Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo

v. junio 2023

RESUMEN EJECUTIVO

Las presentes orientaciones tienen como objeto servir de guía para la realización de una evaluación de impacto para la protección de datos (EIPD) en el marco de la elaboración de la Memoria de Análisis de Impacto Normativo (MAIN), cuando las iniciativas legislativas de las Administraciones Públicas, que son competencia de la AEPD, implican el tratamiento de datos personales.

La EIPD de una norma en la que se plantean tratamientos de datos personales ha de evaluar el impacto que estos tienen sobre los derechos y libertades fundamentales de las personas tomadas individualmente y como sociedad. Por lo tanto, no es una evaluación del riesgo legal o de cumplimiento. La jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) y del Tribunal Europeo de Derechos Humanos (TEDH) indica que la necesidad y proporcionalidad en la normativa de protección de datos es un concepto basado en los hechos, más que una noción jurídica meramente abstracta, y que el tratamiento debe considerarse a la luz de las circunstancias específicas que rodean cada caso, así como de las disposiciones de la medida y de la finalidad concreta que se pretende alcanzar. Por lo tanto, la EIPD requiere aplicar una metodología paso a paso y sin automatismos.

Este documento está orientado a los organismos de las Administraciones Públicas que promuevan proyectos normativos que impliquen tratamientos de datos personales a los que sea de aplicación el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos o RGPD), así como la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (L.O. 7/2021). Asimismo, está dirigido a los Delegados de Protección de Datos (DPD) de los citados organismos con el fin de contribuir al desempeño de sus funciones de asesoramiento en relación con dichos proyectos normativos.

Palabras clave: Evaluación de impacto para la protección de datos, EIPD, idoneidad, necesidad, proporcionalidad, riesgos, derechos y libertades, delegado de protección de datos, DPD, Administraciones Públicas, Memoria de Análisis de Impacto Normativo, MAIN, legislación.

I. CONTENIDO

I. Introducción 4

II. Requisitos previos a la realización de la evaluación de impacto para la protección de datos 5

A. Determinar la existencia de un tratamiento de datos personales 5

B. Determinar cuándo hay que realizar una evaluación de impacto 5

C. Determinar el rango adecuado de la norma 6

D. Determinar la calidad de la norma desde la perspectiva de protección de datos 7

III. Evaluación de impacto para la protección de datos 9

A. Evaluar las limitaciones y riesgos para los derechos y libertades 10

B. Respeto a la esencia del derecho 11

C. Evaluación de la finalidad 11

D. Evaluación de la idoneidad y necesidad 12

E. Evaluación de la proporcionalidad 14

F. Salvaguardas 16

IV. Evaluación de la calidad de la EIPD 18

V. Conclusiones 18

VI. Material para dar soporte a estas obligaciones 19

A. General del Riesgo 19

B. Específica para las AA.PP. 19

C. Específica para el desarrollo normativo 20

I. INTRODUCCIÓN

Las presentes orientaciones tienen como objeto servir de guía para la realización de una evaluación de impacto para la protección de datos (EIPD) en el marco de la elaboración de la Memoria de Análisis de Impacto Normativo (MAIN), cuando las iniciativas legislativas de las Administraciones Públicas, que son competencia de la AEPD, implican el tratamiento de datos personales.

La EIPD ha de realizarse **desde el diseño de la norma**, como establece la Guía Metodológica para la Elaboración de una Memoria de Impacto Normativo (R.D. 931/2017):

- El Análisis de Impacto Normativo es un proceso continuo que ha de permitir adaptar la norma para minimizar dicho impacto.
- No es un puro trámite que deba cumplirse una vez se haya terminado de redactar una nueva propuesta normativa.
- Ni tampoco es un trámite que se agote con la elaboración de la Memoria.
- La Memoria se realizará de manera simultánea a la elaboración del proyecto normativo, desde su inicio hasta su finalización.

Este documento está orientado a los organismos de las Administraciones Públicas que promuevan proyectos normativos que impliquen tratamientos de datos personales a los que sea de aplicación el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos o RGPD), así como la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (L.O. 7/2021). Asimismo, está dirigido a los Delegados de Protección de Datos (DPD) de los citados organismos con el fin de contribuir al desempeño de sus funciones de asesoramiento en relación con dichos proyectos normativos.

Estas orientaciones están basadas y trasladan fragmentos de los siguientes documentos fundamentalmente:

- Supervisor Europeo de Protección de Datos (SEPD): Guía para evaluar la necesidad de los tratamientos en políticas y medidas legislativas.
- SEPD: Guía para evaluar la proporcionalidad de los tratamientos en políticas y medidas legislativas.
- Comité Europeo de Protección de Datos[1] (CEPD) Dictamen 01/2014 sobre la aplicación de los conceptos de necesidad y proporcionalidad y la protección de datos en el sector de los organismos con funciones coercitivas.

[1] Antes denominado Grupo del Artículo 29 (WP29)

Dichos documentos contienen más de 40 ejemplos de evaluaciones de necesidad y proporcionalidad. Para limitar la extensión de este texto, se hace referencia a algunos de ellos sin trasladar el literal de los mismos.

II. REQUISITOS PREVIOS A LA REALIZACIÓN DE LA EVALUACIÓN DE IMPACTO PARA LA PROTECCIÓN DE DATOS

Previamente a realizar una EIPD, es necesario determinar si se cumplen ciertos requisitos de mínimos.

A. DETERMINAR LA EXISTENCIA DE UN TRATAMIENTO DE DATOS PERSONALES

La noción de datos personales es muy amplia, ya que incluye cualquier información relativa a una persona física identificada o identificable; 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. Por consiguiente, un nombre, un apellido, una matrícula de un vehículo, un teléfono, un número de pasaporte, una dirección IP, un perfil vinculado a una persona en cualquiera de los ámbitos antes citados cualquier otro identificador único, incluidos datos o conjuntos de datos que actúen como seudoidentificadores, y los vinculados a los mismos, se considerará un dato personal[2].

Por tratamiento de datos se entiende cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción. (art. 4.2 RGPD y art. 5.b L.O. 7/2021). En el caso de tratamientos no automatizados la regulación sobre protección de datos es de aplicación cuando se traten datos contenidos o destinados a ser incluidos en un fichero[3].

El tratamiento de datos personales con propósito de implementar medidas de seguridad de la red, de la información u otros, en sí mismo, es un tratamiento de datos personales.

Hito: Si la norma no propone o implica tratamiento alguno de datos personales, no es necesario llevar a cabo la EIPD.

B. DETERMINAR CUÁNDO HAY QUE REALIZAR UNA EVALUACIÓN DE IMPACTO

Tanto la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE)[4], así como las opiniones del SEPD (apartado II.5 de la Guía de Necesidad del SEPD) exponen que la

[2] 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.
[3] Art.4.6 del RGPD "fichero: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica"
[4] 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.

evaluación de impacto de una normativa con relación a la protección de datos debe realizarse en los casos en que la medida legislativa propuesta implique el tratamiento de datos personales. Cualquier operación de tratamiento de datos prevista por la legislación supone una limitación del derecho a la protección de los datos personales, independientemente de que dicha limitación pueda estar justificada.

A su vez, el Tribunal Europeo de Derechos Humanos (TEDH) ha sostenido que el almacenamiento por parte de una autoridad pública de datos o informaciones relativas a la vida privada de una persona equivale a una limitación del derecho al respeto de su vida privada[5].

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»[6].

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[7].

C. DETERMINAR EL RANGO ADECUADO DE LA NORMA

El art. 8 de la LOPDGGD establece que el tratamiento de datos personales por obligación legal (6.1.c RGPD), interés público o ejercicio de poderes públicos (6.1.e RGPD), así como las especialidades de los tratamientos sometidos a la L.O. 7/2021[8], solo se podrá considerar fundado cuando así lo prevea o se derive de una competencia atribuida por una norma de Derecho de la Unión Europea o una norma con rango de ley.

Hito: Si la norma no tiene rango de ley, deben identificarse las normas legales que regulan el tratamiento con los requisitos y garantías oportunas y permiten el desarrollo de aspectos parciales del mismo[9]. En caso de no existir dicha norma o no cumplir con los requisitos legales y jurisprudenciales para limitar el derecho fundamental, no se puede continuar con la EIPD y deberá proponerse la elaboración de una norma con rango de ley.

[5] TEDH, Leander c. Suecia, apartado 48.
[6] TJUE, asuntos C-465/00, C-138/01 y C-139/01 Österreichischer Rundfunk y otros, apartado 75 y Digital Rights Ireland, apartado 33.
[7] 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.
[8] La L.O. 7/2021, a través del art.6.2, reconduce a las obligaciones del art.8 de la LOPDGDD, para tratamientos que estén más allá de lo establecido en el art.1 de la L.O. 7/2021, además específicamente para el tratamiento de categorías especiales de datos (art.13) y decisiones automatizadas (art14). Además, así está expresado en la exposición de motivos: "Se exigen igualmente ciertas condiciones que determinan la licitud de todo tratamiento de datos de carácter personal, esto es, que sean tratados por las autoridades competentes; que resulten necesarios para los fines de esta Ley Orgánica y que, en caso necesario y en cada ámbito particular, se especifiquen las especialidades por una norma con rango de ley que incluya unos contenidos mínimos".
[9] STC 292/2000, de 30 de noviembre, FJ 15:, *Esta doble función de la reserva de ley se traduce en una doble exigencia: por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, esa norma legal "ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica", esto es, "ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención" (STC 49/1999, FJ 4). En otras palabras, "no sólo excluye apoderamientos a favor de las normas reglamentarias […], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites"*.

D. DETERMINAR LA CALIDAD DE LA NORMA DESDE LA PERSPECTIVA DE PROTECCIÓN DE DATOS

Toda medida legislativa que habilite un tratamiento debe cumplir con la premisa de "previsto en la ley". Esto implica que debe ser clara y precisa, y su aplicación accesible y previsible para sus destinatarios, de conformidad con el TEDH[10], el TJUE[11] y el Tribunal Constitucional (TC)[12]. Por lo tanto, en la norma han de estar claramente definidos, con precisión y apropiadamente:

1.- La finalidad o finalidades del tratamiento.

La finalidad del tratamiento ha de ser última. Por ejemplo, un tratamiento de vigilancia biométrica no supone un fin en sí mismo, sino un medio (entre otros) para implementar una finalidad última como podría ser la seguridad del Estado, de las instalaciones u otras. En el mismo sentido, una tecnología no es un fin, sino un medio.

2.- La legitimidad del tratamiento

El consentimiento (6.1.a RGPD) no es, con carácter general, la base jurídica adecuada para un tratamiento establecido por norma[13] debido al desequilibro claro entre el interesado y una autoridad pública responsable, aunque en determinadas ocasiones puede exigirse como una garantía adicional, siempre que se cumplan los requisitos exigidos para el consentimiento en el RGPD, singularmente que sea libre por ofrecerse alternativas equivalentes.

3.- La descripción de la implementación[14] del tratamiento en sus aspectos relevantes, como pueden las operaciones y los procedimientos determinantes del tratamiento (por ejemplo, recogida, almacenamiento, acceso, transmisión, difusión,…), las tecnologías planteadas para implementar las operaciones (inteligencia artificial, almacenamiento en Nube, biometría, IoT, móviles, videovigilancia,…), la existencia de decisiones automatizadas, así como la participación o posible participación de encargados y/o subencargados en distintas operaciones del tratamiento, entre otros.

En el apartado III.B de la guía Gestión del Riesgo y EIPD se desarrollan los elementos que definen la naturaleza, el contexto, el alcance y los fines de un tratamiento.

4.- El ámbito y extensión del tratamiento con relación a las categorías de datos personales tratados (especialmente si son categorías especiales), las

[10] TEDH Benedik contra Eslovenia, apartado 132: "el Tribunal de Justicia considera que la ley en la que se basó la medida impugnada, es decir, la obtención por parte de la policía de la información del abonado asociada a la dirección IP dinámica en cuestión [...], y la forma en que fue aplicada por los tribunales nacionales carecían de claridad y no ofrecían suficientes garantías contra la injerencia arbitraria en los derechos previstos en el artículo 8. En tales circunstancias, el Tribunal considera que la injerencia en el derecho del demandante al respeto de su vida privada no fue "conforme a la ley" como exige el artículo 8, apartado 2, del Convenio".

[11] La STJUE de 6 de octubre de 2020, en los casos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, en su apartado 175, recuerda que: *En cuanto a la justificación de dicha injerencia, cabe precisar que el requisito, previsto en el artículo 52, apartado 1, de la Carta, de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que la permita debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada)*. En el mismo sentido, STJUE de 6 de octubre de 2020 (C-623/17), Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros (apartado 65), Más recientemente, la Sentencia del TJUE (Gran Sala) de 21 de junio de 2022, al pronunciarse respecto de la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, recuerdo su propia doctrina en los apartados 112 a 118.

[12] STC 76/2019, de 22 de mayo, y STC 292/2000, de 30 de noviembre

[13] Considerando 43, Directrices 5/2000 sobre el consentimiento en el sentido del RGPD

[14] En el RGPD se utiliza el término "naturaleza" para la descripción de la implementación del tratamiento.

categorías de interesados afectados[15], 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.), los plazos de conservación de los datos, la frecuencia de recogida de datos, la granularidad de los datos y otros factores que definan el alcance del tratamiento.

5.- Los responsables/corresponsables o categorías de responsables y, en su caso, los encargados o categorías de encargos y/o de subencargados, desde el punto de vista RGPD-L.O. 7/2021 han de estar bien definidos.

Consejo: No hay que confundir la figura de responsable RGPD-L.O. 7/2021, figura legal definida en los arts. 4.7 RGPD y 5.g L.O. 7/2021, que generalmente corresponde a una persona jurídica, con la asignación o distribución de responsabilidades dentro del órgano/ente correspondiente o la persona física titular del órgano responsable.

6.- Las entidades que acceden y a las que se pueden comunicar datos personales, así como los fines de tal comunicación, en particular, las condiciones de la comunicación de datos entre autoridades públicas en virtud de una obligación legal para el ejercicio de una misión oficial según las condiciones del RGPD (Cons. 31):

- En el marco de una investigación concreta.
- De interés general.
- De conformidad con el Derecho de la Unión o de los Estados miembros.
- Por escrito y de forma motivada.
- Con carácter ocasional.
- No deben referirse a la totalidad de un fichero.
- No deben dar lugar a la interconexión de varios ficheros[16].

7.- La justificación de la solución adoptada para el acceso[17] a datos personales, teniendo en cuenta que supone la utilización de datos de conformidad con unos requisitos específicos de carácter técnico, jurídico u organizativo, sin que ello implique necesariamente la transmisión o la descarga de los datos[18].

[15] 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.

[16] Asimismo, debe recordarse la doctrina del Tribunal Constitucional contraria a los tratamientos masivos de datos personales, recogida en su sentencia 17/2013, de 31 de enero de 2013, conforme a la cual (i) habrá de evitarse el acceso indiscriminado y masivo a los datos personales (ii) el dato en cuestión solicitado habrá de ser pertinente y necesario (iii) para la finalidad establecida en el precepto (iv) la solicitud de acceso a los concretos datos personales habrá de motivarse y justificarse expresamente, (v) de manera que ello posibilite su control por el cedente (vi) y se evite un uso torticero de esa facultad con accesos masivos. Ello supone (vii) que ha de quedar garantizada la posibilidad de analizar si en cada caso concreto el acceso tenía amparo en lo establecido en la ley.

[17] Considerando 7 del Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos) "*Existen técnicas que permiten realizar análisis en las bases de datos que contienen datos personales, como la anonimización, la privacidad diferencial, la generalización, la supresión y la aleatorización, el uso de datos sintéticos o de métodos similares, y otros métodos punteros de protección de la privacidad que pueden contribuir a un tratamiento de datos más respetuoso de la privacidad. Los Estados miembros deben prestar apoyo a los organismos del sector público con el fin de hacer un uso óptimo de dichas técnicas y, de este modo, facilitar el mayor número posible de datos para su intercambio…*"

[18] Art.4.2.13 del Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos).

8.- Las medidas para garantizar un tratamiento lícito y equitativo, habida cuenta de la naturaleza, alcance (especialmente con relación a las categorías especiales de datos), contexto y finalidades del tratamiento o de las categorías de tratamientos, los mecanismos de información y transparencia, así como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX del RGPD, en particular, aquella orientadas a evitar los accesos o las transferencias de datos ilícitos o abusivos[19].

9.- En el caso de limitación por ley de derechos u obligaciones al amparo de los arts. 23 del RGPD o 24 de la L.O. 7/2021, debe estar muy clara su determinación, las condiciones específicas de limitación de las obligaciones y derechos (Cons. 19 del RGPD), y los perjuicios concretos a la consecución de los fines que justifican la falta de información a los interesados sobre la limitación.

La lista anterior no es exhaustiva, sino que cualquier otra disposición pertinente , para cada caso concreto, debería incluirse en la descripción del tratamiento.

Hito: Si la norma no tiene la calidad necesaria desde el punto de vista de protección de datos, antes de iniciar el proceso de EIPD será necesario redactarla de forma precisa.

III. EVALUACIÓN DE IMPACTO PARA LA PROTECCIÓN DE DATOS

La evaluación de impacto para la protección de datos requiere una valoración basada en hechos objetivos. Debe existir una justificación sólida de las medidas propuestas capaz de resistir un examen. Por lo tanto, las medidas propuestas deben basarse en investigaciones, estadísticas, previsiones basadas en pruebas, etc.

La profundidad y formalidad de la EIPD ha de ser más exhaustiva cuando hay un alto riesgo para los derechos y libertades de los interesados (WP248).

Los elementos por evaluar serán:

- Las limitaciones y riesgos para los derechos y libertades.
- El respeto a la esencia del derecho.
- La finalidad.
- La proporcionalidad del tratamiento, incluyendo la evaluación de la idoneidad, necesidad y proporcionalidad en sentido estricto.

[19] Como recuerda la STC 76/2019, de 22 de mayo respecto de la norma en la que deben recogerse dichas garantías (F.J.8): *(…) La previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. (…). Según reiterada doctrina constitucional, la reserva de ley no se limita a exigir que una ley habilite la medida restrictiva de derechos fundamentales, sino que también es preciso, conforme tanto a exigencias denominadas –unas veces– de predeterminación normativa y –otras– de calidad de la ley como al respeto al contenido esencial del derecho, que en esa regulación el legislador, que viene obligado de forma primaria a ponderar los derechos o intereses en pugna, predetermine los supuestos, las condiciones y las garantías en que procede la adopción de medidas restrictivas de derechos fundamentales. Ese mandato de predeterminación respecto de elementos esenciales, vinculados también en último término al juicio de proporcionalidad de la limitación del derecho fundamental, no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares. (…)*

Evaluar cada uno de estos elementos no se reduce a una mera afirmación o manifestación de su conformidad. La evaluación es un proceso para construir racionalmente una conclusión a partir del examen y estudio de pruebas concretas.

A. EVALUAR LAS LIMITACIONES Y RIESGOS PARA LOS DERECHOS Y LIBERTADES

En marco de la EIPD se han de identificar las limitaciones y los riesgos para los derechos y libertades para las personas físicas que el tratamiento, o los tratamientos necesarios para conseguir los objetivos de la norma pueden suponer.

El mero hecho de que una medida limite o suponga unos riegos para el ejercicio de estos derechos no significa como tal que la medida no deba proponerse. No obstante, la medida tendrá que plantearse de manera que supere una EIPD, es decir, que los riesgos para las personas físicas hayan podido mitigarse adecuadamente y se haya superado el análisis de idoneidad, necesidad y proporcionalidad en sentido estricto.

Los derechos y libertades de los interesados atañen principalmente a los derechos a la protección de datos y a la intimidad, pero también hacen referencia a otros derechos fundamentales (WP248), como son la libertad de expresión, la libertad de pensamiento, la libertad de circulación, la libertad para la autodeterminación personal, la prohibición de discriminación (diferencia de trato entre las personas), la libertad de conciencia y de religión, la inviolabilidad de las comunicaciones, el derecho a la tutela judicial efectiva, la libertad de recibir información, el derecho de reunión y manifestación, etc.

Es necesario realizar un análisis más profundo que determinar simplemente si hay tratamiento de categorías especiales de datos. Aquellas iniciativas que impliquen tratamientos en los que en su implementación intervengan inteligencia artificial, decisiones automatizadas, biometría, vigilancia masiva, centralización a gran escala, tratamiento masivo de datos, datos de menores, de personas vulnerables, etc., podrían implicar riesgos adicionales e impactos colaterales indeseados.

Teniendo en cuenta que los tratamientos llevados a cabo por las AA.PP. afectan a grandes colectivos sociales, sino es a toda la sociedad, los riesgos han de ser estudiados en dos dimensiones:

- Riesgo para los derechos y libertades de los individuos.
- Riesgo para la propia sociedad (o para un grupo representativo de ella)[20].

Es importante señalar que la materialización de un factor de riesgo el impacto puede ser menor en lo que respecta a la persona en cuestión y, sin embargo, significativo o muy significativo en lo que respecta a la sociedad en su conjunto. Algunos ejemplos hipotéticos son: daños al proceso electoral y político (uso indebido de los datos para la manipulación política); la elaboración de perfiles ilegales y la discriminación, que provocan la desconfianza hacia las autoridades públicas; el «efecto amedrentador» sobre la libertad de expresión de unas medidas de vigilancia

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

omnipresente u otros efectos negativos sobre la libertad de las personas derivados de un sistema de elaboración de perfiles y de puntuación omnipresente y sistemáticamente aplicado (paso III.6.2 de la Guía de Proporcionalidad del SEPD).

En la determinación de los riesgos individuales y para la sociedad, hay que tener en cuenta la posibilidad de que existan brechas, incluso masivas, de datos personales.

Para ayudar a la identificación de riesgos para los derechos y libertades aconsejamos consultar la guía "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales", la "Relación de tablas de la guía de Gestión del riesgo y evaluación de impacto en formato editable", o la herramienta Evalúa Riesgo, en la que se encuentran identificados más de 130 factores de riesgos que aparecen en la normativa de protección de datos. Los factores de riesgos ahí identificados no constituyen una lista ni exhaustiva ni exigible[21] para todos los casos, sino sólo una orientación de los que se podrían encontrar en un tratamiento.

B. RESPETO A LA ESENCIA DEL DERECHO

El tratamiento de datos personales supone una limitación al derecho a la protección de datos. Tal como establece el art. 52.1 de la Carta de los Derechos Fundamentales de la Unión Europea, así como el TJEU[22], la limitación debe **respetar la esencia del derecho** a la protección de datos para que sus elementos fundamentales no queden vacíos de contenido y acabar impidiendo así el ejercicio de este[23].

La evaluación del respeto a la esencia del derecho puede, en algunos casos, necesitar un profundo análisis jurídico y ser el punto más crítico de la EIPD.

Hito: Si la esencia del derecho se viera afectada la medida sería ilegal[24] y habría que reformarla antes de continuar la EIPD.

C. EVALUACIÓN DE LA FINALIDAD

Para cada una de las finalidades hay que evaluar:

1.- Si hay una correcta aplicación de **principio de finalidad**, siendo todo lo específico que sea posible sobre los fines para los que una medida propuesta podría autorizar la recopilación y el tratamiento de datos personales (WP211).

[21] Es decir, ni están todos lo que podrían aparecer en un tratamiento, ni todos los mostrados surgen en todos los tratamientos. Se ha detectado que cuando en la norma de protección de datos se enumeran ejemplos o se utilizan las expresiones "entre otros" o "como…", se está interpretando como una relación exhaustiva y exigible (p.ej. en el caso del artículo 25.1 o 32.1.a con relación a la seudonimización).

[22] Michael Schwarz contra Stadt Bochum, TJUE, C-291/12, (TJUE, 17 de octubre de 2013), no publicado. El demandante cuestionaba la negativa de las autoridades de la ciudad alemana de Bochum a expedirle un pasaporte (UE) a menos que tuviera almacenadas en dicho pasaporte dos huellas digitales. Esta obligación tiene su origen en el Reglamento (CE) nº 2252/2004, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje.

[23] STC 292/2000, de 30 de noviembre. FJ 7 7. *"De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos".*

[24] En Schrems, el TJUE consideró que se veía afectado el derecho a la tutela judicial efectiva.

El cumplimiento del criterio SMART, definido por la Comisión Europea, puede ayudar a detallarlo. Dicho criterio establece que los fines han de ser:

a.- **específicos** (lo suficientemente precisos y concretos);

b.- **medibles** (definir un estado futuro deseado en términos medibles, por ejemplo, disminución de los delitos estimada en un porcentaje,…);

c.- **alcanzables**;

d.- **realistas**; y

e.- **delimitados en el tiempo** (relacionados con una fecha o periodo de tiempo fijo en el que deben lograrse los resultados).

2.- La norma persigue un, o unos **objetivos legítimos** (WP211), es decir, un objetivo de interés general reconocido por la Unión o la necesidad de proteger los derechos y libertades, dentro de una sociedad democrática, definido de forma concreta y no hipotética.

Por ejemplo, los objetivos generales mencionados en los artículos 3 o 4 (2) del TUE, otros intereses protegidos por disposiciones específicas de los tratados, los así interpretados por el TJUE, los enumerados en el art. 23.1 del RGPD o el art. 1 de la L. O. 7/2021, el derecho de acceso a los datos de carácter personal, las obligaciones del responsable del tratamiento o la transparencia y el control público (artículos 1 y 15.1 del TUE), protección de los derechos de propiedad intelectual y el derecho a la tutela judicial efectiva, la libertad de expresión y de empresa, entre otros.

3.- La finalidad establecida en la norma ha de ser **definida con lealtad**, como establecen los arts. 5.1. del RGPD y 6.1.a L.O. 7/2021, de forma que el tratamiento no se enmarque en una medida que no aborda realmente el problema declarado sino un propósito diferente[25].

La implementación de videovigilancia de un área de acceso pública justificada en un aumento de la seguridad podría no ser leal si lo que realmente se está buscando es una medida de imagen frente un malestar social, o reducción de costes.

D. EVALUACIÓN DE LA IDONEIDAD Y NECESIDAD

Según el TJUE y del TEDH la necesidad en la normativa de protección de datos es un concepto basado en los hechos, más que una noción jurídica meramente abstracta. La necesidad debe considerarse a la luz de las circunstancias específicas que rodean el tratamiento.

En la evaluación de la necesidad han de examinarse los siguientes elementos:

1.- Aplicación del concepto de **estricta necesidad**[26]: Hay que evaluar que un tratamiento que restringe derechos fundamentales resuelve un problema que debe ser real, presente o inminente, y crítico para el funcionamiento de la sociedad[27].

[25] «Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice» (Documento de reflexión sobre la interoperabilidad de los sistemas de información en el espacio de libertad, seguridad y justicia), 17 de noviembre de 2017
[26] The Sunday Times contra Reino Unido asunto nº 6538/74 (TEDH, jueves, 06 de noviembre de 1980), apartado 59.
[27] TEDH, Szabo y Vissy c. Hungría, apartado 73.

El TEDH[28] estableció que «necesario» «…no era sinónimo de indispensable…y tampoco tiene la flexibilidad de expresiones como 'admisible', 'ordinario', 'útil', 'razonable' o 'deseable'». No basta la mera conveniencia o rentabilidad[29].

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[30].

Hay que razonar la respuesta basándose en hechos a la pregunta siguiente (WP211): ¿El tratamiento está intentando abordar un problema que, si no se aborda, podría dar lugar a daños o tener efectos perjudiciales en la sociedad o una parte de la misma?

En el párrafo 3.15 del WP211 se pueden encontrar ejemplos.

2.- Hay que establecer la **idoneidad de una medida**: hay que evaluar que exista un vínculo lógico y directo entre el tratamiento y el objetivo perseguido.

3.- Hay que determinar la **eficacia real del tratamiento**, es decir, determinar mediante prueba que éste es capaz de alcanzar un nivel mínimo de efectividad en resolver la necesidad planteada.

Hay que aceptar la realidad de que en cualquier tipo de finalidad y para cualquier tratamiento es imposible alcanzar la perfección. Aparte de que no es eficiente desde el punto de vista económico, ni viable técnicamente, existen múltiples factores que impiden la eficacia total, especialmente en temas de seguridad. Asumiendo dicha realidad, hay que determinar el nivel aceptable de eficacia requerido para cumplir con la estricta necesidad y demostrar que el tratamiento propuesto lo alcanza.

4.- **Evaluación del nivel de intrusismo**. Estimando entre otros:

a.- La **naturaleza de la injerencia**: o como se limitan o se ponen en riesgo los derechos y libertades tal como se ha establecido en el apartado III.c.

b.- El **alcance/extensión** del tratamiento.

c.- El **contexto** en que la medida deberá aplicarse o la naturaleza de la actividad objeto de la medida[31].

c.- Si pueden aparecer «**intrusiones colaterales**», es decir, injerencias en la intimidad de personas distintas de los sujetos de la medida[32].

5.- **Mínimo intrusismo**: Hay que evaluar el alcance, la extensión y la intensidad de las interferencias en términos de impacto sobre los derechos fundamentales,

[28] Handyside contra Reino Unido asunto nº 5493/72 (TEDH, 7 de diciembre de 1976), apartado 48.
[29] Grupo de Trabajo del Artículo 29, Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, WP 193, 27.04.2012, p. 8.
[30] 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.
[31] En el asunto Dudgeon, el TEDH hizo hincapié en la naturaleza especialmente sensible de la actividad que se ve afectada, así como las circunstancias en que se aplicó la medida. Mientras que la sensibilidad de la actividad o la información en cuestión serán relevantes, es igualmente relevante considerar si una medida se aplicará en circunstancias en que las personas pueden tener unas expectativas elevadas de respeto de su intimidad.
[32] Véase Big Brother Watch y otros c. Reino Unido, TEDH, 13 de septiembre de 2018, apartado 2.43.

explicando con pruebas por qué otras alternativas posibles no son suficientes para satisfacer esta necesidad de forma suficiente:

a.- Entre las medidas ya existentes con relación a las propuestas, en particular, considerar una aplicación más adecuada que las medidas existentes.

b.- Entre las medidas propuestas con relación a otras opciones que permitan lograr el mismo objetivo, incluso con una combinación de medidas.

Con relación al nivel de eficacia requerido para cumplir con la estricta necesidad, hay que determinar que las medidas existentes no lo cumplían, y que las consecuencias que tenía ese no-cumplimiento ya no son asumibles.

Hito: Tomar una decisión («sí/no») sobre si el tratamiento cumple el principio de necesidad. Si el resultado es «no», es necesario reformar la norma y se detiene la evaluación de la EIPD.

E. EVALUACIÓN DE LA PROPORCIONALIDAD[33]

La protección de datos no es un derecho absoluto y puede limitarse siempre dentro de un justo equilibrio. Un tratamiento desarrollado en una norma debe respetar el principio de proporcionalidad lo que «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)»[34].

Como en el resto de las evaluaciones, evaluar la proporcionalidad no se reduce a simplemente una afirmación de la misma.

La evaluación de la proporcionalidad exige una valoración positiva de la evaluación de necesidad[35] y se nutre de las conclusiones derivadas de ésta. Por lo tanto:

---

[33] STJUE de 16 de julio de 2020, Schrems 2 (apartado 176): *Finalmente, para cumplir el requisito de proporcionalidad según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario, la normativa controvertida que conlleve la injerencia debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 140 y 141 y jurisprudencia citada).*
Conforme a la doctrina de nuestro Tribunal Constitucional, (STC 14/2003, de 28 de enero):*"En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; STC 66/1995, de 8 de mayo, F. 5; STC 55/1996, de 28 de marzo, FF. 7, 8 y 9; STC 270/1996, de 16 de diciembre, F. 4.e; STC 37/1998, de 17 de febrero, F. 8; STC 186/2000, de 10 de julio, F. 6)."*

[34] 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).

[35] En los asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland, el Tribunal de Justicia 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

1.- Utilizando el resultado de **evaluar la estricta necesidad** del tratamiento y **el nivel de intrusismo** realizado en la evaluación de la necesidad, hay que proceder a la **evaluación del equilibrio justo** (ventaja/desventaja; beneficio/coste individual y social) de la medida[36].

a.- El TJUE expuso que es fundamental señalar que la proporcionalidad es una **valoración en concreto,** y **caso por caso**[37].

b.- **Importancia de la finalidad**: hay que evaluar si, además de la estricta necesidad, la finalidad a cumplir trata de proteger un valor constitucional o un derecho fundamental.

b.- Hay que tomar en consideración **todas las circunstancias** del asunto del que conoce y **ser contextual**[38].

El derecho a la protección de datos personales puede desempeñar el papel de un derecho concurrente, es decir, no el que se ve principalmente afectado por la medida, pero que, sin embargo, junto con otros derechos (libertad de empresa; libertad de recibir o de comunicar información), puede inclinar la balanza a favor de la no proporcionalidad de la medida[39].

c.- Hay que determinar si está suficientemente **limitado el alcance** de los tratamientos propuestos. Esto puede cubrir el número de personas afectadas por la medida o la cantidad de información recogida o el período durante el cual se conservará esa información. El alcance puede abarcar la totalidad, parte o ninguno de estos elementos en función de la medida en cuestión.

d.- Hay que tener en cuenta la **opinión general** (aspectos sociales, históricos o políticos, etc.) de la sociedad sobre el tema en cuestión.

e.- Hay que tener debidamente en cuenta las **objeciones** expresadas por la sociedad.

En el párrafo 3.20 del WP211 se encuentran una serie de ejemplos.

f.- Hay que aplicar un **enfoque holístico**. A fin de poder afirmar si una nueva propuesta legislativa es proporcionada, es necesario evaluar la manera en que la nueva medida complementará a las ya existentes y si todas ellas en su conjunto seguirían limitando de manera proporcionada los derechos fundamentales en materia de protección de datos y vida privada (WP211 en el marco del párrafo 6.1).

En el párrafo 5.11 del WP211 hay un ejemplo sobre la limitación del alcance

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).

[36] 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*».

[37] TJUE, asunto C-101/01, Linqvist, ECLI:EU:C:2003:596, apartado 89.

[38] TEDH, M.K. c. Francia, apartado 46

[39] Scarlet Extended (TJUE, C-70/10, ECLI:EU:C:2011:771)

2.- Hay que evaluar qué «**salvaguardias**» acompañan a la medida para reducir los riesgos para los derechos fundamentales (Ver siguiente apartado).

Los pasos 1 y 2 pueden resultar reiterativos, es decir, si el tratamiento no resulta proporcional se pueden aplicar más salvaguardas y volver a realizar la evaluación del equilibrio justo.

3.- Tomar una decisión («sí/no») sobre si el tratamiento cumple el principio de proporcionalidad. Si el resultado es «no», entre otros motivos por no conseguir salvaguardias suficientes que puedan hacer que la medida sea proporcional, entonces será necesaria una nueva redacción de la norma.

F. SALVAGUARDAS

El art. 24.1 RGPD y el art. 27.1 L.O. 7/2021 establecen que el responsable del tratamiento **aplicará medidas** técnicas y organizativas **apropiadas**, teniendo **en cuenta** la **naturaleza, el ámbito/extensión[40], el contexto y los fines** del tratamiento así como **los riesgos** de diversa probabilidad y gravedad **para los derechos y libertades de las personas físicas**, a fin de **garantizar y poder demostrar[41]** que el tratamiento es conforme con la normativa de protección de datos. Dichas medidas se **revisarán** y **actualizarán** cuando sea necesario.

Habrá que revisarlas y actualizarlas, al menos, cuando cambie la naturaleza, el contexto, el ámbito/extensión, los fines o los riesgos. Además, en caso de medidas de seguridad, estas se tendrán que revisar de forma periódica (art. 32.1d RGPD).

Las medidas que se pueden incorporar a un texto normativo pueden tener ciertas especificidades con relación a un tratamiento.

En el capítulo VIII "Controles para disminuir el riesgo" de la guía Gestión del riesgo y EIPD, así como en las Guías de protección de datos por defecto y desde el diseño se encuentran enumeradas más de 200 medidas.

Entre estas especificidades, y a modo de ejemplo pues no es una lista ni exhaustiva ni exigible para todos los casos, se podrían encontrar:

- En cuanto a las medidas sobre el concepto del tratamiento:
  - Aplicación del principio de precaución[42]. Cuando sea difícil determinar de antemano alguno o parte de del impacto del tratamiento, se podría sugerir al legislador que adopte un «enfoque incremental», en el despliegue del tratamiento (limitación geográfica, en categorías de interesados, etc.), de manera que este despliegue incremental permita identificar casos de riesgo que no hubieran sido valorados

[40] Se utilizan ambas expresiones en la traducción del RGPD al castellano, y con ambas se establece de forma más precisa su extensión semántica.
[41] El texto "y estar en condiciones de demostrar" que aparece en el artículo 19.1 de la Directiva LED 680/2016 no se ha traspuesto al texto del artículo 27.1 de la L.O. 7/2021, aunque se presume que se debe interpretar en dicho sentido.
[42] El 2 de febrero de 2000, la Comisión Europea declaró en su Comunicación sobre el principio de precaución (COM(2000)1 final): «Aunque en el Tratado sólo se mencione explícitamente el principio de precaución en el terreno del medio ambiente, su ámbito de aplicación es mucho más amplio. Este principio abarca los casos específicos en los que los datos científicos son insuficientes, no concluyentes o inciertos, pero en los que una evaluación científica objetiva preliminar hace sospechar que existen motivos razonables para temer que los efectos potencialmente peligrosos para el medio ambiente y la salud humana, animal o vegetal pudieran ser incompatibles con el alto nivel de protección elegido.».

adecuadamente, mitigando de esta forma el posible impacto de estas consecuencias inicialmente no identificadas.

- Medidas Jurídicas:
  - Incorporar un sistema de supervisión independiente que evite que una medida temporal se convierta en permanente.
  - Establecer una caducidad total o parcial de los tratamientos en la misma norma (p.ej. cláusulas de extinción «a menos que se confirme o revise, la medida ya no resultará aplicable a partir de …»)
  - Implementar un control judicial previo de los tratamientos efectuados[43] en los supuestos de mayor injerencia en los derechos y libertades[44].
- Medidas organizativas y de gobernanza:
  - Establecimiento de obligaciones de realizar EIPD y/o Consultas Previas a los sujetos obligados por la norma a implementar parte o totalmente el tratamiento.
  - Revaluación periódica de la necesidad y proporcionalidad del tratamiento.

Hay un ejemplo en el párrafo 5.16 del WP211

  - Evaluación periódica de las salvaguardas establecidas.
  - Auditorías de la implementación concreta de los tratamientos por terceros independientes
- Medidas de protección de datos desde el diseño y por defecto:
  - Limitar la conservación de los datos, incluyendo la anonimización, seudonimización, eliminación selectiva de atributos sensibles, u otros en función de su contribución efectiva a los fines perseguidos.

- Hay un ejemplo en el párrafo 5.17 del WP211

  - Limitar la extensión de los individuos afectados (por ejemplo: determinadas categorías de personas, usuarios de un servicio, sospechosos de un delito, extranjeros, nacionales, etc.).
  - Incorporar garantías adicionales según las categorías de interesados (p.ej., para colectivos vulnerables que estén dentro del ámbito de aplicación).
  - Incorporar garantías adicionales en caso de, p.ej., decisiones automatizadas.
  - Limitar las categorías de datos recogidos (p.ej. en videovigilancia se puede procesar vídeo, audio, temperatura, biometría, etc.).
  - Diferenciar, limitar y someter a excepciones a las personas cuya información se utilice en función del objetivo buscado[45].
  - Limitar la extensión geográfica.

[43] SEPD, alegato en la vista oral en el caso del proyecto de acuerdo PNR UE-Canadá, disponible en: https://secure.SEPD.europa.eu/SEPDWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2016/16-04-05_Pleading_Canada_PNR2_EN.pdf.
[44] TJUE, asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland
[45] TJUE, asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland, apartado 57; C-362/14 Schrems, apartado 93.

- Limitar la extensión de las conductas afectadas.
- Limitar las operaciones posibles en el tratamiento (p.ej. con relación a analizar, combinar y comunicar la información.)
- Limitar el periodo de tratamiento de los datos, reduciendo este de un largo plazo a un corto plazo.
- Bloqueo rápido de los datos.
- Establecer políticas de acceso restrictivas para los datos conservados.
- Establecer procedimientos supervisados y no automáticos para el acceso a datos conservados.
- En relación al anterior punto, incrementar los requisitos de nivel de acceso a datos conservador con criterios temporales.
- Guardar registro detallado de quién accede a los datos.
- Guardar registro detallado de comunicación de datos entre entidades públicas.

- Gestión de brechas de datos personales
  - Ampliar las obligaciones establecidas en los arts. 33 y 34 del RGPD y 38 y 39 de la L.O. 7/2021.

IV. EVALUACIÓN DE LA CALIDAD DE LA EIPD

La EIPD realizada en el marco del desarrollo normativo ha de cumplir con los siguientes requisitos para ser considerada aceptable:

- Ser realizada desde el diseño de la norma e incorporarse a la Memoria de Análisis de Impacto Normativo.
- Dar respuesta a todas las cuestiones identificadas en los capítulos II y III.
- Superar los hitos establecidos en los capítulos señalados.
- Basar todas las respuestas en las pruebas adecuadas, estableciendo que se han realizado las evaluaciones requeridas en estas orientaciones y conservando (registrando y almacenando) toda la documentación relevante obtenida o producida durante la realización de las evaluaciones y la redacción del Informe sobre la EIPD. Dicha documentación deberá ser pertinente y suficiente para justificar, o identificar las cuestiones críticas de la medida que se examina, y debe mencionarse en un anexo del informe.
- Alcanzar una simetría de información, por ejemplo, en la evaluación de proporcionalidad, en caso de haber beneficios conocidos, pero costes desconocidos, o viceversa, será difícil, si no imposible, establecer si la medida es proporcionada. (Paso III.6.3 de la Guía de Proporcionalidad del SEPD). De igual forma puede ocurrir en la evaluación de la medida menos intrusiva.

Hito: En el caso de que no se cumplan las condiciones anteriores se presumirá que la EIPD no ha sido correctamente realizada y se tendrá que revisar.

V. CONCLUSIONES

La EIPD de una norma en la que se plantean tratamientos de datos personales ha de evaluar el impacto que estos tienen sobre los derechos y libertades fundamentales de las

personas tomadas individualmente y como sociedad. Por lo tanto, no es una evaluación del riesgo legal o de cumplimiento.

La jurisprudencia del TJUE y del TEDH indica que la necesidad y proporcionalidad en la normativa de protección de datos es un concepto basado en los hechos, más que una noción jurídica meramente abstracta, y que el tratamiento 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 (apartado II.6 de la Guía de Necesidad del SEPD).

La EIPD de una norma en la que se plantea un tratamiento de datos personales no es un informe jurídico que justifica un tratamiento desde una posición de inmutabilidad de la idea preestablecida. Aunque tiene una parte de análisis jurídico muy importante, también tiene una parte de gestión de limitaciones y riesgos para los derechos y libertades fundamentales, de medidas de gestión organizativa y además un planteamiento de medidas jurídicas y técnicas.

La EIPD requiere aplicar una metodología paso a paso, no es una actividad que se pueda automatizar, aunque se pueden emplear herramientas que ayuden en el proceso de realizarla, como Evalúa-Riesgo[46].

Finalmente, señalar que en el Área de Administraciones Públicas de la página web de la AEPD, se recogerán los informes del Gabinete Jurídico más relevantes con relación a la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo.

VI. MATERIAL PARA DAR SOPORTE A ESTAS OBLIGACIONES

En la página web de la AEPD se pueden encontrar recursos que amplían el contenido de estas orientaciones o ayudan a la ejecución de la EIPD en la MAIN:

A. GENERAL DEL RIESGO

- Gestión del riesgo y evaluación de impacto en tratamientos de datos personales
- Relación de tablas de la guía de Gestión del riesgo y evaluación de impacto en formato editable
- Lista de verificación para determinar la adecuación formal de una EIPD y la presentación de consulta previa
- Herramienta EVALUA-RIESGO v2 para el análisis de los factores de riesgo

B. ESPECÍFICA PARA LAS AA.PP.

- Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para Administraciones Públicas
- Guía de Tecnologías y Protección de Datos en las AA.PP

[46] Las herramientas Facilita o Gestiona no son adecuadas para la EIPD de una norma.

C. ESPECÍFICA PARA EL DESARROLLO NORMATIVO

- SEPD: Guía para evaluar la necesidad de los tratamientos en políticas y medidas legislativas
- SEPD: Guía para evaluar la proporcionalidad de los tratamientos en políticas y medidas legislativas
- WP29: Dictamen 01/2014 sobre la aplicación de los conceptos de necesidad y proporcionalidad y la protección de datos en el sector de los organismos con funciones coercitivas (WP211)