EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

11 de abril de 2017

Manual para la evaluación de la necesidad de las medidas que limiten el derecho fundamental a la protección de datos de carácter personal

edps.europa.eu

Índice

I. El objetivo del presente manual y cómo utilizarlo

Los derechos fundamentales, consagrados en la Carta de los Derechos Fundamentales de la Unión Europea (en adelante, «la Carta»), constituyen los valores fundamentales de la Unión Europea[1]. Estos derechos deben respetarse siempre por parte de las instituciones y organismos de la UE 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 importante en el ordenamiento jurídico de la UE, en particular el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades (CEDH).

El presente manual responde a la demanda de las instituciones de la UE de recibir directrices sobre los requisitos particulares derivados del apartado 1 del artículo 52 de la Carta, que establece que cualquier limitación del ejercicio del derecho a la protección de datos de carácter personal (artículo 8 de la Carta) debe ser «necesaria» para un objetivo de interés general o para proteger los derechos y libertades de terceros[2].

Por otra parte, las condiciones de las posibles limitaciones al ejercicio de los derechos fundamentales son una de las características más importantes de la Carta, puesto que determinan el grado de ejercicio efectivo de los derechos.

La necesidad es un requisito esencial que debe cumplir cualquier medida propuesta que implique el tratamiento de datos de carácter personal.

El presente manual pretende 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 y ha sido elaborado para dotar mejor a los responsables políticos y legislativos de la UE encargados de elaborar o examinar las medidas que implican el tratamiento de datos de carácter personal y limitan el derecho a la protección de estos y otros derechos y libertades previstos en la Carta.

El SEPD respeta plenamente la responsabilidad del legislador a la hora de evaluar la necesidad y la proporcionalidad de una medida. En consecuencia, el presente manual no pretende ni puede proporcionar una evaluación definitiva sobre si una medida específica propuesta puede considerarse necesaria o no. Este manual ofrece más bien una lista de control práctica, paso a paso, para evaluar la necesidad de nuevas medidas legislativas, junto con un análisis jurídico de la noción de necesidad en relación con el tratamiento de datos de carácter personal.

Complementa y desarrolla más en profundidad las directrices existentes elaboradas por la Comisión y el Consejo sobre las limitaciones de los derechos fundamentales en general en relación, por ejemplo, con las evaluaciones de impacto y los controles de compatibilidad[3].

Este manual también incluye esta introducción, en la que se expone el contenido y la finalidad del mismo, una lista de comprobación práctica paso a paso para evaluar la necesidad de nuevas medidas legislativas y un análisis jurídico de la evaluación de la necesidad aplicado al tratamiento de datos de carácter personal. La lista de comprobación es la parte fundamental del presente manual y puede usarse de forma independiente.

Este manual se basa en la jurisprudencia[4] del Tribunal de Justicia de la Unión Europea (en adelante, TJUE), del Tribunal Europeo de Derechos Humanos (TEDH) y en anteriores dictámenes del SEPD y del Grupo del Artículo 29. Es la continuación de un documento de referencia[5] publicado en 2016 para su consulta pública.

Agradecemos a los encuestados sus comentarios, los cuales hemos aprovechado para mejorar el documento.

Nota sobre la terminología

En lo que respecta a los derechos mencionados en la Carta de los Derechos Fundamentales, una serie de términos similares, como «limitación», «restricción», «injerencia» y «afectación» y sus respectivas derivaciones, se utilizan de forma aparentemente intercambiable en los debates políticos e incluso en los textos jurídicos, incluida la jurisprudencia del TJUE. En aras de la simplicidad, en el presente manual se seguirá el artículo 52 de la Carta y se utilizará el término «limitación» en todo el texto, excepto en el caso de las citas.

II. Análisis jurídico: la evaluación de la necesidad aplicada al derecho a la protección de datos de carácter personal

1. Evaluación de la necesidad a la hora de valorar la legalidad de cualquier medida propuesta que implique el tratamiento de datos de carácter personal

El artículo 8 de la Carta consagra el derecho fundamental a la protección de los datos de carácter personal. No es un derecho absoluto y puede limitarse, siempre que las limitaciones cumplan los requisitos previstos en el apartado 1 del artículo 52 de la Carta[6]. El mismo análisis se aplica al derecho al respeto de la vida privada consagrado en el artículo 7 de la Carta.

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

- debe estar prevista por ley,
- debe respetar la esencia de los derechos,
- debe responder realmente a objetivos de interés general reconocidos por la Unión o a la necesidad de proteger los derechos y libertades,
- debe ser necesaria, tema que aborda el presente manual, y
- debe ser proporcional.

Esta lista de criterios establece el orden requerido a la hora de evaluar la legalidad. En primer lugar, debe examinarse si una ley accesible y previsible[7] prevé una limitación, y si se respeta la **esencia del derecho**, es decir, si efectivamente el derecho queda vacío de su contenido básico y la persona no puede ejercerlo[8]. 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 apartado 1 del artículo 52 de la Carta.

La siguiente evaluación será si la medida cumple un **objetivo de interés general**. El objetivo de interés general proporciona el contexto en el que se puede evaluar la necesidad de la medida. Por consiguiente, es importante identificar el objetivo de interés general con suficiente detalle para poder evaluar si la medida es necesaria.

El siguiente paso es evaluar la **necesidad** de una medida legislativa propuesta que conlleve el tratamiento de datos de carácter personal.

Si se cumple esta evaluación, se evaluará la **proporcionalidad** de la medida prevista. Si el proyecto de medida no supera la evaluación de la necesidad, no será necesario analizar su proporcionalidad. No deberán proponerse medidas cuya necesidad no haya quedado demostrada hasta que se modifique para cumplir el requisito de necesidad.

La evaluación de la proporcionalidad, a la que está sujeta cualquier limitación de derechos fundamentales, será abordada por el SEPD en un documento independiente.

Es importante contar con una **descripción adecuada de la medida en cuestión**, ya que puede afectar a varios de los criterios mencionados. Por lo tanto, en ocasiones los tribunales pueden evaluar los criterios de forma conjunta. Por ejemplo, una medida definida de forma

poco clara o demasiado extensa puede impedir que se evalúe si está «prevista por la ley» y es «necesaria»[9].

2. La relación entre proporcionalidad y necesidad

La proporcionalidad 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 Tratados»*[10]. Según reiterada jurisprudencia del TJUE, *«el principio de proporcionalidad exige que los actos de las instituciones de la UE sean idóneos para alcanzar los objetivos legítimos perseguidos por la normativa de que se trate y no sobrepasen los límites de lo que es apropiado y necesario para alcanzar tales objetivos»*[11]. Por lo tanto, *«restringe a las autoridades en el ejercicio de sus facultades al exigir un equilibrio entre los medios utilizados y el objetivo previsto (o el resultado alcanzado)»*[12].

Según el apartado 1 del artículo 52 de la Carta, *«sin perjuicio del principio de proporcionalidad, las limitaciones [al ejercicio de los derechos fundamentales] solo podrán realizarse si son necesarias (...)»*.

La proporcionalidad en un sentido amplio abarca tanto la necesidad como la **idoneidad** de una medida, es decir, hasta qué punto existe un vínculo lógico entre la medida y el objetivo (legítimo) perseguido. Asimismo, para que una medida cumpla el principio de proporcionalidad consagrado en el apartado 1 del artículo 52 de la Carta, las ventajas derivadas de la medida no deben ser superadas por las desventajas que la medida cause con respecto al ejercicio de los derechos fundamentales[13]. Este último elemento describe la proporcionalidad en sentido estricto y constituye la prueba de proporcionalidad. Debe distinguirse claramente de la **necesidad.**

La necesidad implica que se requiere una evaluación 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 «necesidad» también es un principio de calidad de los datos y una condición recurrente en casi todos los requisitos sobre la legalidad del tratamiento de los datos de carácter personal que se derivan de la legalidad derivada de la protección de datos de la UE[14]. También existe un vínculo entre el apartado 2 del artículo 8 de la Carta y el derecho derivado, ya que el apartado 2 del artículo 8 hace referencia al fundamento legítimo para el tratamiento «previsto por la ley» y la nota explicativa del artículo 8 hace referencia a este derecho derivado afirmando que la Directiva 95/46 y el Reglamento 45/2001 «contienen condiciones y limitaciones para el ejercicio del derecho a la protección de los datos de carácter personal».

El presente manual se basa en la premisa de que únicamente una medida cuya necesidad quede demostrada debe pasar a la evaluación de la proporcionalidad. En casos recientes, el TJUE no procedió a evaluar la proporcionalidad al considerar que las limitaciones a los derechos de los artículos 7 y 8 de la Carta no eran estrictamente necesarias[15]. Por ejemplo, una medida sobre la aplicación de una ley, en caso de considerarse necesaria, debería analizarse en función de si sería más proporcionada si se limitara únicamente a delitos graves. Una evaluación de la proporcionalidad podría implicar la valoración de las normas que deberían acompañar a una medida de control antes o después de su autorización: dichas normas, a menudo denominadas «garantías», servirían para reducir los riesgos que la medida prevista supone para los derechos fundamentales.

En la práctica, un aspecto específico o una disposición incluida en un proyecto de medida

podría ser relevante tanto para la evaluación de la necesidad como de la proporcionalidad. Por ejemplo, la cuestión de si una medida debe estar destinada a cualquier delito o solo a los más graves puede considerarse una cuestión de necesidad; sin embargo, en caso de que se considere necesaria una disposición de este tipo, habría que evaluar su proporcionalidad y su riesgo de vulneración de los valores de una sociedad democrática. Por tanto, en la práctica, existe una cierta superposición entre las nociones de necesidad y proporcionalidad, y dependiendo de la medida en cuestión, ambas evaluaciones pueden llevarse a cabo de forma simultánea o incluso en orden inverso[16].

No obstante, como enfoque general, en primer lugar, será necesario establecer si una limitación de un derecho fundamental es necesaria antes de proceder a evaluar la proporcionalidad.

3. La Carta y el CEDH

Si bien es cierto que el **derecho al respeto de la vida privada** (también llamado derecho a la intimidad) se aborda en la Carta (artículo 7) y en el CEDH (artículo 8), el **derecho a la protección de datos de carácter personal** como tal es un derecho fundamental reconocido de forma independiente en la propia Carta (artículo 8)[17].

Tras la entrada en vigor del Tratado de Lisboa, la **Carta** se ha convertido en la principal referencia para evaluar la conformidad del Derecho derivado de la UE respecto de los derechos fundamentales[18]. La jurisprudencia reiterada del TJUE establece respecto del CEDH que «éste no constituye, dado que la Unión no se ha adherido a él, un instrumento jurídico integrado formalmente en el ordenamiento jurídico de la Unión »[19]. En consecuencia, el TJUE afirma en su jurisprudencia reciente que la evaluación de la validez de una disposición de derecho derivado de la UE «*debe realizarse únicamente a la luz de los derechos fundamentales garantizados por la Carta*»[20].

Sin embargo, de conformidad con el apartado 3 del artículo 6 del TUE, el TJUE también ha recordado que las disposiciones específicas del CEDH deben tomarse en cuenta *«a efectos de la interpretación*» de las disposiciones correspondientes de la Carta[21]. En particular, el apartado 3 del artículo 6 del TUE establece que «*los derechos fundamentales que garantiza el Convenio Europeo para la Protección 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* ». Asimismo, la propia Carta exige que, en la medida en que contenga *«derechos que correspondan a derechos garantizados por el [CEDH], el sentido y el alcance de dichos derechos serán los mismos que los previstos por el [CEDH]*», mientras que el Derecho de la Unión puede ofrecer una protección más amplia (artículo 52, apartado 3, de la Carta).

Por un lado, el derecho al respeto de la vida privada del artículo 7 de la Carta se corresponde directamente con el artículo 8 del CEDH. Por otra parte, el derecho a la protección de los datos de carácter personal está formulado en la Carta, pero no en el CEDH y, por tanto, no figura entre los derechos que corresponden a un derecho protegido por el CEDH de conformidad con el apartado 3 del artículo 52 de la Carta[22]. Sin embargo, la nota explicativa del artículo 8 de la Carta señala que este derecho se ha basado, entre otros, en el artículo 8 del CEDH. Por lo tanto, la jurisprudencia del TEDH en virtud del artículo 8 del CEDH es pertinente, aunque no necesariamente concluyente, a la hora de evaluar si una limitación es conforme a la Carta[23]. También existe un diálogo constante entre el TJUE y el TEDH, observado en numerosas referencias en la jurisprudencia de cada uno de los tribunales[24].

Los criterios previstos en el apartado 2 del artículo 8 del CEDH y en el apartado 1 del artículo

52 de la Carta para una limitación legal del derecho al respeto de la vida privada son similares[25]. El apartado 2 del artículo 8 del CEDH establece, asimismo, que la limitación debe ser necesaria «en una sociedad democrática». Aunque el apartado 1 del artículo 52 no utiliza el mismo lenguaje, el elemento «sociedad democrática» está entrelazado en el ordenamiento jurídico de la UE, ya que se deriva de los valores fundamentales de la UE, entre los que se encuentra el respeto a la democracia (artículo 2 del TUE).

Por lo tanto, la principal referencia a la hora de evaluar la necesidad de medidas que limiten el ejercicio de los derechos garantizados por el artículo 8 de la Carta es el apartado 1 del artículo 52 de la Carta y la jurisprudencia del TJUE. Asimismo, los criterios del apartado 2 del artículo 8 del CEDH, y en concreto, la condición de que una limitación sea necesaria en una sociedad democrática[26], tal y como se interpreta en la jurisprudencia del TEDH, también deben tenerse en cuenta en el análisis.

4. Las medidas deben ser estrictamente necesarias

La jurisprudencia del TJUE aplica una evaluación de la *necesidad estricta* para cualquier limitación del ejercicio de los derechos a la protección de datos de carácter personal y al respeto de la vida privada en relación con el tratamiento de datos de carácter personal: «*las excepciones y limitaciones en relación con la protección de datos de carácter personal* ***deben aplicarse únicamente en la medida en que sean estrictamente necesarias****»*. El TEDH aplica una evaluación de la *necesidad estricta* en función del contexto y de todas las circunstancias existentes, como en el caso de las medidas secretas de control[27].

De la jurisprudencia del TJUE se desprende que la condición de la estricta necesidad es transversal, con independencia del ámbito de que se trate, como el sector policial o el comercial[28]. La exigencia de «estricta necesidad» se deriva del importante papel que el tratamiento de datos de carácter personal conlleva para una serie de derechos fundamentales, entre ellos la libertad de expresión. Incluso si se adoptan normas específicas en el ámbito de la aplicación de la ley, como por ejemplo la Directiva 2016/680[29], no se justifica una evaluación diferente de la necesidad.

El requisito de estricta necesidad tiene como consecuencia adicional que el control judicial de la medida también es estricto; es decir, la discrecionalidad del legislador a la hora de seleccionar la medida es limitada. Dicho esto, también se analizan las condiciones para un control judicial estricto de la discrecionalidad del legislador junto con la gravedad de la interferencia que una medida concreta podría causar[30]. Del mismo modo, el SEPD subrayó en el caso en curso sobre el proyecto de acuerdo PNR UE-Canadá que, debido al tratamiento sistemático y particularmente intrusivo de los datos de carácter personal que el acuerdo conlleva, el control judicial debe ser estricto[31].

5. Limitación de un derecho fundamental

La evaluación de la necesidad debe realizarse en los casos en que la medida legislativa propuesta implique el tratamiento de datos de carácter personal.

El TJUE evalúa las limitaciones al ejercicio de los derechos y libertades previstos en el Derecho de la UE sobre la base del apartado 1 del artículo 52 de la Carta. El Tribunal ha declarado que un acto «constituye una injerencia en el derecho fundamental a la protección de los datos de carácter personal garantizado por el artículo 8 de la Carta porque prevé el tratamiento de datos de carácter personal»[32]. Por tanto, en principio, cualquier operación de tratamiento de datos (como la recogida, el almacenamiento, el uso o la comunicación de

datos) prevista por la legislación supone una limitación del derecho a la protección de los datos de carácter personal, independientemente de que dicha limitación pueda estar justificada.

Asimismo, el TJUE ha sostenido en la gran mayoría de los casos relativos a actos legislativos que una operación de tratamiento limitaba tanto el derecho a la protección de los datos de carácter personal como el derecho al respeto de la vida privada[33]. El Tribunal de Justicia también ha declarado que para el establecimiento de una limitación «*carece de relevancia si la información en cuestión relativa a la vida privada tiene o no carácter sensible o que los afectados han sufrido algún tipo de inconveniente*»[34].

En lo que respecta al derecho al respeto de la vida privada consagrado en el artículo 8 del CEDH, la jurisprudencia del TEDH establece que el tratamiento de los datos de carácter personal puede limitar el derecho en función del contexto, como el carácter sensible de los datos o la forma en que se utilizan[35].

6. Conclusión: la necesidad en la normativa de protección de datos es un concepto basado en casos y hechos que requiere una evaluación por parte del legislador de la UE

Una medida propuesta debe estar respaldada por pruebas que describan el problema que se va a abordar con la medida, cómo este se abordará con la medida y por qué las medidas existentes o menos intrusivas no pueden abordarlo de forma suficiente.

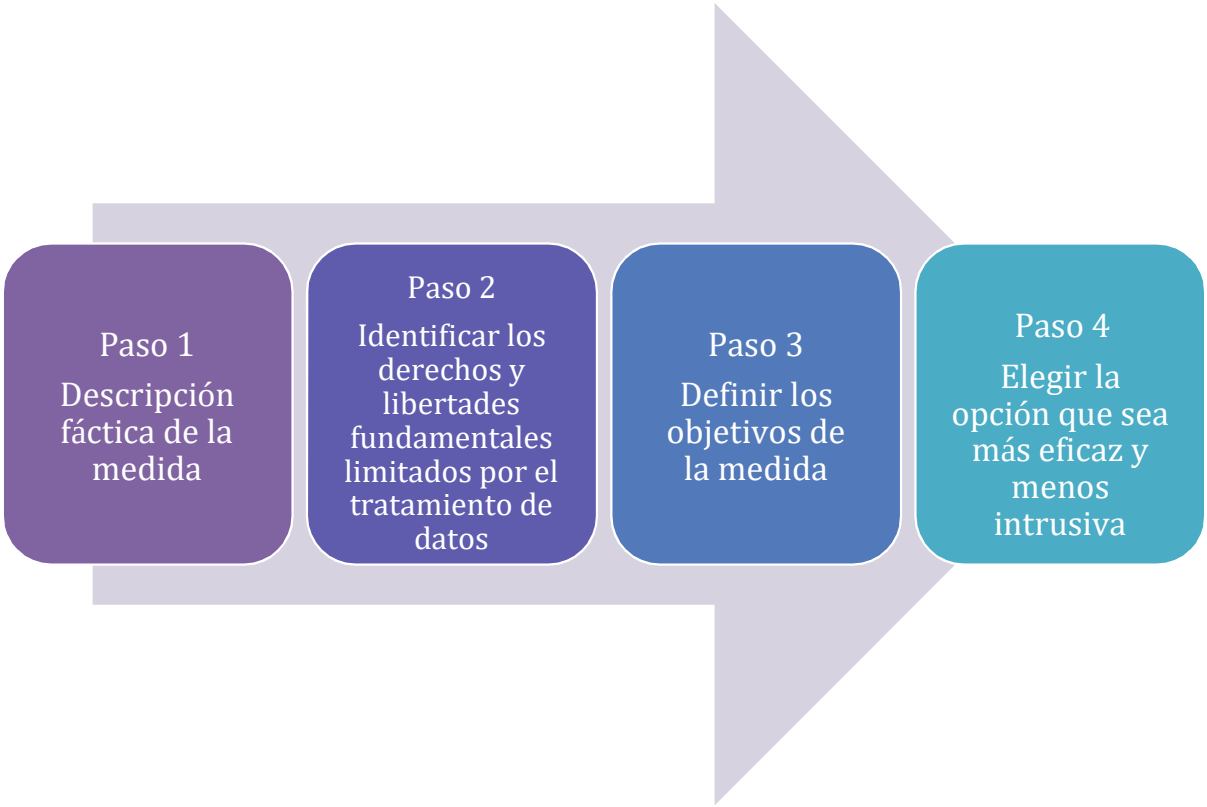
Un análisis de la jurisprudencia del TJUE y del TEDH indica que la necesidad en la normativa de protección de datos es un concepto basado en los hechos, más que una noción jurídica meramente abstracta, y que el concepto debe considerarse a la luz de las circunstancias específicas que rodean el caso, así como de las disposiciones de la medida y de la finalidad concreta que pretende alcanzar[36].

III. Lista de control para evaluar la necesidad de nuevas medidas legislativas

La lista de comprobación para evaluar la necesidad consta de cuatro pasos consecutivos. Cada paso corresponde a un conjunto de preguntas que facilitarán la evaluación de la necesidad.

- El **paso 1** es preliminar; requiere **una descripción fáctica detallada** de la medida propuesta y de 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 de carácter personal 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 necesidad de una medida;
- **El paso 4** proporciona **orientación sobre los aspectos específicos que deben abordarse** al realizar la evaluación de la necesidad, en particular que la medida debe ser **eficaz** y **lo menos intrusiva posible.**

Si la evaluación de cualquiera de los elementos detallados en los pasos 2 a 4 lleva a la conclusión de que una medida podría no cumplir con el requisito de la necesidad, la medida no debería proponerse o debería replantearse en función de los resultados del análisis.



Paso 1: Descripción fáctica de la medida propuesta

Una descripción detallada de la medida prevista no solo es un requisito previo a la evaluación de necesidad, sino que también ayuda a demostrar el cumplimiento de la primera condición del apartado 1 del artículo 52 de la Carta, es decir, la calidad de la ley.

Orientación

- La medida debe estar suficientemente descrita para permitir una clara comprensión de lo que se propone exactamente y para qué fin.
    - Es particularmente importante identificar con precisión qué implica la medida propuesta en términos de tratamiento de datos de carácter personal y cuál es el objetivo o los objetivos concretos de la medida.
    - Como se ha mencionado anteriormente (sección II.1), una medida mal definida puede afectar también a otros requisitos para una limitación legal de los derechos fundamentales e impediría la identificación de los derechos que pudieran verse afectados.

Cómo proceder

- **Describir la medida**
    - Establecer si la medida implica el uso de datos de carácter personal.
        - La **noción de datos de carácter personal** es muy amplia, ya que significa *«cualquier información relativa a una persona física identificada o identificable» («interesado»); una persona identificable es aquella que puede ser identificada, directa o indirectamente, en particular mediante un número de identificación* o por uno o varios factores específicos *de su identidad física, fisiológica, mental, económica, cultural o social»*[37]. Por consiguiente, un nombre, un apellido, una matrícula de un vehículo, un teléfono, un número de pasaporte, una dirección IP o cualquier otro identificador único se considerará un dato personal[38].
    - En caso de tratarse datos de carácter personal, describir:
        - el objetivo de interés general que persigue la medida;
        - la finalidad exacta del tratamiento de los datos personales, explicada con más detalle que el objetivo;
        - las categorías de datos;
        - las personas cuyos datos se tratan (por ejemplo, pasajeros, trabajadores, inmigrantes);
        - quién trata y accede a los datos (por ejemplo, una empresa privada o un organismo público);
        - qué operaciones de tratamiento están previstas (por ejemplo, recogida, almacenamiento, acceso, transferencia);
        - cualquier otra disposición pertinente, como la duración del tratamiento.

Ejemplos relevantes

EJEMPLO 1: Asesoramiento del SEPD *durante la consulta pública organizada por la Comisión en 2011 (véase Consejo de la Unión Europea, Doc 6370/13) sobre la Modificación de la propuesta de la Comisión COM (2011) 628 final/2 de Reglamento del Parlamento Europeo y del Consejo sobre la financiación, gestión y seguimiento de la Política Agrícola Común* (normas adoptadas para dar cumplimiento a la sentencia *Schecke* sobre la publicación de datos personales de los beneficiarios en el contexto de la Política Agrícola Común, actualmente Reglamento 1306/2013, en particular los artículos 111 - 113 y los considerandos 73 - 87)

«El SEPD señala que, para evaluar el cumplimiento de los requisitos de privacidad y protección de datos, es de crucial importancia contar con una finalidad clara y bien definida a la que la medida prevista pretende servir. ... Al comentar el objetivo de control, el representante del SEPD afirmó que la Comisión debía ser clara en cuanto a si el objetivo de la medida incluía también permitir cierta forma de control público sobre el gasto de los fondos de la UE por parte de los receptores como tales, para lo cual sería indispensable la revelación de la identidad de los receptores. Sin embargo, si el objetivo hace únicamente referencia al control público sobre las instituciones de la UE y sobre cómo se gasta el presupuesto de la UE, no resulta tan obvio que la identidad de los beneficiarios deba hacerse al pública...».

Paso 2: Identificación de los derechos y libertades fundamentales limitados por el tratamientode datos personales

Orientación

- Si la medida propuesta implica el tratamiento de datos personales, esta supondrá una limitación del derecho a la protección de datos personales en virtud del apartado 1 del artículo 52 de la Carta.

- Dependiendo de la naturaleza de los datos y del uso que se haga de los mismos, la medida propuesta también podrá limitar el derecho al respeto de la vida privada (también llamado derecho a la intimidad) (véase la sección II.5).

- A este respecto, la jurisprudencia reiterada del TJUE establece que «para determinar la existencia de una injerencia en el derecho fundamental al respeto de la vida privada, **carece de relevancia si la información tiene o no carácter sensible o si los afectados han sufrido algún tipo de inconveniente**»[39].

- Asimismo, el TEDH ha sostenido en repetidas ocasiones que el **almacenamiento por parte de una autoridad pública de datos** relativos a la vida privada de una persona equivale a una limitación del derecho al respeto de su vida privada[40], independientemente del uso que se haga de estos[41].

- Las operaciones de tratamiento distintas o el conjunto de operaciones (es decir, la recogida y otras operaciones, como la conservación o la transferencia o el acceso a los datos) pueden constituir limitaciones independientes del derecho a la protección de los datos de carácter personal y, en su caso, del derecho al respeto de la vida privada. Por ejemplo, el TJUE ha establecido que, si la medida implica el **acceso de las autoridades nacionales competentes** a los datos tratados, dicho acceso constituirá una nueva injerencia en el derecho fundamental al respeto de la vida privada[42].

- La negativa a permitir que el interesado tenga la oportunidad de refutar los datos almacenados y a los que se ha accedido (es decir, el derecho a acceder y rectificar los datos) también equivale a una limitación de su derecho al respeto de la vida privada[43].

  Otros derechos y libertades pueden verse afectados por la medida propuesta, independientemente del uso de los datos de carácter personal, lo que da lugar a un análisis posterior. Por ejemplo, podría verse afectado el derecho a la tutela judicial efectiva[44], el derecho a la no discriminación[45] o el derecho a la libertad de expresión[46].

- De conformidad con el apartado 1 del artículo 52 de la Carta, **deberá respetarse** la «**esencia**» o el contenido básico **del derecho** (véase la sección II.1). Esto significa que la limitación no podrá ir tan lejos como para vaciar el derecho de sus elementos fundamentales y acabar impidiendo así el ejercicio de este.

Cómo proceder

- **Determinar si la medida propuesta implica de alguna manera el uso de datos de carácter personal. Si es el caso, describir:**
  - Qué tipo de operaciones de tratamiento se prevé realizar *(*por ejemplo: recogida, almacenamiento, comunicación, transferencia, etc.);
  - Quién está tratando los datos *(*por ejemplo: entidades privadas, entidades públicas, organizaciones, autoridades competentes, determinados particulares, etc.);
  - Quién tiene acceso a los mismos;
  - Durante cuánto tiempo se almacenan los datos[47];
  - Las circunstancias en las que se utiliza la información personal *(*por ejemplo: de forma sistemática, solo en determinados casos, durante un periodo de tiempo limitado, etc.);
  - Con quién se relacionan los datos *(*por ejemplo: determinadas categorías de personas, usuarios de un servicio, sospechosos de un delito, extranjeros, nacionales, etc.).
- **Identificar qué derechos y libertades fundamentales se ven limitados**
  - Debemos plantearnos en qué medida el tratamiento de datos limita el derecho al respeto de la vida privada;
  - Identificar una posible «diferencia de trato» creada entre las personas que pudiera dar lugar a una discriminación;
  - Evaluar las consecuencias sobre la posibilidad de que las personas emprendan acciones judiciales;
  - Evaluar en qué medida la libertad de expresión, la libertad de pensamiento, la libertad de recibir información se ven limitadas
  - Evaluar si la esencia o el contenido básico de los derechos se ven limitados.

Resultado

- **Cuando se vea afectado un derecho**, el mero hecho de que una medida limite el ejercicio de estos derechos no significa como tal que la medida no deba proponerse. No obstante, la medida deberá cumplir las condiciones previstas en el apartado 1 del artículo 52 de la Carta, incluida la necesidad.

- Si la **esencia del derecho** se viera afectada negativamente por la medida, la limitación no será legal y la medida deberá retirarse o modificarse antes de pasar a los siguientes pasos (véase la sección I.1).

Ejemplos relevantes

EJEMPLO 2: *Huber* (TJUE, asunto C-362/14)

El Tribunal evaluó la legalidad de una base de datos creada por las autoridades alemanas, que incluía datos de carácter personal de ciudadanos de nacionalidades de terceros países y otros ciudadanos de la UE que no tenían nacionalidad alemana. Una de las conclusiones del Tribunal fue que el derecho a la no discriminación entre nacionales de la UE «*procede interpretarlo en el sentido de que se opone a que un Estado miembro instaure, en aras de combatir la delincuencia, un sistema de tratamiento de datos de carácter personal específico para los ciudadanos de la Unión que no sean nacionales de dicho Estado miembro*» (apartado 81). Para llegar a esta conclusión, el Tribunal tuvo en cuenta que la lucha contra la delincuencia «*tiene necesariamente por objeto la persecución de los crímenes y delitos cometidos, con independencia de la nacionalidad de sus autores*» (párrafo 78). « *Así pues, a efectos del objetivo de combatir la delincuencia, para un Estado miembro la situación de sus nacionales no puede ser diferente de la de los ciudadanos de la Unión que no sean nacionales suyos y residan en su territorio*» (apartado 79).

EJEMPLO 3: Dictamen 3/2016 del SEPD *sobre el intercambio de información sobre nacionales de terceros países en relación con el Sistema Europeo de Información de Antecedentes Penales (ECRIS),* 13.4.2016

La propuesta legislativa pretende crear un sistema especial de intercambio de información entre los Estados miembros sobre las condenas de los nacionales de terceros países, que también contendría datos sobre los nacionales de la UE que tengan la nacionalidad de un tercer país. Por consiguiente, recibirían un trato diferente al de los nacionales de la UE que no ostenten la nacionalidad de un tercer país. El SEPD consideró que *«la diferencia de trato prevista en la propuesta no parece necesaria para alcanzar el objetivo perseguido, considerando que para los nacionales de la UE pueden aplicarse los procedimientos existentes del ECRIS para que las autoridades compartan la información*» y que *«esta diferencia de trato podría dar lugar a una discriminación, que infringiría el artículo 21, apartado 1, de la Carta de la UE*» (apartado 33).

EJEMPLO 4: *Rechnungshof* (TJUE, asuntos acumulados C-465/00, C-138/01 y C-139/01)

El Tribunal consideró que « *la mera memorización, por el empresario, de datos nominales relativos a las retribuciones abonadas a su personal no puede, como tal, constituir una injerencia en la vida privada*». Sin embargo, el Tribunal consideró que « *la comunicación de tales datos a un tercero, en el caso de autos, a una autoridad pública, lesiona el derecho al respeto de la vida privada de los interesados*» (apartado 74).

EJEMPLO 5: *Schecke* (TJUE, asuntos acumulados C-92/09 y C-93/09)

La publicación en internet de los nombres y los importes recibidos por los beneficiarios de fondos públicos constituye una limitación de su vida privada en el sentido del artículo 7 de la Carta (apartado 58).

EJEMPLO 6: *Digital Rights Ireland* (TJUE, asuntos acumulados C-293/12 y C-594/12)

En el caso de la Directiva de conservación de datos, el Tribunal consideró que la obligación impuesta a los proveedores de servicios de comunicaciones electrónicas disponibles al público o de redes públicas de comunicaciones de conservar, durante un periodo de 6 meses a dos años, los datos de las comunicaciones, como la línea telefónica que llama y la que recibe la llamada, las direcciones de correo electrónico, las direcciones IP utilizadas para acceder a Internet, «*constituye en sí misma una injerencia en los derechos garantizados por el artículo 7 de la Carta*» (apartado 34). «*El acceso de las autoridades nacionales competentes a los datos constituye una injerencia adicional en ese derecho fundamental*» (apartado 35). El Tribunal consideró asimismo que la «Directiva 2006/24 constituye una injerencia en el derecho fundamental a la protección de datos de carácter personal garantizado por el artículo 8 de la Carta puesto que establece un tratamiento de datos de carácter personal» (apartado 36).

Paso 3: Definir los objetivos de la medida

Orientación

- De conformidad con el apartado 1 del artículo 52 de la Carta, la medida **debe cumplir realmente:**
  - **un objetivo de interés general reconocido por la Unión o**
  - **la necesidad de proteger los derechos y libertades.**
- Los **objetivos de interés general de la Unión** incluyen, por ejemplo, los objetivos generales mencionados en los artículos 3 o 4 (2) del TUE y otros intereses protegidos por disposiciones específicas de los tratados[48], así como interpretados en la jurisprudencia del Tribunal de Justicia.
  - El artículo 23 del Reglamento General de Protección de Datos 2016/679 incluye una lista de objetivos que se consideran legítimos para limitar los derechos de las personas, como el derecho de acceso a los datos de carácter personal, y las obligaciones del responsable del tratamiento.
  - La transparencia y el control público también son objetivos legítimos (artículos 1 y 15.1 del TUE) que permiten al ciudadano participar de forma más estrecha en el proceso de toma de decisiones[49].
- Los **derechos de terceros** son, en primer lugar, los consagrados en la Carta. El derecho a la protección de los datos de carácter personal puede tener que equilibrarse con otros derechos, como la protección de los derechos de propiedad intelectual y el derecho a la tutela judicial efectiva, la libertad de expresión y de empresa[50].
- Aunque la descripción de la medida es independiente de la evaluación de la necesidad, es un requisito previo para la aprobación de la misma, ya que esta debe evaluarse en relación con el objetivo o los objetivos que se persigan.
  - el **problema al que se dirige la medida**, es *decir*, debe especificarse la finalidad del tratamiento de los datos de carácter personal. Esto es aún más importante

cuando un objetivo de interés general puede abarcar varios aspectos o una medida debe abordar varios objetivos de interés general. Por ejemplo, se podrá considerar que el objetivo de salvaguardar la seguridad pública abarca tanto la seguridad interior como la exterior[51], por lo que una medida determinada deberá indicar claramente si pretende abordar una de estas nociones de seguridad o todas ellas.

- El problema que se va a tratar debe ser concreto y no meramente hipotético. Para ello, deberán aportarse **pruebas objetivas del problema.** Las pruebas pueden consistir en hechos o datos estadísticos, y deben permitir la verificación científica y apoyar de forma convincente la existencia del problema.

- Para el TEDH, una **limitación se considerará «necesaria en una sociedad democrática»** para un fin legítimo «si responde a una **necesidad social apremiante».** El problema que se pretende tratar no solo debe ser real, presente o inminente, sino crítico para el funcionamiento de la sociedad.

- Si una medida persigue más de un objetivo, se deberá justificar cada uno de ellos[52].

Cómo proceder

- **Identificar y evaluar la legitimidad del objetivo que persigue la medida:**
  - Asegurarse de que el problema se describe de forma suficiente y clara en la medida;
  - Integrar pruebas suficientes y científicamente verificables que apoyen la existencia del problema;
  - Definir con precisión el objetivo de interés general o el derecho de terceros que la medida pretende abordar;
  - Asegurarse de que la finalidad del tratamiento de los datos de carácter personal persigue realmente un objetivo de interés general reconocido por la Unión o la necesidad de proteger los derechos y libertades de terceros;
  - Explicar la importancia del objetivo que se pretende alcanzar y su importancia para el funcionamiento de la sociedad.

Resultado

- **Si el problema que se quiere tratar no está suficientemente descrito**, deberá explicarse y desarrollarse mejor. En caso contrario, no será posible evaluar la necesidad de la medida.

- **Si el problema no se ve respaldado con pruebas suficientes**, deberán buscarse buscar más pruebas.

- **Si la medida no responde realmente a un objetivo de interés general reconocido por la Unión o a la necesidad de proteger los derechos y libertades de terceros**, no deberá proponerse.

- **Si la medida cumple ese objetivo** debidamente apoyado en las pruebas pertinentes, el análisis podrá pasar a evaluar la necesidad de la medida según el paso

Ejemplos relevantes

EJEMPLO 7: *Digital Rights Ireland* (TJUE, asuntos acumulados C-293/12 y C-594/12)

Al evaluar la legalidad de la Directiva de conservación de datos (Directiva 2006/24), el TJUE tuvo en cuenta las conclusiones del Consejo de Justicia de Asuntos de Interior de 19 de diciembre de 2002, según las cuales los datos relacionados con el uso de las comunicaciones electrónicas son particularmente importantes y, por tanto, un instrumento valioso en la prevención de delitos y en la lucha contra la delincuencia, en particular la organizada, debido al importante aumento de las posibilidades que ofrecen las comunicaciones electrónicas (apartado 43). El TJUE también reconoció que en su jurisprudencia consideró que la lucha contra el terrorismo internacional para mantener la paz y la seguridad internacionales constituye un objetivo de interés general. Lo mismo ocurre con la lucha contra los delitos graves para garantizar la seguridad pública (apartado 42). De este modo, el Tribunal de Justicia consideró que «*la conservación de datos para su eventual acceso por parte de las autoridades nacionales competentes que impone la Directiva 2006/24 responde efectivamente a un objetivo de interés general*» (apartado 44).

EJEMPLO 8: *Promusicae* (TJUE, asunto C-275/06)

El TJUE sostiene que la protección del derecho a la propiedad intelectual es un objetivo legítimo para el tratamiento de los datos de las comunicaciones (direcciones IP) por referencia al artículo 13 de la Directiva 95/46/CE, que establece los objetivos legítimos para las limitaciones del derecho al respeto de la vida privada en relación con el tratamiento de los datos personales (apartados 26).

EJEMPLO 9: Dictamen del SEPD, de 9 de octubre de 2012, *sobre la modificación de la propuesta de la Comisión COM (2011) 628 final/2 de Reglamento del Parlamento Europeo y del Consejo sobre la financiación, gestión y seguimiento de la Política Agrícola* Común (normas adoptadas para dar cumplimiento a la sentencia Schecke sobre la publicación de datos personales de los beneficiarios en el contexto de la Política Agrícola Común, actualmente ahora Reglamento 1306/2013, en particular los artículos 111 - 113 y los considerandos 73 - 87)

Si bien el SEPD reconoció que la transparencia y el control público son objetivos de interés general, de conformidad con lo previsto en la sentencia *Schecke* (apartados 65, 68, 69 y 75), el problema de la reducción de los controles y las comprobaciones sobre el terreno por parte de las autoridades como consecuencia de las limitaciones económicas no puede incluirse en dicho objetivo «*... la transparencia y el control público son objetivos legítimos por sí mismos... y no pueden presentarse como un sustituto de los controles específicos y las comprobaciones sobre el terreno por parte de las autoridades competentes*» (párrafo 17).

EJEMPLO 10: Dictamen 3/2016 del SEPD *sobre el intercambio de información sobre nacionales de terceros países en relación con el Sistema Europeo de Información de Antecedentes Penales (ECRIS)*

El SEPD consideró que la propuesta del ECRIS de la Comisión de facilitar el acceso a las condenas de nacionales de terceros países entraba en el ámbito de la lucha contra el terrorismo y la lucha contra la delincuencia más grave para garantizar la seguridad pública, que se reconocen como objetivos de interés general en la legislación de la UE. «Así, *las medidas propuestas, responden a un objetivo de interés general y pueden estar justificadas desde la perspectiva del principio de proporcionalidad*» (apartado 9).

Paso 4: Elegir la opción que sea más eficaz y menos intrusiva

En la sección II.2 señalamos que la *idoneidad* de una medida no es lo mismo que su *eficacia*. Aunque resulte apropiada, la medida elegida debe ser también eficaz y menos intrusiva que otras opciones para lograr el mismo objetivo.

Una medida adecuada es aquella capaz de alcanzar el objetivo perseguido:

- Deberá existir **un vínculo lógico entre la limitación y** los objetivos legítimos identificados;
- El objetivo perseguido deberá alcanzarse como consecuencia directa de la medida;
- No obstante, una medida adecuada no tiene por qué abordar todos los aspectos particulares del problema[53].

Orientación sobre la eficacia y el carácter intrusivo

- **La medida deberá ser realmente eficaz**, es decir, esencial para lograr el objetivo de interés general que se persigue.
  - No todo lo que «puede resultar útil» para un determinado fin es «deseable o puede considerarse una medida necesaria en una sociedad democrática»[54]. No basta la mera conveniencia o rentabilidad[55].
  - Las categorías seleccionadas de personas afectadas, las categorías de datos de carácter personal recogidos y tratados, el período de almacenamiento de los datos, etc., deberán contribuir de forma eficaz a lograr el objetivo perseguido.
  - Si la medida propuesta incluye el tratamiento de **datos sensibles**, deberá aplicarse un umbral más alto en la evaluación de la eficacia.
    - Los datos sensibles incluyen, entre otros, los que revelen: el origen étnico o racial, las opiniones políticas, las creencias religiosas o similares y el estado de salud. Los datos relativos a las condenas e infracciones penales tienen un estatus similar[56]. Los datos genéticos y biométricos son reconocidos como datos sensibles por los nuevos instrumentos jurídicos de protección de datos de carácter personal[57]. No obstante, el Grupo de Trabajo del Artículo 29 ya destacó en varias ocasiones la «sensibilidad» de estos datos[58].
    - Otras categorías de datos, aunque no estén estrictamente clasificadas como sensibles, en determinados contextos pueden presentar un mayor riesgo para el titular y provocar la aplicación de un umbral más alto de lo estrictamente necesario. Es el caso, por ejemplo, de los identificadores únicos, como los números de identificación nacional o los datos financieros.
- La medida prevista deberá ser **la menos intrusiva para los derechos en juego.**
  - Deberán identificarse medidas alternativas que supongan una menor amenaza para el derecho a la protección de los datos de carácter personal y el derecho al respeto de la vida privada.
  - Una medida alternativa puede consistir en una combinación de medidas.

- Las alternativas deben ser reales, suficientes y comparativamente eficaces en relación con el problema a tratar[59].

- La imposición de una limitación solamente a una parte de la población/área geográfica será menos intrusiva que una imposición a toda la población/área geográfica; una limitación a corto plazo es menos intrusiva que a largo plazo; el tratamiento de una categoría de datos es en general menos intrusivo que el tratamiento de más categorías de datos[60].

- El ahorro de recursos no deberá repercutir en las medidas alternativas; este aspecto deberá evaluarse dentro del análisis de proporcionalidad, ya que requiere el equilibrio con otros objetivos de interés público que compiten entre sí (véase la sección II.2).

- **Cada aspecto particular** de la medida estará sujeto a la prueba de necesidad estricta.

  - Algunas disposiciones específicas, como el tratamiento de una categoría de datos de carácter personal, las categorías de personas afectadas, la duración de la conservación de los datos, pueden resultar necesarias, pero otras no. La evaluación dependerá de «normas claras y precisas que regulen su alcance y aplicación»[61]. Como se menciona en la sección II.1, las normas claras y precisas son importantes también para cumplir con la mayoría de los demás criterios del apartado 1 del artículo 52 de la Carta.
  - Si la medida implica el acceso de las autoridades a los datos, esta deberá establecer **criterios objetivos**, en particular limitando el número de personas autorizadas a acceder y utilizar los datos a lo estrictamente necesario[62].

  - La medida deberá **diferenciar**, **limitar** y **someter a excepciones** a las personas cuya información se utilice en función del objetivo buscado[63].

  - Al establecer **un periodo de conservación** de los datos, la medida deberá **distinguir entre las categorías de datos** en función de su **contribución efectiva** a los fines perseguidos y deberá utilizar criterios objetivos para la determinación de la duración del periodo de conservación[64].

  - La limitación del **derecho a la información** sobre el tratamiento de los datos de carácter personal también deberá ser necesaria para la finalidad que persigue la medida propuesta. Por ejemplo, la finalidad de las medidas de vigilancia secreta puede justificar la restricción de la notificación a las personas afectadas. «*Tan pronto como pueda darse la información sin poner en peligro la finalidad de la medida tras el cese de la medida de vigilancia, la información deberá, no obstante, facilitarse a las personas afectadas*»[65].

- **Las razones por las que es necesario actuar** deberán detallarse en la medida, explicando:

  - por qué las medidas existentes son insuficientes para abordar el problema;

  - por qué las medidas alternativas, menos intrusivas, son insuficientes para resolver el problema;

  - por qué la medida propuesta puede abordar el problema **con mayor eficacia que otras medidas**;

- Deberán aportarse pruebas objetivas de todo lo anterior, incluidos hechos o datos estadísticos, susceptibles de verificación científica, que apoyen de forma convincente la medida propuesta;

- No será necesario aplicar la evaluación de la necesidad a cada estado miembro por separado, aunque sí será pertinente para la evaluación del impacto que considera el valor añadido de la intervención de la UE[66].

Cómo proceder

- **Describir cómo y por qué la medida es esencial para satisfacer la necesidad que debe abordarse:**
  - Por qué las medidas existentes son insuficientes para abordar el problema;
  - Por qué y cómo la medida puede lograr el objetivo.
- **Considerar si otras medidas menos intrusivas podrían ser comparativamente eficaces para alcanzar el objetivo buscado.**
- Aportar pruebas científicamente verificables que puedan respaldar realmente la afirmación de que las medidas existentes y las medidas alternativas menos intrusivas no pueden abordar eficazmente el problema.

Resultado

- **Considerar la aplicación adecuada de las medidas existentes en lugar de nuevas medidas intrusivas.**
- **Considerar una medida alternativa de eficacia comparable, pero con menor impacto sobre la protección de los datos de carácter personal o el derecho al respeto de la vida privada.** Los aspectos de los costes más elevados pueden analizarse en la propia evaluación de la proporcionalidad.
- **Solo si no se dispone de medidas existentes o menos intrusivas según** un análisis basado en pruebas, y únicamente si dicho análisis demuestra que la medida prevista es **esencial y se limita a lo absolutamente necesario** para lograr el objetivo de interés general, esta medida deberá someterse a la evaluación de la proporcionalidad (véase la sección II.2).

Ejemplos relevantes

EJEMPLO 11: Österreichischer Rundfunk y otros (TJUE, asuntos acumulados C-465/00, C-138/01 y C-139/01)

A la hora de evaluar si la publicación de los nombres junto con los ingresos de los empleados de diferentes organismos públicos que estaban sujetos al control del Tribunal de Cuentas era conforme con el derecho a la vida privada, el TJUE instó a los tribunales nacionales a analizar si el objetivo perseguido por dicha publicación «*podría haberse alcanzado con la misma eficacia mediante la transmisión de datos nominales únicamente a los organismos de control*» (apartado 88).

EJEMPLO 12: Schecke (TJUE, asuntos acumulados C-92/09 y C-93/09, 9.11.2010)

Al analizar la necesidad de la publicación de los datos personales de todos los beneficiarios que reciben fondos públicos, el Tribunal destacó que el legislador no tuvo en cuenta medidas alternativas menos intrusivas, como limitar la publicación a los beneficiarios en función de los periodos en los que recibieron la ayuda, o la frecuencia o la naturaleza y el importe de la ayuda recibida. El Tribunal también subrayó que podría lograrse un enfoque menos intrusivo mediante una combinación de esas medidas: «*Dicha publicación limitada por nombres podría ir acompañada, en su caso, de la información pertinente sobre otras personas físicas que se beneficiaran de las ayudas del FEAGA y del FEADER y de los importes que hubieran recibido*». El Tribunal de Justicia concluyó que «*teniendo en cuenta que las excepciones y limitaciones en materia de protección de datos personales únicamente deben aplicarse en la medida en que sea estrictamente necesario (sentencia Satakunnan Markkinapörssi y Satamedia, anteriormente citada, apartado 56) y que es posible prever medidas que afecten de forma menos negativa a dicho derecho fundamental de las personas físicas y que sigan contribuyendo de forma eficaz a los objetivos de la normativa de la Unión Europea en cuestión...*». (apartados, 81, 82, 83, 86).

EJEMPLO 13: Tele2 Sverige AB (TJUE, asuntos acumulados C-203/15 y C-698/15)

En sus conclusiones, el Abogado General volvió a afirmar que «a *la vista de la exigencia de estricta necesidad, resulta obligado que dichos órganos jurisdiccionales no se contenten con comprobar simplemente la utilidad de una obligación general de conservar datos, sino que comprueben estrictamente que ninguna otra medida o combinación de medidas, en particular, una obligación de conservar determinados datos relativos a grupos o personas concretos, acompañada de otras herramientas de investigación pueda ofrecer la misma eficacia en la lucha contra los delitos graves. Debo subrayar, a este respecto, que varios estudios presentados al Tribunal de Justicia cuestionan la necesidad de este tipo de obligación a efectos de la lucha contra los delitos graves*». Estas otras medidas deberán ser eficaces para el objetivo que se persigue. «*En efecto, tales obligaciones pueden tener una amplitud material más o menos grande, en función de los usuarios, de las zonas geográficas y de los medios de comunicación de que se trate*» (apartados 209, 211).

El TJUE sostuvo que una conservación selectiva podía estar justificada siempre que esta se limitara a lo estrictamente necesario para el objetivo de la lucha contra la delincuencia grave: «*... la conservación selectiva de datos de tráfico y de localización, con el fin de luchar contra la delincuencia grave, [debería] limitarse, en lo que respecta a las categorías de datos que deban conservarse, los medios de comunicación afectados, las personas afectadas y el período de conservación adoptado, a lo estrictamente necesario*». Además, «*la legislación nacional debe basarse en pruebas objetivas que permitan identificar a un público cuyos datos puedan revelar un vínculo, al menos indirecto, con infracciones penales graves, y contribuir de un modo u otro a la lucha contra la delincuencia grave o a la prevención de un riesgo grave para la seguridad pública*». *Dichos límites podrán establecerse siguiendo un criterio geográfico cuando las autoridades nacionales competentes consideren, sobre la base de pruebas objetivas, que existe, en una o varias zonas geográficas, un alto riesgo de planificación o comisión de dichos delitos.*» El Tribunal también sostuvo que el acceso a dichos datos por parte de las autoridades competentes debe basarse en criterios objetivos y, como regla general, solo a los datos de los sospechosos. Como excepción, «*... cuando, por ejemplo, los intereses vitales de la seguridad nacional, la defensa o la seguridad pública se vieran amenazados por actividades terroristas, también podría concederse el acceso a los datos de otras personas cuando existan pruebas objetivas de las que pudiera deducirse que dichos datos podrían contribuir de manera eficaz, en un caso concreto, a la lucha contra dichas actividades*» (Apartados 102, 103, 108, 111, 115, 119).

EJEMPLO 14: Dictamen del GC 1/15 (Solicitud de dictamen presentada por el Parlamento Europeo) sobre el Proyecto de Acuerdo entre Canadá y la UE sobre la transferencia y el tratamiento de los registros de nombres de pasajeros

En lo que respecta a la estricta necesidad de la medida, el Abogado General subraya que los términos del Proyecto de Acuerdo sobre los registros de nombres de pasajeros «deben consistir en las medidas menos perjudiciales para los derechos reconocidos por los artículos 7 y 8 de la Carta, a la vez que contribuyen de manera eficaz al objetivo de seguridad pública perseguido por el acuerdo previsto. Dichas medidas alternativas deben ser también suficientemente eficaces;

es decir, su eficacia debe (...) ser comparable a la de las medidas previstas en el acuerdo en cuestión, para alcanzar el objetivo de seguridad pública perseguido por dicho acuerdo». En relación con esta evaluación de la necesidad, el Abogado General analiza diversos aspectos de la medida, tales como «las categorías de datos que figuran en el anexo del acuerdo deberían redactarse de forma más concisa y precisa, sin que pueda dejarse margen de apreciación alguno ni a los transportistas aéreos ni a las autoridades competentes canadienses en cuanto al alcance concreto de tales categorías». «Esta observación hace pensar, a falta de una explicación más fundamentada en el acuerdo previsto sobre la estricta necesidad de tratar los datos sensibles, que el objetivo de lucha contra el terrorismo y contra los delitos graves de carácter transnacional puede alcanzarse de forma igualmente eficaz sin que tales datos sean siquiera transferidos a Canadá» «... para limitar a lo estrictamente necesario los delitos por los que pueda autorizarse el tratamiento de datos del PNR y para garantizar la seguridad jurídica de los pasajeros cuyos datos se transmitan a las autoridades canadienses, considero que los delitos incluidos en la definición del artículo 3, apartado 3, del acuerdo previsto deberían estar enumerados taxativamente...». En lo que respecta a la duración de la conservación, el Abogado General declaró que «el acuerdo previsto no indica las razones objetivas que impulsaron a las partes contratantes a ampliar el período de conservación de los datos del PNR a cinco años como máximo». (Apartados 205, 220, 222, 235, 261, 267).

EJEMPLO 15: Dictamen del SEPD sobre la Propuesta de Directiva del PE y del Consejo sobre la utilización de datos de los registros de nombres de pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves, 25.03.2011.

El SEPD indicó que la evaluación de impacto de la directiva propuesta incluía amplias explicaciones y estadísticas para justificar la medida, pero que estos elementos no resultaban convincentes. A modo de ejemplo, la descripción de la amenaza del terrorismo y la delincuencia grave en la evaluación de impacto y en la exposición de motivos de la propuesta citaba el número de 14 000 infracciones penales por cada 100 000 habitantes en los estados miembros en 2007. Aunque esta cifra resulta impresionante, se refiere a tipos indiferenciados de delitos y no puede servir de apoyo para justificar una medida destinada a combatir únicamente un tipo limitado de delitos graves y transnacionales y el terrorismo. Otro ejemplo sería el hecho de que citar un informe sobre «problemas» de drogas sin vincular las estadísticas al tipo de tráfico de estupefacientes al que se refiere la directiva propuesta no constituía, en opinión del SEPD, una referencia válida (apartado 11). El SEPD llegó a la conclusión de que la documentación de referencia no resultaba pertinente ni precisa para demostrar la necesidad del instrumento (apartado 12).

EJEMPLO 16: Dictamen 7/2010 del Grupo de Trabajo del Artículo 29 sobre la Comunicación de la Comisión Europea relativa al enfoque global de las transferencias de datos de los registros de nombres de los pasajeros a terceros países, 12.11.2010

Al evaluar la necesidad de las transferencias de datos de los registros de nombres de pasajeros a terceros países, el Grupo de Trabajo del Artículo 29 aconsejó a la Comisión que *«evalúe si la solicitud de datos de pasajeros de terceros países podía satisfacerse a través de estos sistemas y mecanismos (ya existentes), antes de celebrar nuevos acuerdos*». El Grupo de Trabajo también destacó que *«deben plantearse cuidadosamente las opciones alternativas antes de establecer un sistema de este tipo, en vista del carácter intrusivo de las decisiones adoptadas, al menos en gran parte, de forma automatizada sobre la base de patrones estándar, y a la luz de las dificultades de los interesados para oponerse a tales decisiones»* (página 4).

JEMPLO 17: Dictamen 3/2016 del SEPD Dictamen sobre el intercambio de información sobre nacionales de terceros países en relación con el Sistema Europeo de Información de Antecedentes Penales (ECRIS), 13.04.2016

La propuesta legislativa analizada consagra la obligación de que los Estados miembros incluyan en el ECRIS los datos biométricos (huellas dactilares) de todos los nacionales de terceros países condenados, argumentando que resulta necesario a efectos de identificación. El SEPD pidió más pruebas que demostraran la necesidad de almacenar las huellas dactilares*: «Por consiguiente, no se puede considerar que no haya otra manera de garantizar la identificación de las personas que utilizar las huellas dactilares y, por tanto, deberá demostrarse la necesidad del uso obligatorio de las huellas dactilares para el TCN en el ECRIS»* (apartado 15).

EJEMPLO 18: Dictamen 5/2015 del SEPD Segundo dictamen sobre la propuesta de Directiva sobre el uso de los registros de nombres de los pasajeros

El SEPD subrayó que «*de acuerdo con los elementos disponibles, las últimas versiones de la Propuesta no muestran que se haya realizado una evaluación adecuada, de conformidad con las sentencias del TJCE, sobre las lagunas existentes en la lucha contra el terrorismo y las posibles formas de abordarlas con los instrumentos existentes a disposición de los estados miembros. Si bien esta evaluación debería referirse también a los nuevos enfoques de investigación para vigilar de forma más eficaz a los sospechosos conocidos por parte de las autoridades policiales y judiciales, varios acontecimientos recientes en la UE demuestran la existencia de lagunas en materia de inteligencia no relacionadas con los pasajeros aéreos, y que dirigir los recursos e intensificar los esfuerzos a los sospechosos conocidos sería en determinados casos más eficaz que elaborar perfiles por defecto de millones de viajeros*». (párrafo 14).

EJEMPLO 19: Carta del Grupo de Trabajo del Artículo 29 a la Comisión LIBE sobre los
registros de nombres de los pasajeros de la UE, 19.3.2015

El artículo 29 subraya que la necesidad de los registros de nombres de los pasajeros de la UE debe justificarse; es decir, por qué los instrumentos existentes (SIS, API) no son suficientes, por qué otras alternativas menos intrusivas no lograrían el objetivo, hasta qué punto son los registros de nombres de los pasajeros de la UE la solución para lograr el objetivo en comparación con otras medidas menos intrusivas. Las explicaciones deben estar respaldadas por pruebas, posiblemente estadísticas, por estudios de la UE o de los estados miembros.

EJEMPLO 20: Dictamen 07/2016 del SEPD sobre el primer paquete de reformas del sistema europeo común de asilo (Eurodac, OEAA y reglamentos de Dublín)

El SEPD hizo hincapié en que la necesidad de añadir una segunda categoría de datos biométricos, es decir, imágenes faciales, en una base de datos a gran escala debe basarse en «*... una evaluación (...) que se base en un estudio coherente o en un enfoque basado en pruebas*». En lo que respecta al período de conservación, el SEPD estableció que aumentar el período de conservación a cinco años para que esté en línea con lo que establecen otros instrumentos «*no es pertinente como tal, ya que estos instrumentos pueden tener otros fines y su período de conservación podría estar justificado por otros elementos*». En su dictamen, el SEPD consideró que el período de conservación de cinco años no está suficientemente justificado, y recomendó que se aportaran más pruebas (apartados 22, 30 y 31).

Notas

[1] El artículo 2 del Tratado de la Unión Europea (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 personas pertenecientes a minorías*». Además, el artículo 6.1 del TUE reconoce los derechos, libertades y principios recogidos en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, adaptada en Estrasburgo el 12 de diciembre de 2007, que tiene el mismo valor jurídico que los tratados, y el artículo 6.3 del TUE establece que «*los derechos fundamentales que garantiza el Convenio Europeo para la Protección 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* ».

[2] La intención del SEPD de publicar este manual se anunció a la Comisión de Libertades Civiles del Parlamento Europeo el 24 de mayo de 2016.

[3] Véase la Herramienta n.º 24 sobre Derechos Fundamentales y Derechos Humanos, incluida en el manual «Legislar mejor», disponible en http://ec.europa.eu/smart-regulation/guidelines/tool_24_en.htm y el análisis más en profundidad que se ofrece en el documento de trabajo de los servicios de la Comisión: Directrices Operativas relativas a la consideración de los derechos fundamentales en las evaluaciones de impacto de la SEC (2011) 567 final. Véase también las directrices sobre las medidas metodológicas que se han de tomar para verificar la compatibilidad de los derechos fundamentales en los órganos preparatorios del Consejo, 5377/15, 20 de enero de 2015. Estos documentos son más generales, aunque varios ejemplos de jurisprudencia en estas directrices se refieren a los derechos consagrados en los artículos 7 y 8 de la Carta, puesto que el TJUE ha dictado importantes sentencias sobre la limitación de estos derechos.

[4] Para una visión general de la jurisprudencia pertinente del TJUE y del TEDH, véase «Handbook on European data protection Law», publicado por la Agencia de Derechos Fundamentales de la UE en junio de 2014. Véase también «Factsheet - Personal data protection», publicado en noviembre de 2016 por el TEDH a través de la Unidad de Prensa, disponible en: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf.

[5] Véase «Developing a "toolkit" for assessing the necessity of measures that interfere with fundamental rights», disponible en: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Papers/16-06-16_Necessity_paper_for_consultation_EN.pdf.

[6] En el caso *Schecke*, el dictamen del fiscal general afirmó que «al igual que varios de los derechos clásicos del CEDH, el derecho a la intimidad no es un derecho absoluto». El apartado 2 del artículo 8 del CEDH reconoce expresamente la posibilidad de que se produzcan excepciones a este derecho, al igual que el artículo 9 del Convenio n.º 108 en lo que respecta al derecho a la protección de los datos personales. El artículo 52 de la Carta también establece (en términos generales) criterios similares que, si se cumplen, permiten excepciones (o derogaciones) de los derechos de la Carta», párrafo 73. Este planteamiento lo retoma la sentencia del TJUE en sus apartados 48 - 50.

[7] En lo que respecta a la noción de «previsto por la ley», deberían utilizarse los criterios desarrollados por el Tribunal Europeo de Derechos Humanos, tal y como se sugiere en varios dictámenes de los abogados generales del TJUE; véanse, por ejemplo, los dictámenes del abogado general en *Tele2 Sverige AB* , apartados 137-154, C-70/10 *Scarlet Extended* y C-291/12, apartados 88-114. Este enfoque se desarrolla en el Reglamento General de Protección de Datos 2016/679 considerando (41).

[8] Aunque no abunda la jurisprudencia en cuanto a las condiciones en las que se ve afectada la esencia de un derecho, se puede 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 *Schrems*, el TJUE consideró que se veía afectado el derecho a la tutela judicial efectiva. «Una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta» (apartado 95). A continuación, 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 el caso *Digital Rights Ireland*, el TJUE consideró que la 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. Asimismo, el TJUE consideró que la esencia del derecho a la protección de los datos de carácter personal no se veía afectada porque la 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 a partir de ese momento, el Tribunal procedió a evaluar la necesidad de la medida. La privación de la revisión, por parte de una autoridad independiente, del cumplimiento del nivel de protección garantizado por el Derecho de la UE podría afectar también a la esencia del derecho a la protección de los datos de carácter personal, ya que así lo exige expresamente el artículo 8, apartado 3, de la Carta y «*Si no fuera así, las personas cuyos datos personales han sido conservados se verían privadas del derecho, garantizado en el artículo 8, apartados 1 y 3, de la Carta, a solicitar la protección de sus datos personales ante las autoridades nacionales de control*», véase *Tele2 Sverige AB*, apartado 123.

[9] En el caso *Szabo y Vissy c. Hungría*, el TEDH consideró que la noción de «*personas afectadas identificadas (...) como una serie de personas*» podía incluir a cualquier persona sin que fuera necesario que las autoridades demostraran la relación de las personas afectadas y la prevención de un atentado terrorista. Dicha medida no cumple el requisito de previsibilidad y necesidad (párrafos, 58 62, 66, 67).

[10] Véase el apartado 4 del artículo 5 del Tratado constitutivo de la Unión Europea.

[11] Asunto C-62/14 Gauweiler (OMT), apartado 67.

[12] K. Lenaerts, P. Van Nuffel, *European Union Law*, Sweet and Maxwell, 3ª edición, Londres, 2011, p. 141. (Asunto C-343/09 *Afton Chemical*, apartado 45; *Volker und Markus Schecke y Eifert*, apartado 74; Asuntos C-581/10 y C-629/10 *Nelson y otros*, apartado 71; Asunto C-283/11 *Sky Österreich*, apartado 50; y Asunto C-101/12 *Schaible*, apartado 29).

[13] Véase, por ejemplo, el caso C-83/14 *Razpredelenie Bulgaria Ad,* apartado. 123. El Tribunal de Justicia señala que «*... suponiendo que no se pudiera identificar otra medida de igual eficacia que la práctica discutida, el tribunal remitente deberá además verificar si los inconvenientes causados por la práctica discutida no son desmesurados en relación con los objetivos perseguidos y si esa práctica no perjudica en grado excesivo los intereses legítimos de las personas que habitan en los barrios afectados*». Véase también el dictamen del Abogado General en los asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB*, apartados 132,172, 247, 248 en los que se afirma que el TJUE en el asunto Digital Rights Ireland no evaluó la proporcionalidad «*dado que el régimen establecido por la Directiva 2006/24 sí rebasaba los límites de lo estrictamente necesario a los efectos de la lucha contra los delitos*». A continuación, señaló que la «*exigencia de proporcionalidad en una sociedad 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 solo puede considerarse proporcionada si las desventajas ocasionadas no son desproporcionadas con respecto a los objetivos perseguidos* ».También señaló que la exigencia de proporcionalidad en el caso concreto de la conservación de una cantidad tan grande de datos «*abre así un debate sobre los valores que deben prevalecer en una sociedad democrática y, en definitiva, sobre el tipo de sociedad en el que deseamos vivir*». La sentencia del Tribunal, en los apartados 102-103, expone su análisis con consideraciones relativas más bien a la proporcionalidad cuando analiza si la lucha contra la delincuencia, incluso la más grave, justifica una conservación general e indiscriminada de datos de comunicaciones electrónicas. El Tribunal de Justicia afirma que «*... si bien es cierto que la eficacia de la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, puede depender en gran medida del uso de técnicas modernas de investigación, este objetivo de interés general, por muy fundamental que sea, no puede por sí solo justificar que una normativa 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*». También afirma que solo la lucha contra la delincuencia grave podría justificar la conservación selectiva y el acceso a los datos de las comunicaciones electrónicas. « *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*». «*Además, dado que el objetivo perseguido por dicha normativa debe guardar una relación con la gravedad de la injerencia en los derechos fundamentales que supone este acceso, de ello se deriva que, en materia de prevención, investigación, descubrimiento y persecución de delitos, sólo la lucha contra la delincuencia grave puede justificar dicho acceso a los datos conservados*».

14 Véanse el artículo 6, apartado 1, letra c), y el artículo 7 de la Directiva 95/46, el artículo 4, apartado 1, letra c), y el artículo 5, apartado 1, letra c), y el artículo 6, apartado 1, del Reglamento 2016/679, así como el considerando 49, que hace hincapié en la evaluación de la necesidad estricta en relación con el tratamiento de datos personales con el fin de garantizar la seguridad de la red y de la información de los sistemas del responsable del tratamiento, y el artículo 8, apartado 1, de la Directiva 2016/680.

En las orientaciones publicadas para que las instituciones de la UE evalúen si las medidas de videovigilancia son necesarias de conformidad con el Reglamento 45/2001, el SEPD destacó que «*los sistemas no deben instalarse si no son eficaces para lograr sus objetivos, por ejemplo, si solo proporcionan la ilusión de una mayor seguridad». (sección 5.4) y si «existen alternativas adecuadas». Una alternativa puede considerarse adecuada a menos que no sea factible o sea significativamente menos eficaz que la videovigilancia... La mera disponibilidad de la tecnología a un coste relativamente bajo no es suficiente para justificar el uso de la videotecnología».* (sección 5.5). Solo entonces pasó a evaluar si la medida era proporcional «*Por último, incluso si una institución llega a la conclusión de que existe una clara necesidad de utilizar la videovigilancia y no existen otros métodos menos intrusivos disponibles, solo deberá utilizar esta tecnología si los efectos perjudiciales de la videovigilancia se ven superados por los beneficios de la videovigilancia».* (sección 5.6). Véanse las directrices de videovigilancia del SEPD, Bruselas, 17.03.2010, disponibles en:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Directrices de videovigilancia_ES.pdf .

En el contexto de una notificación de control previo, de conformidad con el artículo 27 del Reglamento 45/2001, de una medida que proponía el uso de impresiones dactilares para el control del tiempo de trabajo, el SEPD destacó que esa operación de tratamiento no resultaba necesaria. «*El SEPD advierte de que el uso de sistemas basados en las huellas dactilares para el control del tiempo de trabajo de los funcionarios no se considera necesario, y, por consiguiente, no es legítimo en virtud del citado artículo 5 (n. - del Reglamento 45/2001). El requisito de que el tratamiento de los datos de carácter personal sea necesario en relación con la finalidad obliga al responsable del tratamiento a evaluar si la finalidad del tratamiento podría alcanzarse con medios menos intrusivos. De hecho, en lugar de optar por un sistema que utilice datos biométricos, [el organismo de la Unión] debería haber considerado otros sistemas en este contexto, como: firmar la entrada, utilizar partes de asistencia o utilizar sistemas de fichaje mediante tarjetas magnéticas*» (sección 3), véase la carta del SEPD sobre «Notificación de control previo relativa a la «Tramitación de las vacaciones y el horario flexible», 13.10.2014, disponible en:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Letters/2014/14-10-13_Letter_Mr_Mifsud_EBA_EN.pdf.

[15] En los asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland*, el Tribunal de Justicia declaró en primer lugar que la proporcionalidad se compone de los pasos de adecuación y necesidad (apartado 46), y a continuación estableció que la

limitación de los derechos protegidos en los artículos 7 y 8 no resultaba necesaria (véase el apartado 65) y, por consiguiente, concluyó que las limitaciones no resultaban proporcionadas (apartado 69). Del mismo modo, en el asunto C-362/14 *Schrems*, apartados 92, 93, donde el TJUE evaluó la necesidad y consideró que la Decisión de puerto seguro no era válida, sin hacer ninguna referencia a la proporcionalidad antes de llegar a esta conclusión (apartado 98).

[16] Por ejemplo, en los asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB*, el TJUE, en los apartados 102-103, expone su análisis con consideraciones relativas a la proporcionalidad en ese sentido estricto cuando evalúa si la lucha contra la delincuencia, incluso la grave, justifica una conservación general e indiscriminada de datos de comunicaciones electrónicas. El Tribunal de Justicia afirma que *«... si bien es cierto que la eficacia de la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, puede depender en gran medida del uso de técnicas modernas de investigación, este objetivo de interés general, por muy fundamental que sea, no puede por sí solo justificar que una normativa 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*». También afirma que solo la lucha contra la delincuencia grave podría justificar la conservación selectiva y el acceso a los datos de las comunicaciones electrónicas. «*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*». «*Además, dado que el objetivo perseguido por dicha normativa debe guardar una relación con la gravedad de la injerencia en los derechos fundamentales que supone este acceso, de ello se deriva que, en materia de prevención, investigación, descubrimiento y persecución de delitos, sólo la lucha contra la delincuencia grave puede justificar dicho acceso a los datos conservados*». Solo entonces procede a la evaluación de los requisitos de necesidad para una conservación selectiva de los datos de las comunicaciones (apartado 108).

[17] Véase también el Dictamen del Grupo de Trabajo del Artículo 29 4/2007 sobre el concepto de datos personales, página 7.

[18] Los recientes casos emblemáticos del TJUE en materia de protección de datos, en particular *Digital Rights Ireland* y *Schrems* ilustran esto.

[19]Véanse los asuntos del TJUE C-617/10, *Åkerberg Fransson*, apartado 44, C-398/13 P, *Inuit Tapiriit Kanatami y otros* c. *Comisión*, apartado 45, C-601/15 PPU *J.N. c. Staatssecretaris van Veiligheid en Justitie*, apartado 45 y los asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB*, apartados 127-129.

[20] Véanse el asunto C-199/11, *Otis y otros*, apartado 47, el asunto C-398/13 P, *Inuit Tapiriit Kanatami y otros* c. *Comisión*, apartado 46 y el asunto C-601/15 PPU, *J.N. c. Staatssecretaris van Veiligheid en Justitie*, apartado 46.

[21] Véase el asunto C-601/15 PPU*, J.N. contra Staatssecretaris van Veiligheid en Justitie*, apartado 77.

[22] Véase la nota explicativa del artículo 52 de la Carta.

[23] Véase H. Kranenborg, artículo 8, pg. 235, en S. Peers y J. Kenner, Carta de Derechos Fundamentales de la UE, 2014 y S. Peers, artículo 52, pág. 1515 y siguientes, ibid.

[24] Véanse, por ejemplo, los asuntos acumulados del TJUE C-92/09 y C-93/09, *Volker und Markus Schecke*, apartado 59, los asuntos acumulados C-293/12 y C-594/12*, Digital Rights Ireland*, apartado 35, los asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB,* apartados 119 y 120, y el TEDH *Zakharov c. Rusia* y *Szabo y Vissy c. Hungría*, apartado 23.

[25] Artículo 8(2) del CEDH: «*No podrá existir injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y* ***constituya una medida que, en una sociedad democrática, sea necesaria*** *para la seguridad nacional, la seguridad pública o el bienestar económico del país, para la prevención de desórdenes o delitos, para la protección de la salud o de la moral, o para la protección de los derechos y libertades de los demás*». Para la Carta, véase el apartado 1 del artículo 52
-«*Cualquier limitación del ejercicio de los derechos y libertades reconocidos en la presente Carta deberá estar prevista por la ley y respetar la esencia de dichos derechos y libertades. Sin perjuicio del principio de proporcionalidad, las limitaciones solo podrán hacerse si son* ***necesarias*** y responden realmente a objetivos de interés general reconocidos por la Unión o a la necesidad de proteger los derechos y libertades».

[26] Para un análisis detallado de la jurisprudencia del TEDH sobre la aplicación de los requisitos del artículo 8.2 del Convenio, véase el Dictamen 01/2014 del Grupo de Trabajo del Artículo 29 sobre la aplicación de los conceptos de necesidad y proporcionalidad y la protección de datos en el sector de los organismos con funciones coercitivas, 27.02.2014.

[27] TEDH, *Szabo y Vissy c. Hungría*, apartado 73.

[28] Véase el asunto del TJUE C-73/07 *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy, Satamedia Oy*, apartado 56; asuntos acumulados C-92/09 y C-93/09 *Volker und Markus Schecke*, apartado 77; asunto C-473/12 *IPI*, apartado 39; asuntos acumulados C-293/12 y C-594/12 *Digital Rights Ireland y Seitlinger y otros*, apartado 52; Asunto C- 212/13 *Rynes*, apartado 28 y Asunto C-362/14 *Schrems* , apartado 92, C-698/15, *Tele2 Sverige AB*, apartado 96 y el Dictamen AG 1/15 (Solicitud de dictamen presentada por el Parlamento Europeo) sobre el Proyecto de Acuerdo entre Canadá y la UE sobre la transferencia y el tratamiento de los registros de nombres de los pasajeros, apartado 226.

[29] Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de estos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, DO L119 de 4.5.2016.

[30] TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland*, apartados 47-48.

[31] SEPD, alegato en la vista oral en el caso del proyecto de acuerdo PNR UE-Canadá, disponible en: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2016/16-04-05_Pleading_Canada_PNR2_EN.pdf.
El Dictamen AG 1/15 (Solicitud de dictamen presentada por el Parlamento Europeo) sobre el Proyecto de Acuerdo entre Canadá y la UE sobre la transferencia y el tratamiento de los registros de nombres de los pasajeros, establece que el control estricto de la discrecionalidad del legislador se basa en el importante papel que el tratamiento de los datos personales tiene en la sociedad y en la gravedad de la limitación que la medida en cuestión puede causar (apartado 201). Véase también TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland*, apartado 47.

[32] TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland*, apartados 34 - 36; véase también los asuntos acumulados C-92/09 y C-93/09 *Volker und Markus Schecke*, apartado 58.

[33] Véanse, por ejemplo, los asuntos acumulados C-92/09 y C-93/09 *Volker und Markus Schecke*, apartado 55 y los asuntos acumulados C-468/10 y C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y Federación de Comercio Electrónico y Marketing Directo (FECEMD), contra la Administración del Estado*, apartado 41. El TJUE únicamente sostuvo en un caso que no existía una limitación del derecho a la vida privada cuando los datos de carácter personal relacionados con los salarios fueron tratados por las empresas para su finalidad original, véase TJUE, asuntos acumulados C-465/00, C-138/01 y C-139/01, *Rechnungshof y otros contra Österreichischer Rundfunk*, apartado 74.

[34] TJUE, asuntos acumulados C-465/00, C-138/01 y C-139/01, *Rechnungshof et al v. Österreichischer Rundfunk*, apartado 75 y asuntos acumulados C-293/12 y C-594/12 *Digital Rights Ireland*, apartado 33.

[35] TJUE, asuntos acumulados C-465/00, C-138/01 y C-139/01, *Rechnungshof y otros contra Österreichischer Rundfunk*, apartado 75, asuntos acumulados C-293/12 y C-594/12 *Digital Rights Ireland*, apartado 33. TEDH, *S. y Marper v. Reino Unido*, apartado 67. El Tribunal declaró que «*Sin embargo, para determinar si la información personal conservada por las autoridades implica alguno 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 que dichos registros se utilizan y se procesan y los resultados que pueden obtenerse (véase, mutatis mutandis, Friedl, citada, §§ 49-51, y Peck, citada, § 59)*».

[36] Asimismo, tal y como afirmó el TJUE, la necesidad tiene un significado propio e independiente en el Derecho derivado de la UE. Sobre el significado independiente del concepto de necesidad en el artículo 7 (e) de la Directiva 95/46/CE, véase TJUE, C-524/06, *Huber v. Bundesrepublik Deutschland*, apartado 52.

[37] Véase la Directiva 95/45, artículo 1 (a).

[38] Véase el Dictamen 4/2007 del Grupo de Trabajo del Artículo 29 sobre el concepto de datos personales, disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf.

[39] TJUE, asuntos C-465/00, C-138/01 y C-139/01 *Österreichischer Rundfunk y otros*, apartado 75 y *Digital Rights Ireland*, apartado 33.

[40] TEDH, *Leander c. Suecia*, apartado 48.

[41] TEDH, *Amman c. Suiza*, apartado 65, 69 y 80.

[42] Por lo que respecta al artículo 8 del TEDH, véase *Leander c. Suecia*, 26 de marzo de 1987, apartado 48; *Rotaru c. Rumanía* GC], no. 28341/95, párrafo 46 y *Weber y Saravia v. Alemania* no. 54934/00, apartado 79, TEDH 2006-XI. Para el artículo 7 de la Carta, véase TJUE, *Digital Rights Ireland*, apartado 35.

[43] TEDH, *Leander c. Suecia*, 26 de marzo de 1987, apartado 48; *Rotaru c. Rumanía* [GC], nº 28341/95, apartado 46.

[44] TJUE, C-362/14, *Schrems*, apartado 97.

[45] TJUE, *Huber*, apartados 75, 79, 80, 81.

[46] TJUE, asuntos acumulados C-293/12 y C-594/12 *Digital Rights Ireland*, apartado 28, *Tele2 Sverige AB,* apartado 92. Véase también C. Docksey, Four Fundamental rights: finding the balance, (2016) 6 International Data Privacy Law, pp. 2.

[47] Dictamen del GC 1/15 (Solicitud de dictamen presentada por el Parlamento Europeo) sobre el Proyecto de Acuerdo entre Canadá y la UE sobre la transferencia y el tratamiento de los registros de nombres de los pasajeros, apartados 274-281.

[48] Como por ejemplo los artículos 36 y 346 del TFUE. Sobre los objetivos de interés general, véase también la nota explicativa del artículo 52 de la Carta.

[49] TJUE, asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke*, apartados 65, 68, 69, 75.

[50] TJUE, C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU*, apartado 65; C-70/10, *Scarlet Extended SA contra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, apartados 46, 49, 53.

[51] TJUE, C-145/09, *Tsakouridis*, sobre el concepto de seguridad pública, apartados 43 y 44; C-601/15 PPU *J. N. v. Staatssecretaris voor Veiligheid en Justitie*, apartado 66.

[52] SEPD, Dictamen sobre la propuesta de Reglamento de la Guardia Europea de Fronteras y Costas, 02/2016, apartado 8.

[53] TJUE, *Digital Rights Ireland,* apartados 49-50.

[54] Grupo de Trabajo del Artículo 29, Dictamen 9/2004 sobre un proyecto de Decisión marco relativa al almacenamiento de

datos tratados y conservados a efectos de la prestación de servicios públicos de comunicaciones electrónicas, WP 99, 9.11.2004.

[55] Grupo de Trabajo del Artículo 29, Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, WP 193, 27.04.2012, p. 8.

[56] Véase el artículo 8 de la Directiva 95/46, los artículos 9 y 10 del Reglamento General de Protección de Datos 2016/679 y la Directiva 2016/680.

[57] Artículo 9 del Reglamento 2016/679, artículo 10 de la Directiva 2016/680.

[58] Véase, por ejemplo, Grupo de Trabajo del Artículo 29, Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, p. 4.

[59] TJUE, C-291/12, *Schwarz*, El Tribunal de Justicia declaró que «*En tales circunstancias, procede señalar que no se ha puesto en conocimiento del Tribunal de Justicia la existencia de medidas que contribuyan, con la suficiente eficacia, al objetivo de proteger los pasaportes contra su uso fraudulento vulnerando de forma menos grave los derechos reconocidos por los artículos 7 y 8 de la Carta que el método basado en las impresiones dactilares.*». apartado 53; Véase también el Dictamen AG 1/15 (Solicitud de dictamen presentada por el Parlamento Europeo) sobre el Proyecto de Acuerdo entre Canadá y la UE sobre la transferencia y el tratamiento de los registros de nombres de los pasajeros, según el cual el Acuerdo sobre los registros de nombres de los pasajeros debe consistir en las medidas menos perjudiciales para los derechos reconocidos por los artículos 7 y 8 de la Carta, contribuyendo al mismo tiempo de manera eficaz al objetivo de seguridad pública, apartados 208, 244.

[60] Sin embargo, esto no se aplica a los identificadores de aplicación general. Véase el artículo 87 del Reglamento 2016/679.

[61] TJUE, *Digital Rights Ireland*, apartado 54 y la jurisprudencia citada del TEDH *(Liberty y otros contra el Reino Unido*, apartados 62 y 63; *Rotaru contra Rumanía*, apartados 57 a 59, y *S. y Marper contra el Reino Unido*, apartado 99).

[62] TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland,* apartado 60; C-362/14, *Schrems*, apartado 93.

[63] TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland*, apartado 57; C-362/14 Schrems, apartado 93.

[64] TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland*, apartados 63-64.

[65] TEDH, *R. Zakharov c. Rusia*, apartado 287. Véase también TEDH, *Szabo y Vissy c. Hungría*, apartado 86.

[66] Véase, en relación con el principio de subsidiariedad, la herramienta nº 3 sobre la base jurídica, la subsidiariedad y la proporcionalidad, que forma parte de la caja de herramientas «Legislar mejor», disponible en http://ec.europa.eu/smart-regulation/guidelines/tool_3_en.htm.