enumerados en esta última disposición*» (la negrita es nuestra).Si bien la **importancia** del objetivo (la protección de la seguridad pública y la aplicación del derecho penal) es evidente en este caso, el Tribunal también reconoció que la medida aumentaría las posibilidades de utilizar técnicas modernas de investigación y, por tanto, «*la* ***eficacia*** *de la lucha contra la delincuencia grave, especialmente la delincuencia organizada y el terrorismo*» (la negrita es nuestra).

EJEMPLO 2: Ministerio Fiscal (TJUE, C-207/16, ECLI:EU:C:2018:788)

Teniendo en cuenta la importancia del objetivo, el Tribunal reconoció que el objetivo de la medida se limita a «prevenir, investigar, descubrir y perseguir ”delitos” en general» (en este caso, el robo de una cartera y un teléfono móvil), en contraposición a un «delito grave». Por lo tanto, se puede argumentar que el Tribunal consideró la «magnitud» de la importancia del objetivo como relativamente menor.

Sobre la **eficacia de la medida** para perseguir el citado objetivo, el Tribunal señaló que, a través de la medida examinada, «la Policía Judicial solicita, a efectos de la investigación de un delito, autorización judicial*para* ***acceder a los datos personales conservados por los proveedores de servicios de comunicaciones electrónicas****, (..)* ***para identificar a los titulares de las***

tarjetas SIM activadas durante un período de 12 días con el código IMEI del teléfono móvil sustraído». «*Los datos a que se refiere la solicitud de acceso controvertida en el litigio principal (...)* ***permiten vincular, durante un período determinado, la tarjeta o tarjetas SIM activadas con el teléfono móvil sustraído,*** los datos personales o de filiación de los titulares de estas tarjetas SIM***).*** *Por consiguiente, es evidente que la medida sería* ***eficaz*** *para rastrear, en su caso, al ladrón o al comprador del teléfono (en caso de que decidiera hacer uso del mismo, instalando una tarjeta SIM) y permitir así identificar, deforma directa o indirecta a través de investigaciones posteriores y así habilitadas, al autor del delito» (la negrita es nuestra).*

EJEMPLO 3: «PNR UE-Canadá» (Conclusiones del Abogado General, ECLI:EU:C:2016:656 y TJUE, Dictamen 1/15, ECLI:EU:C:2017:592)

El Abogado General Mengozzi, en el apartado 205 de sus conclusiones, reconoció tanto la **importancia del objetivo** como **la eficacia** de la medida para alcanzarlo: «*no pienso que existan verdaderos obstáculos para reconocer que la injerencia que implica el acuerdo* previsto **sea apta para lograr el objetivo de seguridad pública**, en particular de lucha contra el terrorismo y los delitos graves de carácter transnacional, perseguido por éste..

En efecto, como han alegado principalmente el Gobierno del Reino Unido y la Comisión, la transmisión de los datos del PNR con el fin de analizarlos y conservarlos permite a las autoridades canadienses disponer de posibilidades adicionales de identificación de pasajeros hasta ese momento desconocidos y no sospechosos que podrían tener vínculos con otras personas y/o pasajeros implicados en una red terrorista o que participen en actividades delictivas graves de carácter transnacional. *Esos datos,* ***como ponen de manifiesto*** *las estadísticas comunicadas por el Gobierno del Reino Unido y la Comisión en relación con la práctica anterior de las autoridades canadienses, constituyen* ***herramientas útiles*** *para las investigaciones penales, que pueden asimismo favorecer, en particular desde el punto de vista de la cooperación policial instaurada por el acuerdo previsto, la prevención y la detección de un delito de terrorismo o un delito grave de carácter transnacional dentro del territorio de la Unión » (la negrita es nuestra).*

El Tribunal tuvo en cuenta las **medidas ya existentes** y concluyó que los datos ya disponibles «***no son suficientes*** *para alcanzar una eficacia comparable a las establecidas por el acuerdo previsto, con el fin de realizar el objetivo de seguridad pública perseguido por éste »*(la negrita es nuestra).

EJEMPLO 4: Bevándorlási és Állampolgársági Hivatal (TJUE, C-473/16, ECLI:EU:C:2018:36)

En este caso, la medida que se analiza es la recogida y el tratamiento del **informe de un psicólogo** sobre la orientación sexual de una persona que solicita el estatuto de refugiado en virtud de la Directiva 2011/95. El Tribunal reconoció que **el objetivo** de la medida es «*permitir la búsqueda de información que permita evaluar su necesidad real de protección internacional*».

El Tribunal también observó que «***el carácter adecuado*** *de un examen como el que es objeto del litigio principal sólo puede admitirse si ese examen se basa en métodos y principios suficientemente fiables según las normas admitidas por la comunidad científica internacional.*» (la negrita es nuestra).

No obstante, en lo que respecta a la **eficacia** de la medida para alcanzar el objetivo mencionado, el Tribunal observó que: «*un examen de tal tipo* ***no puede considerarse indispensable*** *para confirmar las declaraciones de un solicitante de protección internacional relativas a su orientación sexual con el fin de pronunciarse sobre una solicitud de protección internacional basada en el temor a ser perseguido por razón de dicha orientación.*» (la negrita es nuestra).

En particular, el Tribunal declaró que: «*cuando los Estados miembros aplican el principio según el cual corresponde al solicitante fundamentar su solicitud, las declaraciones de éste relativas a su orientación sexual que no estén avaladas por pruebas documentales o de otra naturaleza* ***no requieren ulterior confirmación en caso de que se cumplan los requisitos enunciados en esta disposición, que se refieren, en particular a la coherencia y la credibilidad de dichas declaraciones, y en ningún caso a la realización o utilización de un dictamen pericial****.»* (la negrita es nuestra).

«*Por otra parte, incluso suponiendo que un examen basado en tests de personalidad proyectivos, como el controvertido en el litigio principal,* ***pueda contribuir*** *a determinar con cierta fiabilidad la orientación sexual de la persona de que se trate, se desprende de las afirmaciones del órgano jurisdiccional remitente que* ***las conclusiones de tal examen sólo podrían ofrecer una imagen*** *de esta orientación sexual. Por lo tanto, dichas conclusiones tienen, en cualquier caso,* ***carácter aproximativo y tienen, por tanto, un interés limitado*** *en la valoración de las declaraciones del solicitante de protección internacional, en particular si, como ocurre en el litigio principal, estas declaraciones no adolecen de contradicción alguna »* (la negrita es nuestra).

EJEMPLO 5: Dictamen 3/2017 del SEPD sobre la propuesta de un Sistema Europeo de Información y Autorización de Viajes (SEIAV)

Es posible que el legislador también se refiera **al objetivo** de la medida como «**riesgo a evitar**». También en este caso, como destaca el SEPD, los riesgos deben definirse en la medida de lo posible. «El artículo 1 de la Propuesta menciona que el SEIAV tiene por objeto determinar si la presencia de un viajero exento de visado en el territorio de los estados miembros supone un **riesgo migratorio irregular, de seguridad y/o de salud pública**. El SEPD observa que la Propuesta **define el riesgo para la salud** pública refiriéndose a categorías específicas de enfermedades, pero **no define los riesgos para la seguridad y la migración irregular**» (la negrita es nuestra).

Paso 2: evaluar (el alcance, extensión e intensidad de) la interferencia en términos de impacto efectivo de la medida sobre los derechos fundamentales a la intimidad y a la protección de datos

La evaluación detallada de la interferencia de la medida prevista con los derechos fundamentales a la privacidad y a la protección de datos es el otro paso clave de la prueba de proporcionalidad.

Es importante señalar que **los derechos y libertades fundamentales limitados** por la medida ya se han**definido** en el paso 2 de la evaluación de la necesidad (prueba 1). En este paso, nos replanteamos estos derechos y libertades fundamentales para determinar, aún *ex ante*, pero *in concreto*, cómo se verían afectados. De hecho, como se menciona en el manual de la FRA «Aplicación de la Carta de los Derechos Fundamentales de la Unión Europea en la elaboración de normas y políticas de ámbito nacional», «*la medida no debe imponer una* ***carga desproporcionada y excesiva*** *a las personas afectadas por la limitación en relación con el objetivo perseguido*»[37].

Es importante señalar que el impacto puede ser **menor** en lo que respecta **a la persona** en cuestión y, sin embargo, **significativo o muy significativo** en lo que respecta a la **sociedad** en su conjunto **(impacto en las personas individuales** frente a **impacto en la sociedad en su conjunto)**[38].

Los **costes** de la medida que afecta a la privacidad, bajo esta perspectiva, están representados por las **externalidades** de la falta de protección de datos (la «contaminación de datos»). Algunos ejemplos hipotéticos de estas externalidades son: los daños al proceso electoral y político (uso indebido de los datos para la manipulación política)[39]; la elaboración de perfiles ilegales y la discriminación que provocan la desconfianza hacia las autoridades públicas; el «efecto amedrentador» sobre la libertad de expresión de unas medidas de vigilancia omnipresente[40]

---

[37] Manual de la FRA mencionado anteriormente, p. 76. Véase también TJUE, asunto C-258/14, *Eugenia Florescu y otros contra Casa Judeţeană de Pensii Sibiu y otros*, ECLI:EU:C:2017:448, apartado 58.

[38] Véase Omri Ben-Shahar, *Data Pollution*, Universidad de Chicago, junio de 2018, disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3191231 Véase la página 3: «*El paradigma de la privacidad se basa en la premisa de que el daño producido por la empresa de datos personales es de naturaleza privada, al "núcleo del yo", aunque por mera agregación (o por canales más matizados) estos daños de naturaleza profundamente privada tienen un impacto social derivado*»; y la página 4: «*La bibliografía ha examinado todos los aspectos de los daños privados derivados de la recogidade datos, las posibles vulneraciones de la intimidad de las personas cuyos datos se recogen. Sin embargo, se ha descuidado por completo el* ***problema de la externalidad****: cómo la participación de las personas en los servicios de recogida de datos afecta a* ***los demás, y al público en general***».

[39] Véase el Dictamen del SEPD sobre la manipulación en línea, mencionado en la nota 42.
ICO, «*Democracy disrupted? Personal information and political influence*», 11 de julio de 2018, disponible en: https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf.
Comunicación conjunta al Parlamento Europeo, el Consejo Europeo, el Consejo, el Comité Económico y Social Europeo y elComité de las Regiones: «Plan de acción contra la desinformación» (JOIN (2018) 36 final), disponible en: https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de lasRegiones: «Garantizar unas elecciones europeas libres y justas», disponible en https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-free-fair-elections-communication- 637_en.pdf.

[40] En sus conclusiones, ECLI:EU:C:2013:845, en *Derechos Digitales*, el Abogado General Cruz Villalón se refirió a este preocupante efecto: «*no puede hacerse caso omiso de que el sentimiento difuso de vigilancia que la aplicación de la Directiva 2006/24 puede ocasionar puede ejercer una influencia decisiva en el ejercicio que los ciudadanos europeos hacen de su libertad de expresión e información, por lo que debe reconocerse también una injerencia en el derecho garantizado por el artículo11 de la Carta*» (apartado 52); «*La recopilación de estos datos crea las condiciones de una vigilancia que, aunque sólo se ejerce retrospectivamente en el momento de su explotación, amenaza no obstante de manera permanente, durante todo su período de conservación, el derecho de los ciudadanos de la Unión al secreto de su vida privada. El sentimiento difuso de vigilancia generado suscita de manera especialmente acusada la cuestión de la duración de conservación de los datos.*» (apartado 72).
El TJUE, confirmando el planteamiento del Abogado General, declaró, en el apartado 37 de la sentencia, que «*[...] la circunstancia de que la conservación de los datos y su posterior utilización se efectúen sin que el abonado o el usuario registrado hayan sido informados de ello puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante.*».

u otros efectos negativos sobre la libertad de las personas derivados de un sistema de elaboración de perfiles y de puntuación omnipresente y sistemáticamente aplicado[41].

Aunque sean difíciles de cuantificar en la práctica[42], estas externalidades deberán ser tomadas en cuentapor el legislador en su evaluación del «coste de la privacidad» de la medida.

En el caso de una medida de vigilancia propuesta, es importante evaluar **el nivel de intrusividad** del método de vigilancia. Para esta evaluación, debemos valorar las **dimensiones de la vigilancia.** La jurisprudencia pertinente del TEDH y del TJUE ha identificado las dimensiones de la vigilancia, empezando por la «dimensión sensorial» (por ejemplo, grabación de audio o vídeo)[43], hasta las posibilidades de analizar, combinar y comunicar la información. El **nivel de intromisión** en la vida privada de las personas a las que se dirige, así como la posible intromisión en la vida privada de **terceros**, debe ser evaluado cuidadosamente por las autoridades que deciden la medida.

El impacto en este paso también se relaciona con el posible **efecto perjudicial** de la medida sobre una **base más amplia que la de la protección de la privacidad**, conllevando así riesgos para otros derechos fundamentales. Esto está en consonancia con el enfoque adoptado por el RGPD que se refiereexplícitamente y en repetidas ocasiones a los «riesgos para los derechos y libertades de las personas físicas», destacando así el hecho de que un efecto perjudicial para el derecho a la intimidad está a menudo **inextricablemente vinculado** a la vulneración **otros derechos fundamentales**, como los derechos a la **libertad de expresión, la libre circulación, la libertad de asociación**[44] y respecto de los principios generales del derecho de la UE, como **el principio de «no discriminación»**[45]. En este sentido, estas Directrices adoptan un «enfoque de derechos fundamentales».

---

41 Véase, como ejemplo hipotético, H.J. Pandit, D. Lewis, *Ease and Ethics of User Profiling in Black Mirror*, 2018, disponible en https://dl.acm.org/citation.cfm?id=3191614 Véase, como modelo de evaluación de impacto, *Ethics Canvas*, página 1582.

42 Véase la página 31 de *Data Pollution,* mencionada en la nota 38: «*Las externalidades de los datos suelen ser cualitativas y conjeturales. ¿Cuál es la cifra del coste respecto de las elecciones presidenciales distorsionadas? ¿Respecto de los perfiles raciales discriminatorios?*»

43 En el asunto *Uzun contra Alemania*, el TEDH consideró que el uso de un dispositivo GPS para el seguimiento de la ubicación era una medida menos intrusiva que la interceptación de las comunicaciones personales.

- Sobre la **videovigilancia** (CCTV), véanse **las Directrices sobre videovigilancia del SEPD**, 17 de marzo de 2010,disponibles en https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf.

Orientación (cómo proceder)

El impacto debe estar lo suficientemente descrito para permitir una comprensión clara **del alcance, la extensión y el nivel de intrusión de la interferencia** en los derechos fundamentales a la privacidad y a la protección de datos personales. Es especialmente importante identificar con precisión:

- **el impacto**[46]**,** tomando en cuenta:

---

44 El SEPD ha abogado por un enfoque más amplio de la protección de datos que tenga en cuenta estas interfaces. Véase, en particular, el **Dictamen 3/2018 del SEPD sobre la manipulación en línea y los datos personales**, página 13: «*La privacidad y la protección de datos personales se sitúan entre las "libertades" de la UE, que incluyen la* ***libertad de pensamiento, conciencia y religión***, ***la libertad de expresión e información*** *y la* ***libertad de reunión y asociación*** *(artículos 10, 11 y 12).****También está claramente en juego*** *la capacidad de los principales intermediarios de las plataformas para facilitar o impedir la difusión dela información. Por ejemplo, los contenidos que no están indexados o clasificados en un lugar destacado en un motor de búsqueda de internet tienen menos probabilidades de llegar a una gran audiencia o directamente de ser encontrados. Por otra parte, un algoritmo de búsqueda también podría estar sesgado hacia ciertos tipos de contenidos o proveedores de contenidos, con lo que se corre el riesgo de afectar a valores relacionados como el pluralismo y la diversidad de los medios de comunicación*»; y página 5: «*La legislación de la UE sobre protección de datos y confidencialidad de las comunicaciones electrónicas se aplica a la recopilación de datos, la elaboración de perfiles y la microfocalización, y* ***si se aplica correctamentedebería ayudar a minimizar los daños*** *derivados de los intentos de manipulación de personas y grupos*». El dictamen está disponible en https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

45 Por ejemplo, el Comité Meijers, en sus «*Comments on the Proposal for a Regulation of the European Parliament and of theCouncil on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), 12 December 2017, COM (2017) 794*» (Comentarios sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE (cooperación policial y judicial, asilo y migración), de 12 de diciembre de 2017, COM(2017) 794), de 19 de febrero de 2018, señaló la intersección entre **la limitaciónde la privacidad** (recogida y tratamiento de datos personales relativos a un grupo/categoría de personas) **y la vulneración del principio de no discriminación**. Véase la página 3 de los comentarios: «*El objetivo explícito de la propuesta de facilitar los controles de identidad de los nacionales de terceros países por parte de la organización policial en el territorio de la UE, para comprobar si la información sobre la persona está almacenada en una o más de las bases de datos de la UE, aumentará la posibilidad de que los nacionales de terceros países (o los que se consideran nacionales de terceros países) sean parados para realizar controles de identidad.*». En este contexto, el Comité Meijers recuerda el asunto *Huber contra Alemania*, en el que el TJUEtrató la **diferencia de trato entre los nacionales y los ciudadanos de la UE que viven en Alemania** con respecto al **almacenamiento central y el uso múltiple de datos personales en una administración de extranjería, incluido el uso con fines policiales** (TJUE, *Huber contra Alemania,* C-524/06, 16 de diciembre de 2008, apartados 78-79).

46 El análisis del impacto al que se refieren estas Directrices tiene en cuenta la **vulneración** contextual **de la protección de datos y el riesgo de vulneración potencial, derivado de la medida legislativa objeto de evaluación, para las personas afectadas y para la sociedad en su conjunto**. Por consiguiente, es diferente (más amplio) que la noción de «**riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas**», a la que se refiere el artículo 24 del RGPD.
Otra diferencia con la **evaluación del impacto relativa a la protección de datos (EIPD)** de conformidad con el artículo 35 del RGPD es que en estas Directrices nos referimos a la evaluación del «nivel más abstracto» de la proporcionalidad de *la medidalegislativa* (y no de un *tipo de tratamiento* previsto por un responsable del tratamiento). En consecuencia, la proporcionalidadpodría considerarse como una «*EIPD sobre la ley*» (que debe realizarse en el contexto de la función consultiva sobre las medidas legislativas que afectan al derecho a la intimidad y a la protección de los datos personales).
No obstante, puede ser útil señalar que **muchos de los factores que son relevantes para realizar la EIPD también lo sonpara la evaluación de los costes de privacidad de una medida legislativa.**
Véase, en este sentido las **Directrices del WP29, actualmente CEPD, sobre la evaluación del impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679**, WP248, revisado y adoptado por última vez el 4 de octubre de 2017, disponible en: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.
En las páginas 9 a 11 se señalan los nueve factores siguientes (para establecer los riesgos elevados): (i) **Evaluación o puntuación**, incluidas la elaboración de perfiles y la predicción; (ii) **Toma de decisiones automatizada** con efecto jurídico significativo o similar; (iii) **Observación sistemática**; (iv) **Datos sensibles** o datos muy personales; (v) Tratamiento de datosa **gran escala**; (vi) **Asociación o combinación** de conjuntos de datos; (vii) Datos relativos a **interesados vulnerables**;
(viii) Uso innovador o aplicación de **nuevas soluciones tecnológicas u organizativas,** como la combinación del uso del reconocimiento facial y de huellas dactilares

- *el **alcance*** de la medida: ¿es suficientemente limitado? *Número de personas* afectadas; si plantea «*intrusiones **colaterales**»*, es decir, injerencias en la intimidad de personas distintas de los sujetos de la medida[47];

- *el **alcance**: ¿cómo se restringe el derecho? Cantidad de* información recogida; durante *cuánto tiempo; si la medida examinada requiere la recogida y el tratamiento de categorías especiales de datos*[48];

- *el **nivel de intrusión***, tomando en cuenta: *la naturaleza de la actividad* sometida a la medida (si afecta a actividades cubiertas por el deber de confidencialidad o no, la relación abogado-cliente; actividad médica); *el contexto*; si equivale a la ***elaboración de perfiles*** de las personas afectadas o no[49]; si

---

para mejorar el control del acceso físico, *etc*.; (ix) Cuando el propio tratamiento «**impida a los interesados ejercer underecho o utilizar un servicio o ejecutar un contrato**».

El anexo I de las Directrices ofrece ejemplos de marcos **específicos del sector,** por ejemplo, «***Data Protection ImpactAssessment Template for Smart Grid and Smart Metering systems***» (Modelo de informe de evaluación de impacto en la protección de datos para sistemas de redes inteligentes y de contadores inteligentes), disponible en http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf.

Véanse, en particular, las páginas 27-31 sobre la **identificación, la cuantificación (gravedad y probabilidad) y la evaluación** del «riesgo.

- Por último, véase el **proyecto de lista de la**(s) **autoridad(es) de control competente(s) en relación con las operaciones de tratamiento sujetas al requisito de una evaluación de impacto sobre la protección de datos (artículo 35, apartado 4, del RGPD),** disponible en https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

47 Véase *Big Brother Watch y otros c. Reino Unido*, TEDH, 13 de septiembre de 2018, apartado 2.43: «2.*43. La **intrusión colateral**es la obtención de cualquier información relativa a personas distintas del sujeto o sujetos de la investigación. La valoración dela intrusión colateral forma parte de las valoraciones sobre la proporcionalidad, y resulta cada vez más relevante a la hora de solicitar datos de tráfico o de uso de servicios. Las solicitudes deben incluir detalles sobre **la posible intrusión de las garantíasy la forma en que los periodos de tiempo solicitados repercuten sobre la intrusión de las garantías**. Cuando **no existen riesgos de intrusión colateral significativos**, como cuando se solicitan los datos de los abonados de la persona investigada, **debe señalarse la ausencia de intrusión colateral***» (la negrita es nuestra).

48 Véase TJUE, asuntos acumulados C-465/00, C-138/01 y C-139/01, *Rechnungshof*, ECLI:EU:C:2003:294 apartado 52: «*El Gobierno austriaco destaca, en particular, que, en el marco del control de proporcionalidad, se ha de tener en cuenta **la medida** en la que los datos afectan a la intimidad. Así, los datos relativos a **la intimidad de la persona, a la salud, a la vida familiar o a la sexualidad** deben protegerse más que los datos relativos a los ingresos y a los impuestos que, si bien revisten también un carácter personal, afectan en menor medida la identidad de la persona y son, por tanto, menos sensibles*» (la negrita es nuestra).

- Sobre el tratamiento de **datos sanitarios**, véase el **Dictamen 3/2017 del SEPD sobre la propuesta de un Sistema Europeo de Información y Autorización de Viajes (SEIAV)**, en la página 13: «*El SEPD duda de que el tratamiento de esta categoríade datos especialmente sensibles a tan gran escala y durante este período de tiempo cumpla las condiciones previstas en el artículo 52, apartado 1, de la Carta y, en consecuencia, se considere necesario y proporcionado. El SEPD cuestiona la pertinencia de la recogida y el tratamiento de los datos sobre la salud, tal como se prevé en la Propuesta, debido a la falta de fiabilidad de los mismos y a la necesidad de tratar dichos datos debido a la escasa relación entre los riesgos para la salud y los viajeros exentosde visado*».

- Recientemente se ha prestado especial atención a los riesgos de la Inteligencia Artificial aplicada al reconocimiento facial(y de las «emociones»). Véase el informe *AI Now Report 2018*, diciembre de 2018, disponible en: https://ainowinstitute.org/AI_Now_2018_Report.pdf.

- Sobre los **datos biométricos**, véase el **Dictamen 3/2012 del Grupo de Trabajo del Artículo 29 sobre la evolución de las tecnologías biométricas**, páginas 30-31, sobre los riesgos específicos que plantean los datos biométricos; y el **Dictamen 02/2012 del Grupo de Trabajo del Artículo 29 sobre el reconocimiento facial en los servicios en línea y móviles**, sección 5 (Riesgos específicos y recomendaciones).

49 En este contexto, nos referimos al término «elaboración de perfiles» en sentido amplio, como «establecer un perfil del individuo», como se menciona en el asunto *Tele2*, y no necesariamente a la definición del artículo 4, apartado 4, del RGPD:
«*"Elaboración de perfiles": toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física*».

el tratamiento implica el uso de un sistema de toma de decisiones (parcial ototalmente) ***automatizado*** con un «margen de error»[50];

- independientemente de que se trate o no de *personas* ***vulnerables***[51];

- si **también afecta a *otros derechos fundamentales*** (podría haber un derecho fundamental «inextricablemente vinculado»[52], por ejemplo, el derecho a la protección de la intimidad y el derecho a la libertad de expresión, como en los asuntos *Digital Rights*y *Tele2* del TJUE).

En los casos en los que no se pueda determinar de antemano alguno o parte de del impacto, podría serútil aplicar el llamado **principio de precaución**[53]. Como ejemplo de la aplicabilidad de este principio, se podría sugerir al legislador, en función de todas las circunstancias pertinentes del caso, que adopte un «enfoque incremental», optando por el uso de una
herramienta informática ya *experimentada y testada* en lugar de una herramienta informática cuya eficacia (falsos negativos, falsospositivos) aún no se habría comprobado plenamente.

---

[50] Véase, teniendo en cuenta la automatización de las decisiones, el Dictamen 1/15, ECLI:EU:C:2017:592, del TJUE relativo a la propuesta de acuerdo de intercambio de datos PNR entre la UE y Canadá. El dictamen del Tribunal destacó que el sistemacanadiense de evaluación del riesgo de los viajeros de la UE funcionaba de forma sistemática y automatizada, y **con un margende error «significativo»** que exponía a un gran número de personas que no suponían ningún riesgo al escrutinio continuo de la CBSA y otros organismos. El dictamen subrayaba que los sistemas algorítmicos y la tecnología de evaluación de riesgos deben «*aplicarse de forma* ***no discriminatoria***» y que las decisiones finales «*se basAn de forma "única y decisiva" en una evaluación individualizada* ***basada en la persona***»). También en este caso cabe señalar que el derecho a la intimidad y a la protección de los datos personales puede vincularse con otros derechos y principios fundamentales (en este caso, la no discriminación).

- Más concretamente, sobre el **impacto de la toma de decisiones automatizada utilizada por el Estado/las autoridadespúblicas**, véase Gobierno australiano, *Automated Assistance in Administrative Decision Making, Better Practice Guide* (Guía de mejores prácticas para la asistencia automatizada en la toma de decisiones administrativas), febrero de 2007 (aunque no esté actualizada, contiene un conjunto de preguntas pertinentes), disponible en https://www.oaic.gov.au/images/documents/migrated/migrated/betterpracticeguide.pdf.

[51] TEDH, *S. y Marper*, apartado 124: «*El Tribunal considera, además, que la conservación de los datos de las personas no condenadas puede ser* ***especialmente perjudicial*** *en el caso de los* ***menores*** *como el primer demandante, dada su especial situación y la importancia de su desarrollo e integración en la sociedad*».

- Véase, como ejemplo sobre la atención especial necesaria en caso de tratamiento de datos personales relativos a menores, la **respuesta del SEPD a la consulta pública de la Comisión sobre la reducción de la edad para la toma de impresiones dactilares para los menores en el procedimiento de visado de 12 a 6 años**, 9 de noviembre de 2017, página 2: «*El SEPD recomienda que la necesidad y la proporcionalidad de la recogida de* ***datos dactiloscópicos de los menores*** *a partir de una edad más temprana sean objeto de una* ***reflexión y una evaluación previas adicionales****, como* ***parte de la evaluación del impacto*** *quese realice para acompañar la futura propuesta de la Comisión de revisar el Reglamento VIS*». La respuesta del SEPD está disponible en https://edps.europa.eu/sites/edp/files/publication/17-11-09_formal_comments_2017-0809_en.pdf.

[52] Véase Christopher Docksey, *Four fundamental rights: finding the balance* (Los cuatro derechos fundamentales: encontrar el equilibrio), International Data Privacy Law, 2016, Vol. 6, núm. 3, página 203: «*En algunos contextos, como la vigilancia masiva y la regulación independiente, los derechos de privacidad y protección de datos y la libertad de expresión funcionan de forma totalmente complementaria, reforzando cada uno de ellos al otro*».

[53] Ya en los años 70, Hans Jonas fue el precursor del principio de precaución. El 2 de febrero de 2000, la **Comisión Europea**declaró en su **Comunicación sobre el principio de precaución** (COM(2000)1 final): «*Aunque en el Tratado sólo se mencione explícitamente el principio de precaución en el terreno del* ***medio ambiente****, su ámbito de aplicación es* ***mucho más amplio****. Este principio abarca los casos específicos* ***en los que los datos científicos son insuficientes, no concluyentes o inciertos****, pero en los que una evaluación científica objetiva preliminar hace sospechar de que existen* ***motivos razonables para temer*** *que los efectos potencialmente peligrosos para el medio ambiente y la salud humana, animal o vegetal pudieran ser incompatibles con el alto nivel de protección elegido.* ». La Comunicación está disponible en: https://eur-lex.europa.eu/legal- content/EN/TXT/PDF/?uri=CELEX:52000DC0001&from=EN.
Consideramos que este principio, en consonancia con la metáfora de la pérdida de la intimidad como «contaminación de losdatos», es también aplicable a los riesgos para la intimidad y la protección de los datos personales.

- P. Popelier y C. Van De Heyning, *Procedural Rationality: Giving Teeth to the Proportionality Analysis*,European Constitutional Law Review, 9, 2013, página 243: «*Cuando no existe un consenso en relación con el desarrollo de nuevas tecnologías que interfieren en la vida privada, el TEDH espera que un estado miembro «que reclama un papel pionero» asuma una «responsabilidad especial para alcanzar el equilibrio adecuado*». En referencia al asunto *S. y Marper contra Reino Unido,* TEDH.

- En su **Dictamen 4/2018 sobre las propuestas de dos Reglamentos por los que se establece un marco para la interoperabilidad entre los sistemas de información a gran escala de la UE**, el SEPD tuvo en cuenta los riesgos imprevisibles y pidió un debate más amplio y basado en pruebas (sobre la interoperabilidad), *«[...] la interoperabilidad no es principalmente una opción técnica; es ante todo una opción política que debe tomarse, con* ***importantes implicaciones jurídicas y sociales en***

de este principio, se podría sugerir al legislador, en función de todas las circunstancias pertinentes del caso, que adopte un «enfoque incremental», optando por el uso de una herramienta informática ya *experimentada y testada* en lugar de una herramienta informática cuya eficacia (falsos negativos, falsospositivos) aún no se habría comprobado plenamente.

Ejemplos relevantes

EJEMPLO 1: *Tele2 Sverige AB* (TJUE, C-203/15 y C-698/15, ECLI:EU:C:2016:970)

El Tribunal valoró la **injerencia** como **grave**, particularmente a la vista de que las medidas implicaban establecer un perfil de la persona afectada.

El Tribunal observó que: «*debe señalarse que ésta prevé una **conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados** en relación con **todos los medios de comunicación electrónica**, y obliga a los proveedores de servicios de comunicaciones electrónicas a conservar esos datos de manera sistemática y continuada, sin ninguna excepción. Como se desprende de la resolución de remisión, las categorías de datos a las que se refiere dicha normativa se corresponden, en esencia, con aquellas cuya conservación estaba prevista por la Directiva 2006/24.*».

«[...] *los **datos** que deben conservar los proveedores de servicios de comunicaciones electrónicas **permiten rastrear e identificar el origen de una comunicación y su destino, determinar la fecha, la hora, la duración y la naturaleza de una comunicación así como el equipo de comunicación de los usuarios, y localizar el equipo de comunicación móvil**. Entre esos datos se encuentra **el nombre y la dirección del abonado o usuario registrado, los números de teléfono de origen y destino y una dirección IP para los servicios de Internet**. Estos datos **permiten, en concreto, saber con qué persona se ha comunicado un abonado o un usuario registrado y de qué modo, así como determinar el momento de la comunicación y el lugar desde el que se ha realizado**. Además, permiten conocer **la frecuencia de las comunicaciones del abonado o del usuario registrado con determinadas personas durante un período concreto** (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 26).*».

«*Estos **datos, considerados en su conjunto, permiten extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los círculos sociales que frecuentan** (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 27). En particular, estos datos proporcionan medios para **determinar [...] el perfil de las personas afectadas**, información tan sensible, a la luz del respeto de la vida privada, como el propio contenido de las comunicaciones.*».

«*La **injerencia que supone una normativa** de este tipo en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta tiene **una gran magnitud y** debe considerarse **especialmente grave**. El hecho de que la conservación de los datos se efectúe sin que los*

usuarios de los servicios de comunicaciones electrónicas hayan sido informados de ello puede generar en las personas afectadas ***el sentimiento de que su vida privada es objeto de una vigilancia constante (véase, por analogía,*** *respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 37).».*

En lo que respecta a la repercusión de la medida sobre ***otros derechos fundamentales****, relacionados con el derecho a la intimidad y a la protección de datos personales, el Tribunal señaló que «la retención de datos de tráfico y localización podría (...) influir en el uso de los medios de comunicación electrónica y, en consecuencia, en el ejerciciopor los usuarios de esos medios de su* ***libertad de expresión****, garantizada por el artículo 11 de la Carta (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 28).»* (la negrita es nuestra).

El Tribunal también examinó la repercusión de la medida *ratione persona*, es decir, la obligación impuesta por lalegislación de conservar y hacer accesibles (también) los datos relativos a **los miembros de las profesiones que manejan información privilegiada o confidencial**: «*debe prestarse especial atención (...) a la necesidad y a la proporcionalidad cuando los datos de comunicaciones solicitados se refieran a una persona que sea miembro de una profesión que dispone de información protegida por el secreto profesional o que es confidencial por algún otro motivo*» (la negrita es nuestra).

EJEMPLO 2: *Ministerio Fiscal* (TJUE, C-207/16, ECLI:EU:C:2018:788)

El Tribunal sostuvo que: «*Debe (...)* ***determinarse si****, en el presente asunto, en función de las circunstancias del caso de autos, la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta que entraña el acceso de la Policía Judicial a los datos de que se trata en el litigio principal debe considerarse '****grave****'.*

«*A este respecto,* ***el oficio*** *controvertido en el litigio principal, por el que la Policía Judicial solicita, a efectos de la investigación de un delito, autorización judicial para acceder a los datos personales conservados por los proveedores de servicios de comunicaciones electrónicas, tiene por único objeto identificar a los titulares de las tarjetas SIM activadas durante un período de doce días con el número IMEI del teléfono móvil sustraído. (...) esta solicitud no tiene más objeto que el acceso a los números de teléfono correspondientes a las tarjetas SIM así como a los datos personales o de filiación de los titulares de dichas tarjetas, como su nombre, apellidos y, en su caso, la dirección.*

En cambio, ***esos datos no se refieren, como confirmaron tanto el Gobierno español como el Ministerio Fiscal en la vista, a las comunicaciones efectuadas con el teléfono móvil sustraído ni a la localización de este****».*

los años venideros*. Con el telón de fondo de la clara tendencia a mezclar distintos objetivos legislativos y políticos de la UE(es decir, controles fronterizos, asilo e inmigración, cooperación policial y ahora también cooperación judicial en asuntos penales), así como a conceder a los cuerpos de seguridad el acceso rutinario a bases de datos no policiales, la decisión del legislador de la UE de hacer interoperables los sistemas informáticos a gran escala no solo afectaría de forma permanente yprofunda a su estructura y a su forma de funcionamiento, sino que también cambiaría la forma en que se han interpretado hasta ahora los principios jurídicos en este ámbito y, como tal, marcaría un «punto de no retorno». Por estas razones, el SEPD pide un* ***debate más amplio sobre el futuro del intercambio de información de la UE, su gobierno y las formas de salvaguardar los derechos fundamentales en este contexto" (apartado 25).***

«*Por tanto, los datos a que se refiere la solicitud de acceso controvertida en el litigio principal solo permiten vincular, durante un período determinado, la tarjeta o tarjetas SIM activadas con el teléfono móvil sustraído y los datos personales o de filiación de los titulares de estas tarjetas SIM. Sin un cotejo con los datos relativos a las comunicaciones realizadas con esas tarjetas SIM y de localización, estos datos no permiten conocer la fecha, la hora, la duración o los destinatarios de las comunicaciones efectuadas con las tarjetas SIM en cuestión, ni los lugares en que estas comunicaciones tuvieron lugar, ni la frecuencia de estas con determinadas personas durante un período concreto.* ***Por tanto, dichos datos no permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados.***» (la negrita y el subrayado son nuestros).

En base a todo lo anterior, el Tribunal consideró que la **interferencia** no **resultaba grave**. Podemos observar queun factor clave que impulsó la valoración por parte del Tribunal como «no grave» de la injerencia (razonando a este respecto *a contrario* de *Tele2*) es **la ausencia del establecimiento de un perfil de la persona afectada.**

EJEMPLO 3: Dictamen 1/15 PNR Canadá (TJUE, ECLI:EU:C:2017:592)

La **injerencia** en el caso PNR de Canadá fue evaluada por el Tribunal en particular con referencia a la extensión,el nivel de intrusión y el alcance *ratione personae*. Esto último se consideró un problema en el acuerdo (junto conotros aspectos). El Tribunal sostuvo que «*si bien la injerencia que constituye el acuerdo previsto es* ***menos amplia*** *que la prevista* en la Directiva 2006/24, y es también **menos intrusiva** en la vida cotidiana de todos, su **carácterindiferenciado y generalizado** plantea interrogantes» (la negrita es nuestra).

Los demás aspectos problemáticos criticados por el Tribunal se refieren a: (i) la identificación de la autoridad competente responsable del tratamiento de los datos; (ii) el tratamiento automatizado (falta de garantías identificadas en los apartados 258-260); (iii) las condiciones de acceso a los datos conservados por parte de las autoridades policiales; (iv) el periodo de conservación de los datos; (v) la divulgación y transferencia de los datos; (vi) la supervisión por parte de una autoridad independiente. Estos problemas han sido señalados por el TJUE *también* en los casos *Digital Rights* y *Tele2*.

EJEMPLO 4: Bevándorlási és Állampolgársági Hivatal (TJUE, C-473/16, ECLI:EU:C:2018:36)

Sobre **la injerencia** de la medida en cuestión, el Tribunal observó: «*la* ***injerencia*** *en la vida privada del solicitante de protección internacional que se produce con la realización y utilización de un informe pericial, como el controvertido en el litigio principal, presenta, en cuanto a su naturaleza y objeto, una* ***especial gravedad***.».

«*Un informe de este tipo se basa particularmente en el hecho de que la persona de que se trate* ***se someta a una serie de tests psicológicos*** *que pretenden determinar un factor relevante de la identidad de esa persona que concierne a la esfera personal, dado que recae sobre* ***aspectos íntimos de la vida de dicha persona****.(...)*».

«*Asimismo, para poder valorar* ***la gravedad de la injerencia*** *de la realización y utilización de un examen psicológico como el controvertido en el litigio principal, debe tenerse en cuenta el principio 18 de los Principios de Yogyakarta sobre la aplicación de la*

« legislación internacional de derechos humanos en relación con la orientación sexual y la identidad de género, al que han hecho referencia los Gobiernos francés y neerlandés, que señala, en concreto, que ninguna persona será obligada a someterse a ninguna forma de examen psicológico por motivo de su orientación sexual o identidad de género.».

«De la interpretación conjunta de todos estos elementos se deduce que ***la gravedad de la injerencia*** *en la vida privada que resulta de la realización y utilización de un dictamen pericial, como el que es objeto del litigio principal, va más allá de la que supondría evaluar las declaraciones del solicitante de protección internacional sobre el temor a ser perseguido por su orientación sexual o recurrir a un informe pericial que tenga un objetivo distinto de determinar la orientación sexual de dicho solicitante.»*(la negrita es nuestra).

EJEMPLO 5: Dictamen 06/2016 del SEPD sobre el segundo paquete de fronteras inteligentes de la UE[54]

«El SEPD desea subrayar en primer lugar que, desde el punto de vista de los artículos 7 y 8 de la Carta, ***el tratamiento de datos personales que supondrá el EEE propuesto es significativo e intrusivo,*** *teniendo en cuenta el* ***número de personas afectadas*** *por este régimen, el* ***tipo de información*** *tratada,* ***los medios*** *utilizados para el tratamiento de dicha información y las diferentes finalidades que se persiguen, como se explica a continuación».*

EJEMPLO 6: Dictamen 3/2017 del SEPD sobre la propuesta de un Sistema Europeo de Información y Autorización de Viajes (SEIAV)

«La propuesta prevé la evaluación de todas las solicitudes de nacionales de terceros países exentos de visado conarreglo a las normas de control del SEIAV, mientras que solo un número limitado de ellos puede plantear en realidad determinados tipos de riesgos y se les puede denegar una autorización de viaje. Estas operaciones automatizadas y poco transparentes sobre los datos personales suponen como tales una ***injerencia*** *grave en los derechos fundamentales de un* ***número ilimitado de solicitantes****, que serían* ***objeto de elaboración de perfiles****. Debe sopesarse con el resultado esperado de dicha herramienta.*

Además, en función del ***método utilizado*** *para elaborar los indicadores de riesgo específicos, que podrían interpretarse de forma muy amplia,* ***el número de personas a las que se les deniega la autorización automatizada debido a un resultado basado en las normas de detección puede ser relativamente elevado****, aunque estas personas no representen realmente un riesgo».*

Paso 3: proceder a la evaluación del justo equilibrio de la medida

Cuando el legislador haya reunido **toda la información necesaria** (y solo entonces) y haya realizado la evaluación de la importancia y la eficacia y eficiencia de la medida y de su interferencia en la privacidad y en la protección de datos personales, deberá proceder a examinar el justo equilibrio de estos dos aspectos.

[54] Disponible en https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_en.pdf.

Ante una **asimetría de información**, por ejemplo, en caso de haber beneficios conocidos, pero costes desconocidos, o viceversa, será difícil, si no imposible, establecer si la medida es proporcionada, sopesando todos los factores.

En la práctica, el principio de proporcionalidad exige establecer un **equilibrio** entre el alcance y la naturaleza de la injerencia y las razones para interferir (las necesidades), traducidas en objetivos efectivamente perseguidos por la medida. El TJUE subrayó que *«Cuando están en juego varios derechos y libertades fundamentales protegidos por el ordenamiento jurídico de la Unión, la valoración de si una disposición del Derecho de la Unión resulta desproporcionada debe efectuarse respetando la necesaria* ***conciliación de las exigencias*** *relacionadas con la protección de distintos derechos y libertades y el* ***justo equilibrio*** *entre ellos»*[55].

En otras palabras, el principio sirve de instrumento para equilibrar los intereses en conflicto según un criterio racional en los casos en que no se da prioridad *a priori* a ninguno de los mismos[56].

En efecto, existe un método posible para revisar si un acto jurídico de la UE puede considerarse compatible con los artículos 7 y 8 de la Carta y con el principio de proporcionalidad previsto en el artículo 52, apartado 1, de la Carta. Dicho método se derivaría, en particular, de las sentencias del TJUE a las que se hace referencia en las presentes Directrices, en particular, pero no exclusivamente, en el ámbito específico de los «programas generales de vigilancia»[57].

Orientación (cómo proceder)

- En primer lugar, *antes* del ejercicio de la ponderación, verificar si existe una situación de **asimetría de información**: *¿se ha recopilado toda la información pertinente y se han evaluadotanto los «beneficios» como los «costes» de la medida?*
- A continuación, **comparar** las limitaciones a la privacidad y la protección de datos y los beneficios (el ejercicio de la **ponderación**): *¿son las medidas previstas para cumplir el objetivouna respuesta proporcionada a la necesidad que fundamenta una propuesta de legislación, dadas las limitaciones a los derechos de protección de datos y privacidad?*

---

55 Asuntos del TJUE: C-283/11, *Sky Österreich GmbH contra Österreichischer Rundfunk* (Gran Sala), ECLI:EU:C:2013:28, apartado 60; C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU*, ECLI: EU:C:2008:54, apartados 65 y 66; y C-544/10, *Deutsches Weintor*, ECLI:EU:C:2012:526, apartado 47; sentencia del TEDH, *Big Brother Watch y otros contra Reino Unido*, 13 de septiembre de 2018, «*2.42. La evaluación de la proporcionalidad de la solicitud debe incluir, en particular, una consideración de los derechos (particularmente a la intimidad y, en los casos pertinentes, a la libertad de expresión) de la persona y una ponderación de estos derechos con el beneficio de la investigación*».

56 En concreto, véase el asunto del TJUE C-28/08, *Bavarian Lager*, apartado 56: «*Los Reglamentos nº 45/2001 y nº 1049/2001 fueron adoptados en fechas muy próximas. No contienen ninguna disposición que establezca expresamente la primacía de uno de los Reglamentos sobre el otro.*».

57 En el **Dictamen 4/2018 sobre las Propuestas de dos Reglamentos por los que se establece un marco de interoperabilidad entre los sistemas de información a gran escala de la UE**, en la página 12, el SEPD aclaró que «*las nuevas operaciones de tratamiento de datos* ***destinadas a identificar correctamente a las personas*** *constituyen una* ***injerencia en sus derechos fundamentales protegidos por los artículos 7 y 8 de la Carta****. En consecuencia, deben superar las pruebas de necesidad y proporcionalidad (artículo 52, apartado 1, de la Carta)*».

- Véase también *S. y Marper contra Reino Unido*, TEDH, apartado 67: «*El* ***mero almacenamiento de datos relativos a la vida privadade una persona*** *equivale a una injerencia en el sentido del artículo 8* [...]. *El uso posterior de la información almacenada no influye en esa conclusión* [...]. *Sin embargo, para determinar si la información personal conservada por las autoridades implicaalguno de los aspectos de la vida privada mencionados anteriormente, el Tribunal tendrá debidamente en cuenta el contexto específico en el que la información en cuestión ha sido registrada y conservada, la naturaleza de los registros, la forma en quedichos registros se utilizan y se procesan y los resultados que pueden obtenerse*».

- Después de realizar el ejercicio de la ponderación, asegúrese de que se produzcan y, en su caso,se publiquen las **pruebas** adecuadas, estableciendo que **se ha realizado el análisis** *(Informe sobre la prueba de proporcionalidad*, es decir, un análisis sintético del **resultado** de laevaluación realizada).
- **Conservar (registrar y almacenar) toda la documentación relevante** obtenida o producida durante la realización del ejercicio de la **ponderación** y la redacción del *Informe sobre la prueba de proporcionalidad*. Dicha documentación deberá ser pertinente y suficiente para justificar (o identificar las cuestiones críticas) de la medida que se examina (objetivo de la evaluación), y debe mencionarse en un anexo del informe[58].

Ejemplos relevantes

EJEMPLO 1: *Tele2 Sverige AB* (TJUE, C-203/15 y C-698/15, ECLI:EU:C:2016:970)

En *Tele2*, el Tribunal sostuvo que «*Habida cuenta de la **gravedad** de la injerencia en los derechos fundamentales afectados que supone una normativa nacional que prevé, a efectos de la lucha contra la delincuencia, la conservación de datos de tráfico y de localización, **sólo la lucha contra la delincuentica grave puede justificar una medida de este tipo*** ». (la negrita es nuestra).

*El Tribunal tenía clara, por un lado, la importancia y la eficacia de la medida; por otro, el **ámbito de aplicación** (no se limita a los datos relativos a un período de tiempo y/o a una zona geográfica determinada y/o a las personassusceptibles de estar implicadas en un delito grave) y el **nivel/intensidad** (incluida la **elaboración de perfiles**) dela injerencia.*

58 En sus conclusiones , ECLI:EU:C:2013:845, en los asuntos acumulados C-293/12 y C-594/12, *Digital Rights*, el Abogado Generalseñaló la **falta de motivación pertinente y suficiente** sobre el **periodo de conservación de datos** de dos años previsto por laDirectiva como factor clave para rechazar la proporcionalidad del periodo de conservación de datos de dos años (frente al tiempo de conservación inferior a un año, que resulta más justificado). Ver apartados 148-149: «*puede entenderse que un período de conservación de datos personales «que se mide en meses» debe diferenciarse de un período «que se mide en años». El primero corresponde al que se sitúa en la vida que se percibe como presente y el segundo al que se sitúa en la vida que se percibe como memoria. La injerencia en el derecho al respeto de la vida privada es, desde esta perspectiva, diferente en ambos supuestos y la necesidad de cada una de estas injerencias debe poder justificarse . […] **no encuentro ninguna justificación para una injerencia que debe extenderse en el tiempo histórico**. Expresado más directamente, y sin negar que existen actividades delictivas que se preparan con mucha antelación, no he encontrado, en las distintas posturas que defienden la proporcionalidad del artículo 6 de la Directiva 2006/24, ninguna justificación suficiente para que el período de conservación de datos que deben fijar los Estados miembros no deba mantenerse dentro de un límite inferior a un año.*».

- Véanse también los asuntos acumulados *Volker und Markus Schecke y Hartmut Eifert*, **C-92/09 y C-93/09**, ECLI:EU:C:2010:662, apartado 81: «***nada indica que**, al adoptar el artículo 44 bis del Reglamento nº 1290/2005 y el Reglamento nº 259/2008, el Consejo y la Comisión hayan tomado en consideración otras formas de publicación de la información relativa a los beneficiarios afectados que respetasen el objetivo perseguido por dicha publicación y, al mismo tiempo, fueran menos lesivas para el derecho de tales beneficiarios al respeto de su vida privada, en general, y a la protección de sus datos de carácter personal, en particular […]*». (la negrita es nuestra).

- En el **Dictamen 7/2018** sobre la propuesta de Reglamento sobre el refuerzo de la seguridad de los documentos de identidadde los ciudadanos de la Unión y otros documentos, de 10 de agosto de 2018 (disponible en: https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en_0.pdf) en la página 3, el SEPD « *observa que la evaluación de impacto que acompaña a la propuesta **no parece respaldar la opción política elegida** por la Comisión, es decir: la inclusión obligatoria de imágenes faciales y de (dos) impresiones dactilares en los documentos de identidad (y en los documentos de residencia) […] por tanto, el SEPD recomienda volver a evaluar la necesidad y la proporcionalidad del tratamiento de los datos biométricos (imagen facial junto con impresiones dactilares) en este contexto.*».

- Asimismo, en el **Dictamen 7/2017 sobre la nueva base jurídica del Sistema de Información de Schengen**, de 2 de mayode 2017 (disponible en: https://edps.europa.eu/sites/edp/files/publication/17-05-02_sis_ii_opinion_en.pdf), el SEPD, en la página 3, consideró «*que la introducción de nuevas categorías de datos, entre las que se incluyen nuevos identificadores biométricos, plantea la cuestión de la necesidad y proporcionalidad de los cambios propuestos. Por esta razón, las propuestas deberían complementarse con la evaluación del impacto en el derecho a la protección de datos y el derecho a la intimidad, ambos recogidos en la Carta de los Derechos Fundamentales de la UE.*».

Tras sopesar ambas cuestiones, el Tribunal sostuvo que: «*La eficacia de la lucha contra la delincuencia grave* ***no puede por sí solo justificar*** *que una legislación nacional que establezca la* ***conservación generalizada e indiferenciada*** *de todos los datos de tráfico y de localización deba ser considerada necesaria a los efectos de dicha lucha* ». Así, la medida «***excede*** *los límites* ***de lo estrictamente necesario*** *y no puede considerarse justificada, dentro de una sociedad democrática*» (la negrita es nuestra).

EJEMPLO 2: *Ministerio Fiscal* (TJUE, C-207/16, ECLI:EU:C:2018:788)

En el caso *del Ministerio Fiscal*, el Tribunal sostuvo que la medida examinada es **proporcional** (supera con éxito la prueba de proporcionalidad y, por tanto, es legal en virtud de los principios de necesidad y proporcionalidad).

Un factor clave para esta evaluación es el hecho de que la interferencia había sido considerada como «no grave»,y por consiguiente no podía superar la importancia («igualmente» no grave/alta) del objetivo efectivamente cumplido por la medida.

Refiriéndose a las palabras del Tribunal: «cuando la injerencia que implica dicho acceso no es **grave**, puede estar **justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general**». *Por el contrario, «conforme al principio de proporcionalidad, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos solo puede justificar una injerencia grave el objetivo de luchar contra la delincuencia que a su vez esté* ***también calificada de "grave"*** (la negrita es nuestra).

EJEMPLO 3: Dictamen 1/15, PNR Canadá (TJUE, ECLI:EU:C:2017:592)

La medida que se examina en este caso presenta **una asimetría de información** entre los beneficios esperados y el impacto sobre el derecho fundamental a la intimidad y a la protección de los datos personales. Esto se debe, en particular, al hecho de que **las categorías de datos personales** que deben tratarse no están redactadas de **forma clara y precisa**; las normas aplicables a la preselección automatizada de los pasajeros **tampoco** están **especificadas** por la medida.

De hecho, esta falta de especificaciones no solo imposibilita el ejercicio de comparabilidad, sino que lleva al Tribunal a declarar directamente que el acuerdo, en su versión actual, **no** es compatible con los artículos 7 y 8 y con el artículo 52, apartado 1, de la Carta.

EJEMPLO 4: Bevándorlási és Állampolgársági Hivatal (TJUE, C-473/16, ECLI:EU:C:2018:36)

En este caso, el Tribunal, teniendo en cuenta todos los elementos sobre la importancia y la eficacia de la medida y sobre su injerencia (en una sola persona determinada, en este caso), concluyó que: «el artículo 4 de la Directiva 2011/95, a la luz del artículo 7 de la Carta, debe interpretarse en el sentido de que se opone a que, para valorar la credibilidad de la orientación sexual alegada por un solicitante de protección internacional, se realice y se utilice un examen psicológico, como el controvertido en el litigio principal, que tiene por objeto proporcionar una imagen de la orientación sexual de dicho solicitante, basándose en tests de personalidad proyectivos.» (la negrita es nuestra).

En otras palabras, el Tribunal consideró que la medida examinada **no era proporcional**, debido a la gravísima injerencia de la medida, pero también a la falta de eficacia para alcanzar el objetivo perseguido.

EJEMPLO 5: *Scarlet Extended* (TJUE, C-70/10, ECLI:EU:C:2011:771)

Este caso es interesante porque demuestra que el **derecho a la protección de datos** personales puede desempeñar el papel de un *derecho concurrente*, es decir, no el que se ve principalmente afectado por la medida, pero que, sin embargo, **junto** con otros derechos (libertad de empresa; libertad de recibir o de comunicar información), puede inclinar la balanza a favor de la no proporcionalidad de la medida (que persigue el objetivo de proteger mejor los derechos de propiedad intelectual).

Recogemos los extractos más relevantes de esta sentencia: «Dadas las circunstancias, procede considerar que el requerimiento judicial por el que se ordena establecer el **sistema de filtrado** litigioso no respeta el requisito de garantizar un **justo equilibrio** entre, por un lado, la **protección del derecho de propiedad intelectual** que ampara a los titulares de derechos de autor y, por otro, la protección de la... que ampara a los operadores, como los PAI.

*Por otro lado, los efectos de dicho requerimiento judicial no se limitarían al PAI afectado, ya que el sistema de filtrado litigioso **también** puede **vulnerar los derechos fundamentales de los clientes de ese PAI, a saber, su derecho a la protección de datos de carácter personal y su libertad de recibir o comunicar informaciones**, derechos que se encuentran protegidos por los artículos 8 y 11 de la Carta* (...))

«*Por consiguiente, procede declarar que, si adoptara el requerimiento judicial por el que se obliga al PAI a establecer el sistema de filtrado litigioso, el órgano jurisdiccional nacional en cuestión **no respetaría el requisito de garantizar un justo equilibrio** entre, por un lado, **el derecho de propiedad intelectual** y, por otro, **la libertad de empresa**, el **derecho a la protección de datos de carácter personal** y la **libertad de recibir o comunicar informaciones**.*» (la negrita es nuestra).

EJEMPLO 6: Dictamen 1/2017 del SEPD sobre una propuesta de la Comisión que modifica la Directiva (UE) 2015/849 y la Directiva 2009/101/CE. Acceso a la información sobre la propiedad efectiva e implicaciones para la protección de datos

En este Dictamen, así como en la Propuesta, el objetivo se denomina «riesgo que debe evitarse» (en este caso, el riesgo de blanqueo de capitales y financiación del terrorismo). Por regla general, la recogida y el tratamiento de datos personales, para ser proporcionados al objetivo, deben «ajustarse» (tener en cuenta) al riesgo (por ejemplo, al «orden público económico») que suponen las personas afectadas. Esto permitiría **optimizar** la injerencia en el derecho a la intimidad y a la protección de los datos personales.

El dictamen del SEPD sobre la propuesta de modificación de la Directiva contra el blanqueo de capitales señaló que, en contra del planteamiento mencionado: «*la Propuesta* [...] *elimina las salvaguardias existentes que habrían concedido un cierto **grado de proporcionalidad**.*

Por ejemplo, al establecer las condiciones de acceso a la información sobre las operaciones financieras por parte de las UIF, la Propuesta establece que, en el futuro, la necesidad de las UIF (Unidades de Inteligencia Financiera) de obtener información adicional ***ya no*** *podrá ser* ***activada y no solo por las transacciones sospechosas*** *(como ocurre ahora [el llamado «enfoque basado en el riesgo» de la lucha contra el blanqueo de capitales]), sino también por el propio análisis e inteligencia de las UIF,* ***incluso sin una notificación previa de operaciones sospechosas****. Por consiguiente, el papel de las UIF está pasando de estar "basado en la investigación" a estar "basado en la inteligencia". Este último enfoque se asemejamás a la extracción de datos que a una investigación selectiva, con las evidentes consecuencias en términos de protección de datos personales*».

EJEMPLO 7: Directrices de videovigilancia del SEPD

El mismo enfoque, consistente en buscar **la optimización de la interferencia en el derecho a la intimidad y a la protección de los datos personales con el objetivo perseguido por la medida** (por ejemplo, la seguridad de los locales), se aplica en las directrices del SEPD sobre la videovigilancia: «*Utilizando un enfoque pragmático basado en el doble principio de selectividad y* ***proporcionalidad,*** *los sistemas de videovigilancia pueden satisfacerlas necesidades de seguridad respetando al mismo tiempo nuestra intimidad. Las cámaras pueden y deben utilizarse de forma inteligente y* ***únicamente*** *deben* ***centrarse en problemas de seguridad específicamente identificados****, minimizando así la recopilación de imágenes irrelevantes. Esto no solo minimiza la intrusión en laintimidad, sino que también ayuda a garantizar un uso* ***más específico y, en última instancia, más eficiente*** *de la videovigilancia*». En las Directrices se ofrecen indicaciones específicas (entre otras, sobre: ubicación de las cámaras y ángulos de visión; número de cámaras; horarios de vigilancia; resolución y calidad de la imagen; categorías especiales de datos; zonas con mayores expectativas de privacidad; videovigilancia de alta tecnología y/o inteligente; interconexión de sistemas de videovigilancia).

EJEMPLO 8: Véase el Dictamen 5/2015 del SEPD sobre la propuesta de Directiva relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves.

«El requisito previo esencial para un sistema de PNR, es decir, el cumplimiento de los principios de necesidad y proporcionalidad sigue sin cumplirse en la Propuesta. La propuesta (...) no establece ningún análisis detallado de la medida en que medidas menos intrusivas podrían lograr el propósito del sistema PNR de la UE. Por último, la recogida y el tratamiento de datos no selectivos y masivos del sistema de PNR equivalen a una medida de vigilancia general.

En opinión del SEPD, la única finalidad que se ajustaría a los requisitos de transparencia y proporcionalidad sería la utilización de los datos de PNR caso por caso, pero únicamente en caso de amenaza grave y concreta establecida por indicadores más específicos. Dado que ***no se dispone de información que demuestre adecuadamente la necesidad y la proporcionalidad de las medidas*** *propuestas,*

*el SEPD considera que la Propuesta, **incluso modificada, sigue sin cumplir** las normas de los artículos 7, 8 y 52 de la Carta de los Derechos Fundamentales de la Unión, del artículo 16 del TFUE y del artículo 8 del CEDH. El SEPD insta a los legisladores a que sigan estudiando la viabilidad, frente a las amenazas actuales, de **medidas de vigilancia más selectivas y menos intrusivas basadas en iniciativas más específicas centradas, en su caso, en categorías específicas de vuelos, pasajeros o países**».*

Paso 4: analizar las conclusiones sobre la proporcionalidad de la medida propuesta. *Si* la conclusión es «no proporcional», identificar e introducir salvaguardias que puedan hacer que la medida sea proporcional

Si el ejercicio de ponderación descrito en el paso 3 lleva a la conclusión de que una medida propuesta **no** cumple el requisito de proporcionalidad, entonces o bien **no debe proponerse** la medida, o bien debe **modificarse** para que cumpla estos requisitos.

Orientación (cómo proceder)

- Analizar sintéticamente el **resultado** de la evaluación realizada en el paso 3, como se describe en el *Informe sobre la evaluación de la proporcionalidad*, destacando en particular **los factores** que dieron lugar a la conclusión de «no proporcionalidad» («prueba de proporcionalidad negativa»);
- **Reformular** la propuesta, redactando, si fuera posible, una o varias **opciones correctoras** que aborden las cuestiones críticas **(definir** de forma más concreta la finalidad, las categorías y la cantidad de datos personales que se van a tratar[59], y reducir así el nivel de interferencia de la medida con la privacidad y la protección de datos);
- Prever e introducir **salvaguardias** que reduzcan el impacto de la propuesta sobre los derechos fundamentales en juego *(por ejemplo*, introducir la necesidad de verificación humana en caso de que la legislación prevea medidas totalmente automatizadas)[60].

---

[59] Como ejemplo, véanse **las observaciones formales del SEPD sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a los administradores de créditos, los compradores de créditos y la recuperación de las garantías**, en las que se recomienda definir mejor las categorías y la cantidad de documentos (que contienen datos personales) que deben tratarse en virtud de la Propuesta, en la página 3. Los comentarios formales están disponibles en: https://edps.europa.eu/sites/edp/files/publication/19-01-24_comments_proposal_directive_european_parliament_en.pdf

[60] Como ejemplo de **salvaguardias**, véase el **Dictamen 4/2018 del SEPD sobre las propuestas de dos Reglamentos por los que se establece un marco de interoperabilidad entre los sistemas de información a gran escala de la UE**, página 16: «*los diferentes instrumentos también exigen la **verificación por parte de una autoridad independiente** de que se cumplen las condiciones antes del acceso. En el caso del SEIAV, el EES y el sistema Eurodac, las autoridades policiales también deben **consultar en primer lugar otros sistemas pertinentes** (por ejemplo, bases de datos nacionales, datos de Europol, Prüm, el VIS)*».
Véase también el Dictamen de la FRA sobre «Interoperabilidad e implicaciones para los derechos fundamentales» (*Interoperability and fundamental rights implications*), de 11 de abril de 2018, en relación con la necesidad de un trato diferenciado (salvaguardias) para las personas vulnerables, observaciones (página 33): «*Sustituir el sistema de cascada por un mecanismo racionalizado, como la propuesta de comprobación de aciertos y errores en el registro común de datos de identidad significa que los datos de todas las personas se consideran igualmente sensibles y que los datos de las personas en **situación vulnerable vulnerable** (como los de las personas que solicitan protección internacional) no requerirían **garantías reforzadas***».
Con respecto a las salvaguardias (verificación humana, explicaciones significativas, notificación) en el contexto de un posible uso de medidas automatizadas, véanse **los comentarios formales del SEPD sobre la propuesta de la Comisión relativa a la prevención de la difusión de material terrorista en línea**, en la página 8: «*El artículo 8, apartado 1, en el marco de las "obligaciones de transparencia", establece que los PSH deben exponer en sus condiciones su política de prevención de contenidos terroristas, «incluyendo, en su **caso**, una explicación significativa del funcionamiento de las medidas proactivas, incluido el uso de herramientas automatizadas*» (la negrita es nuestra).
Asimismo, el artículo 9, apartado 1, establece que los PSH que utilicen herramientas automatizadas introducirán salvaguardias efectivas y

- Prever la **reevaluación** y las **cláusulas de extinción**: lo más probable es que la situación que se quiere abordar se caracterice por un entorno muy dinámico, tanto desde el punto de vista tecnológico como social. Esta incertidumbre podría contribuir a la evaluación de la medida como no proporcional por «razones prudenciales» (principio de precaución), debido a las incertidumbres sobre el impacto efectivo de la medida (por ejemplo, debido a las herramientastecnológicas previstas). En este caso, además de otras salvaguardias, es aconsejable prever una **reevaluación** estricta (controles regulares/evaluación del impacto *post factum*, también con el objetivo de abordar los efectos inesperados) y las **cláusulas de extinción** («a menos que se confirme o revise, la medida *ya no resultará aplicable a partir de*»). También podría considerarse la posibilidad de crear mecanismos u organismos de **supervisión específicos**[61].
- **Volver a realizar** la evaluación de la necesidad y la proporcionalidad (ambas pruebas, ya que la modificación introducida podría provocar la necesidad de realizar de nuevo cada paso de laspruebas 1 y 2).

Ejemplos relevantes

EJEMPLO 1: *Tele2 Sverige AB* (TJUE, C-203/15 y C-698/15, ECLI:EU:C:2016:970)

El **resultado** de la evaluación de la proporcionalidad (denominada 'necesidad estricta') en *Tele2* es **negativo**. El Tribunal de Justicia señala los **factores** que determinaron su apreciación negativa: en particular, dichos factores se refieren a la (falta de) relación entre los datos que deben conservarse y la amenaza a la seguridad pública, cuyalucha es el objetivo de la medida (véase el apartado 106 de la sentencia).

A contrario, el Tribunal también estableció expresamente las características de la medida proporcionada. En particular, la medida «*debe establecer, en primer lugar, normas claras y precisas que regulen el alcance y la aplicación de una medida de conservación de datos de este tipo y que establezcan unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos personales frente a los riesgos de abusos*

apropiadas para garantizar que las decisiones tomadas, en particular para eliminar o inutilizar contenidos, sean exactas y estén bien fundadas. El artículo 9, apartado 2, especifica que dichas salvaguardias consistirán en «*la supervisión y las verificaciones humanas **cuando proceda** y,en cualquier caso, cuando se requiera una evaluación detallada del contexto pertinente* [...]» (la negrita es nuestra). Teniendo en cuenta estas salvaguardias, el SEPD recomienda sustituir en el artículo 8, apartado 1, y en el artículo 9, apartado 2, la expresión «cuando proceda» por «en cualquier caso», o bien suprimir la expresión «cuando proceda». El SEPD también observa que, de conformidad con el artículo 6, apartado 2, los PSH deben presentar un informe sobre las medidas proactivas adoptadas, incluidas las basadas en herramientas automatizadas, a la autoridad competente para supervisar la aplicación de las medidas proactivas en virtud del artículo 17, apartado 1, letra c). El SEPD recomienda que se especifique en la Propuesta, en el considerando 18, que los PSH debenproporcionar a las autoridades competentes toda la información necesaria sobre las herramientas automatizadas utilizadas parapermitir una supervisión pública exhaustiva de la eficacia de las herramientas y para garantizar que no producen resultados discriminatorios, no específicos o injustificados». Los comentarios formales están disponibles en:
https://edps.europa.eu/data-protection/our-work/publications/comments/formal-comments-edps-preventing-dissemination_en

[61] Véase **el Documento de trabajo 01/2016 del WP29 sobre la justificación de las injerencias en los derechos fundamentales a la intimidad y a la protección de datos a través de medidas de vigilancia cuando se transfieren datos personales (garantías esenciales europeas),** WP237 de 13 de abril de 2016, sección 6, «Garantía C - **Debe existir unmecanismo de supervisión independiente**», páginas 9-10. El documento está disponible en:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf.

EJEMPLO 2: *Ministerio Fiscal* (TJUE, C-207/16, ECLI:EU:C:2018:788)

En el caso *del Ministerio Fiscal*, la medida fue considerada por el Tribunal como **proporcionada** al objetivo. El Tribunal no realizó ninguna observación sobre las cuestiones críticas que debe abordar el legislador. Por consiguiente, no es necesario necesario reelaborar la medida (redefinir la finalidad, el ámbito de aplicación, el nivel de interferencia; establecer más o diferentes salvaguardias) y/o **volver a realizar** la evaluación de la necesidad y la proporcionalidad.

EJEMPLO 3: Dictamen 1/15, PNR Canadá (TJUE, ECLI:EU:C:2017:592)

El Tribunal consideró que la medida **no** era compatible con los artículos 7 y 8 y el artículo 52.1 de la Carta. Los factores que dieron lugar a esta evaluación final se referían básicamente a: a) la falta de claridad y especificación de la medida (y, por consiguiente, a la imposibilidad de medir el impacto); b) la falta de salvaguardias (por ejemplo, el control por parte de una autoridad independiente).

Al mismo tiempo, el Tribunal detalló las condiciones (precedidas por la expresión «siempre que», «en la medida en que») que harían que la medida fuera proporcionada. Así, por un lado, la discrecionalidad del legislador en este caso es bastante reducida, ya que tendrá que seguir las instrucciones puntuales proporcionadas por el Tribunal. Al mismo tiempo, el trabajo del legislador se ve claramente facilitado ya que, siguiendo el consejo del Tribunal de Justicia al volver a redactar la medida, debe estar a salvo del riesgo de otra declaración de incompatibilidad por parte del Tribunal.

EJEMPLO 4: Bevándorlási és Állampolgársági Hivatal (CJEU, C-473/16, ECLI:EU:C:2018:36)

El Tribunal de Justicia consideró que el artículo 7 de la Carta debe interpretarse en el sentido de que se **opone** a que, para valorar la credibilidad de la orientación sexual alegada por un solicitante de protección internacional, se realice y se utilice un examen psicológico, como el controvertido en el litigio principal, que tiene por objeto proporcionar una imagen de la orientación sexual de dicho solicitante, basándose en tests de personalidad proyectivos. En este caso, parece difícil, dada en particular el **altísimo nivel** de la injerencia, prever **salvaguardias** que puedan hacer proporcionado el recurso a la medida objeto de examen.