0024/2026

Antes de entrar a analizar el texto sometido a informe es preciso señalar que, habida cuenta de la fundamentación legal del informe que inmediatamente va a evacuarse y su carácter preceptivo, a tenor de lo dispuesto en las normas que acaban de señalar, debería indicarse en la Exposición de Motivos de la norma que la misma ha sido sometida al previo informe de la Agencia Española de Protección de Datos.

I

El proyecto de Real Decreto (en adelante, el Reglamento) desarrolla lo dispuesto en la disposición adicional centésima cuadragésima primera y en la disposición transitoria tercera de la **Ley 6/2018, de 3 de julio, de Presupuestos Generales del Estado para el año 2018**. Esta ley creó la **Tarjeta Social Digital** (TSD) como un sistema de información compartida entre el Estado, las comunidades autónomas y las entidades locales para la mejora y coordinación de las políticas de protección social. El mandato legal establece la necesidad de regular reglamentariamente el procedimiento para que la ciudadanía tenga acceso a sus utilidades, la determinación de situaciones subjetivas relevantes (como discapacidad, dependencia o niveles de renta) y el calendario para la integración gradual de las prestaciones sociales públicas de carácter económico. Según expone la Memoria del Análisis de Impacto Normativo, la aprobación de esta norma es además necesaria para sustituir al actual **Registro de Prestaciones Sociales Públicas**, integrando su contenido en el nuevo sistema informático gestionado por el Instituto Nacional de la Seguridad Social. Además, se enmarca en el Plan de Recuperación, Transformación y Resiliencia, concretamente en la reforma 1 del Componente 11, que busca la modernización y digitalización de la Administración Pública.

El texto que se informa consta de un artículo único que aprueba el Reglamento adjunto, dos disposiciones adicionales, una disposición derogatoria y tres disposiciones finales. Por su parte, el Reglamento que se aprueba se estructura en 5 capítulos y 19 artículos.

Tras definir en su artículo 1 el objeto y usos de la Tarjeta Social Digital, el artículo 2 establece que la administración y gestión del sistema corresponde al **Instituto Nacional de la Seguridad Social**. El artículo 3 delimita el ámbito de aplicación subjetivo y el artículo 4 define las entidades responsables y las prestaciones sociales públicas que deben ser objeto de inscripción. El capítulo

II se dedica al contenido del sistema, especificando los datos identificativos de los beneficiarios y las prestaciones, mientras que el capítulo III regula el suministro de información y el procedimiento de integración gradual de los datos. Por su parte, el capítulo IV detalla las funcionalidades y utilidades de la tarjeta para los ciudadanos y las administraciones. Finalmente, el capítulo V garantiza el régimen de protección de datos personales y el ejercicio de los derechos de acceso, rectificación, supresión y oposición por parte de los interesados.

En cuanto al encuadre de competencias, el Real Decreto se dicta al amparo del **artículo 149.1.1.ª de la Constitución Española**, que atribuye al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de sus derechos y el cumplimiento de sus deberes constitucionales

II

En primer lugar, debe partirse de la naturaleza reglamentaria del proyecto informado y de la vigencia del principio de reserva de ley en materia de limitación del derecho fundamental a la protección de datos personales, conforme al artículo 53.1 de la Constitución y al artículo 8 de la LOPDGDD. Según reiterada doctrina del Tribunal Constitucional, no solo es necesaria una habilitación legal para legitimar la injerencia, sino que dicha norma debe reunir condiciones de calidad normativa suficientes, expresando los presupuestos, condiciones y garantías de la intervención (por todas, SSTC 49/1999 y 292/2000). Asimismo, la regulación debe respetar en todo caso el principio de **proporcionalidad** (STC 14/2003).

En este contexto, el Tribunal Constitucional ha admitido la intervención reglamentaria en materias vinculadas a la reserva de ley, pero únicamente con carácter complementario y subordinado a una regulación legal suficiente, sin que pueda suponer una deslegalización de los elementos esenciales del derecho fundamental (STC 292/2000). En consecuencia, la remisión al reglamento debe limitarse a aspectos técnicos o de desarrollo, sin desplazar al legislador en la determinación de los límites y garantías del tratamiento.

Desde la perspectiva del RGPD, el artículo 6.1 establece las condiciones de licitud del tratamiento, mientras que su apartado 3 exige que la base jurídica, cuando el tratamiento se funde en el cumplimiento de una obligación legal o en una misión de interés público, se establezca en una norma con rango adecuado que determine la finalidad del tratamiento y pueda concretar aspectos como las condiciones de licitud, los tipos de datos tratados, los interesados afectados, las comunicaciones de datos, los plazos de conservación o las garantías aplicables. En la misma línea, el Considerando 45

del RGPD exige que este tipo de tratamientos tenga fundamento en el Derecho de la Unión o de los Estados miembros.

Por su parte, el artículo 8 de la LOPDGDD refuerza esta exigencia al disponer que los tratamientos basados en obligación legal o misión de interés público deben derivar de una norma con rango de ley, que podrá establecer las condiciones del tratamiento y las garantías correspondientes.

Desde esta base, procede analizar la **necesidad** del tratamiento proyectado. Conforme a la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE), en particular en el asunto Huber contra Alemania, el tratamiento de datos personales debe limitarse a lo estrictamente necesario para alcanzar la finalidad perseguida, sin que puedan tratarse más datos de los imprescindibles. Esta misma exigencia se reitera en el asunto Rīgas satiksme, que subraya que las excepciones al derecho a la protección de datos no pueden exceder de lo estrictamente necesario.

Desde esta perspectiva, el sistema de Tarjeta Social Digital puede considerarse, en términos generales, idóneo para mejorar la interoperabilidad administrativa, facilitar la coordinación entre Administraciones públicas y reducir cargas administrativas para los ciudadanos, en línea con el principio de “solo una vez” previsto en el artículo 28 de la Ley 39/2015.

No obstante, podemos ya anticipar que el proyecto objeto de este informe no justifica de forma suficientemente individualizada por qué todas las categorías de datos previstas resultan estrictamente necesarias para cada una de las funcionalidades del sistema, ni delimita adecuadamente qué entidades pueden acceder a qué información y para qué fines concretos.

En particular, aunque pueden derivarse efectos como el control de duplicidades o la detección de irregularidades, estos no aparecen expresamente definidos como finalidades autónomas, lo que plantea dudas sobre su cobertura jurídica. Esta indeterminación afecta directamente a la posibilidad de evaluar la proporcionalidad del tratamiento y su adecuación al principio de minimización.

Asimismo, la comunicación de datos entre Administraciones constituye un tratamiento autónomo que debe contar, en cada caso, con una **base jurídica** específica conforme al artículo 6 del RGPD. A este respecto, la jurisprudencia del TJUE, en particular en el asunto Smaranda Bara, ha establecido que la transmisión de datos entre organismos públicos debe respetar los principios de protección de datos, contar con habilitación normativa suficiente y cumplir las obligaciones de información a los interesados.

El artículo 6.3 del RGPD exige que la norma habilitante determine con un grado suficiente de precisión determinados elementos esenciales del tratamiento, entre ellos las finalidades perseguidas, las categorías de datos objeto de tratamiento, los interesados afectados, las entidades destinatarias de los datos, los supuestos de comunicación y las garantías aplicables. Tales exigencias responden al principio de predeterminación normativa derivado del artículo 53.1 CE y de la doctrina constitucional y europea relativa a las limitaciones del derecho fundamental a la protección de datos.

En este punto, el proyecto presenta determinadas insuficiencias regulatorias que a continuación se van a analizar. Aunque identifica una finalidad general legítima (coordinación, interoperabilidad y mejora de la gestión de prestaciones sociales), la configuración de algunas funcionalidades y usos del sistema aparece formulada en términos amplios, sin delimitar con suficiente precisión los concretos tratamientos habilitados, los distintos accesos interadministrativos o los supuestos específicos de reutilización de la información.

Determinadas funcionalidades de supervisión administrativa, verificación de incompatibilidades o prevención del fraude pueden considerarse vinculadas a las competencias públicas en materia de gestión de prestaciones sociales, pero el Reglamento no delimita con suficiente precisión el alcance material de dichas finalidades ni las concretas operaciones de tratamiento que podrían ampararse en ellas

En consecuencia, aunque el tratamiento puede incardinarse, con carácter general, en el artículo 6.1.e) RGPD (misión en interés público), la amplitud en la definición de finalidades y funcionalidades dificulta verificar el cumplimiento de los principios de necesidad y proporcionalidad, especialmente en relación con accesos interadministrativos y tratamientos masivos.

En relación con las **categorías especiales de datos**, en el Reglamento que establece la TSD son objeto de tratamiento datos relativos a la salud, como son el grado de discapacidad y la situación de dependencia (artículo 8.2. 3º y 4º). Si bien el artículo 9.1 del RGPD prohíbe con carácter general el tratamiento de estos datos, la TSD se ampara en la excepción del artículo 9.2.g) del RGPD: "*el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros...”*

El artículo 4.15 del RGPD define como «datos relativos a la salud», como “*aquellos datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud”*

Por su parte el Considerando (35): "*Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. (…) todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro*."

De lo expuesto debe concluirse que la información relativa a la condición de discapacidad de una persona es un dato de salud, y por tanto debe incluirse dentro de las "categorías especiales de datos" de acuerdo con el artículo 9 del RGPD.

Del mismo modo, esta Agencia ha señalado que la información sobre el grado de dependencia y las prestaciones asociadas puede revelar datos sobre la salud presente, pasada o futura de la persona, por lo que su tratamiento debe cumplir con las garantías establecidas para los datos de salud (Informe 2013-0133): "*De este modo, la Ley consagra como derecho esencial de las personas con dependencia su derecho a la protección de datos de carácter personal, lo que resulta de lógica inclusión en el artículo 4, teniendo en cuenta que la condición de persona dependiente implicará la existencia de determinada información relacionada con la salud de la misma, respecto de la que el artículo 7.3 de la Ley Orgánica 15/1999 impone un deber especial de protección, que justifica la exigencia de la concurrencia del consentimiento del interesado o de una habilitación legal específica para que dichos datos puedan ser objeto de tratamiento. Del mismo modo, esta especial protección se materializa en la exigencia de medidas de seguridad de nivel alto en el tratamiento de esos datos, de conformidad con lo establecido en el artículo 81.3 del reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1721/2007, de 21 de diciembre*."

También son objeto de tratamiento datos relativos a los ingresos declarados en el IRPF: "*Para el nivel de rentas: la base imponible general y del ahorro correspondiente a la última declaración de renta., cuantía de las prestaciones sociales"* (artículo 8.2. 1º), así como una numerosa serie de datos relativos a cada prestación social pública de carácter económico de la que el interesado sea titular. Sin ser datos incluidos en las categorías especiales de datos del artículo 9.1 del RGPD, el tratamiento de estos datos conlleva un alto riesgo para los derechos y libertades de los interesados, tal como establece la doctrina del Comité Europeo de Protección de Datos (CEPD) en sus Directrices

07/2020 y, especialmente, en el Dictamen 248/2020 (WP248), donde se señala que:

"El tratamiento de datos personales de personas en situación de vulnerabilidad (económica, social, sanitaria, etc.) puede suponer un alto riesgo para sus derechos y libertades, especialmente cuando se trata de categorías especiales de datos o datos que revelen aspectos sensibles de su vida privada."

Por último, las personas en situación de vulnerabilidad económica pueden encontrarse en una posición de desequilibrio frente a las administraciones, lo que puede dificultar la comprensión sobre cómo se tratarán sus datos (falta de transparencia) y la posibilidad de ejercer sus derechos (ej. acceso, rectificación, supresión) debido a barreras administrativas o falta de información clara.

La TSD tratará datos de menores de edad, como los hijos a cargo en familias numerosas. El Considerando 38 del RGPD destaca que los menores merecen protección específica porque: "*Pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de sus datos personales".* Los datos de menores solo podrán tratarse para fines específicos y justificados, evitando usos secundarios no autorizados. Si la TSD incluye datos de menores beneficiarios de ayudas familiares, debe garantizarse que solo se recojan datos imprescindibles (ej. nombre, fecha de nacimiento, relación familiar) y se informará a los padres/tutores sobre el tratamiento y sus derechos (art. 13 RGPD).

Por último, la TSD supone el tratamiento a gran escala de numerosas categorías de datos de los interesados, teniendo en cuenta el ámbito de aplicación de la TSD, definido en el artículo 3 del Reglamento que incluirá prestaciones sociales públicas de contenido económico (contributivas, no contributivas y asistenciales) y las situaciones subjetivas relevantes: niveles de renta, grado de discapacidad, dependencia, demanda de empleo, familia numerosa, trabajador autónomo, etc. así como todas las categorías de datos recogidas en el artículo 8 del Reglamento.

El tratamiento de datos personales relativos a la salud, a personas en situación de vulnerabilidad, a menores de edad y el tratamiento a gran escala de numerosas categorías de datos de los ciudadanos presenta una especial relevancia en RGPD, en la medida en que puede incrementar la probabilidad de que se produzcan los riesgos a los que se refiere su Considerando 75: "*Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de*

discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados."

Asimismo, para el tratamiento de categorías especiales de datos, la doctrina del Tribunal Constitucional, especialmente la STC 76/201, exige que la ley incorpore de forma expresa las garantías adecuadas, sin que puedan diferirse a desarrollos reglamentarios. Esta exigencia se ve reforzada por la jurisprudencia del TJUE (por ejemplo, asuntos Privacy International y La Quadrature du Net), que insiste en que cualquier limitación del derecho fundamental debe estar definida con claridad en la propia norma habilitante y circunscribirse a lo estrictamente necesario.

En este marco, la habilitación contenida en la Ley 6/2018 permite fundamentar, en términos generales, la base de licitud del tratamiento, pero su remisión amplia a desarrollos reglamentarios, especialmente respecto a "situaciones subjetivas relevantes", plantea dudas desde la perspectiva de la predeterminación normativa exigida cuando el tratamiento afecta a categorías especiales de datos.

En consecuencia, sin cuestionar la existencia de una habilitación legal general ni la posible concurrencia de la excepción del artículo 9.2.g) del RGPD, se considera conveniente que el desarrollo reglamentario incorpore una delimitación más precisa de las categorías especiales de datos tratadas, así como de la habilitación legal que permita entender levantada la prohibición general de tratamiento de datos sensibles prevista en el artículo 9.1 RGPD al concurrir alguno de los supuestos contemplados en el artículo 9.2 RGPD.

El artículo 2 atribuye la gestión de la TSD al Ministerio de Inclusión, Seguridad Social y Migraciones, a través del INSS, el cual será responsable del diseño, gestión y mantenimiento de la infraestructura de la TSD, determinando

los elementos esenciales del tratamiento vinculados al funcionamiento del sistema. De este modo, el INSS está correctamente identificado como **responsable del tratamiento**, pero no se aclara el papel de las entidades colaboradoras (comunidades autónomas, mutualidades…) que suministran datos relativos a la TSD.

El artículo menciona que el INSS podrá requerir la colaboración de otras administraciones, pero no se especifica cómo se garantizará el cumplimiento del RGPD en estas colaboraciones, especialmente en lo relativo a la seguridad de los datos y el ejercicio de derechos por los interesados, por lo que resulta necesario que sea analizada la posición del INSS y del resto de Administraciones y entidades participantes en el sistema.

No obstante, las restantes Administraciones públicas y entidades intervinientes, en particular las comunidades autónomas y mutuas colaboradoras, no pueden ser consideradas, con carácter general, como encargadas del tratamiento del INSS, en la medida en que no actúan siguiendo sus instrucciones, sino en el ejercicio de sus propias competencias y para finalidades propias, consistentes en la gestión de las prestaciones de su ámbito respectivo.

Asimismo, tampoco cabe apreciar, de forma automática, la existencia de una relación de corresponsabilidad en los términos del artículo 26 del RGPD, dado que no se observa una determinación conjunta de los fines y medios del tratamiento, sino una concurrencia de tratamientos vinculados a un mismo sistema, pero con finalidades diferenciadas y bajo el control de cada entidad en el ámbito de sus competencias.

En este contexto, las distintas entidades intervinientes deben ser consideradas, con carácter general, como responsables independientes respecto de los tratamientos que llevan a cabo, lo que implica que cada una de ellas debe contar con una base jurídica propia, determinar las finalidades de sus tratamientos y asumir las responsabilidades derivadas del cumplimiento de la normativa de protección de datos.

No obstante, la existencia de un sistema común que permite el acceso y la interconexión de datos entre múltiples entidades exige una delimitación precisa de las responsabilidades de cada uno de los intervinientes, así como la articulación de mecanismos de coordinación que garanticen el cumplimiento efectivo de las obligaciones establecidas en el RGPD, en particular en lo relativo al ejercicio de derechos por parte de los interesados, la seguridad del tratamiento y la trazabilidad de los accesos.

En consecuencia, si bien el modelo no responde a un supuesto de corresponsabilidad en sentido estricto, **la complejidad del sistema requiere**

una regulación más detallada que permita identificar con claridad las funciones y responsabilidades de cada entidad interviniente, evitando situaciones de indeterminación que puedan comprometer la protección de los datos personales.

No consta en la documentación analizada la realización de una **evaluación de impacto en protección de datos** (EIPD) en los términos exigidos por el artículo 35 del RGPD, ni se aportan elementos suficientes que permitan inferir su existencia o contenido, respecto de los riesgos asociados a los tratamientos de datos, amplios, variados y que afectan de manera importante al derecho fundamental a la protección de datos, que la norma proyectada conlleva.

En el Reglamento concurren varios criterios del artículo 35 del RGPD y de las directrices del Comité Europeo de Protección de Datos que apuntan claramente a su procedencia: tratamiento a gran escala, interconexión de múltiples Administraciones, utilización de información relativa a situaciones subjetivas que pueden revelar categorías especiales de datos, tratamiento de colectivos potencialmente vulnerables y elaboración de visiones agregadas sobre la situación socioeconómica de los ciudadanos. El artículo 35 del RGPD dispone lo siguiente:

"*1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.*

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o […]"

El Grupo de Trabajo del Artículo 29 (GT 29), antecesor del Comité Europeo de Protección de Datos, cuyos Dictámenes y Directrices mantienen su vigencia y relevancia jurídica siempre que su contenido no resulte incompatible con el marco normativo actual, en las "*Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679"* señala que:

"*Con el fin de ofrecer un conjunto más concreto de operaciones de tratamiento que requieran una EIPD debido a su inherente alto riesgo, teniendo en cuenta los elementos particulares del artículo 35, apartado 1, y del artículo 35, apartado 3, letras a) a c), la lista que debe adoptarse a nivel nacional en virtud del artículo 35, apartado 4, y los considerandos 71, 75 y 91, y otras referencias del RGPD a operaciones de tratamiento14 que «probablemente entrañen un alto riesgo», se deben considerar los nueve criterios siguientes:*

[…]

4. Datos sensibles o datos muy personales: esto incluye las categorías especiales de datos personales definidas en el artículo 9 (por ejemplo, información sobre las opiniones políticas de las personas), así como datos personales relativos a condenas e infracciones penales según la definición del artículo 10. Un ejemplo sería un hospital general que guarda historiales médicos de pacientes o un investigador privado que guarda datos de delincuentes. Más allá de estas disposiciones del RGPD, puede considerarse que algunas categorías de datos aumentan el posible riesgo para los derechos y libertades de las personas. Estos datos personales se consideran sensibles (dado que este término es de uso común) porque están vinculados a hogares y actividades privadas (como comunicaciones electrónicas cuya confidencialidad debe ser protegida), porque afectan al ejercicio de un derecho fundamental (como datos de localización cuya recogida compromete la libertad de circulación) o porque su violación implica claramente graves repercusiones en la vida cotidiana del interesado (como datos financieros que podrían usarse para cometer fraude en los pagos). En este sentido, puede resultar relevante que los datos ya se hayan hecho públicos por el interesado o por terceras personas. El hecho de que los datos personales sean de acceso público puede considerarse un factor en la evaluación si estaba previsto que estos se usaran para ciertos fines. Este criterio también puede incluir datos tales como documentos personales, correos electrónicos, diarios, notas de lectores de libros electrónicos equipados con opciones para tomar notas e información muy personal incluida en aplicaciones de registro de actividades vitales.

5. Tratamiento de datos a gran escala: el RGPD no define qué se entiende por gran escala, aunque el considerando 91 ofrece alguna orientación. En cualquier caso, el GT29 recomienda que se tengan en cuenta los siguientes factores, en particular, a la hora de determinar si el tratamiento se realiza a gran escala:

a. el número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;

b. el volumen de datos o la variedad de elementos de datos distintos que se procesan;

c. la duración, o permanencia, de la actividad de tratamiento de datos;

d. el alcance geográfico de la actividad de tratamiento.

6. Asociación o combinación de conjuntos de datos, por ejemplo procedentes de dos o más operaciones de tratamiento de datos realizadas para distintos fines o por responsables del tratamiento distintos de una manera que exceda las expectativas razonables del interesado.

7. Datos relativos a interesados vulnerables (considerando 75): El tratamiento de este tipo de datos representa un criterio debido al aumento del desequilibrio de poder entre los

interesados y el responsable del tratamiento, lo cual implica que las personas pueden ser incapaces de autorizar o denegar el tratamiento de sus datos, o de ejercer sus derechos. Entre los interesados vulnerables puede incluirse a niños (se considera que no son capaces de denegar o autorizar consciente y responsablemente el tratamiento de sus datos), empleados, segmentos más vulnerables de la población que necesitan una especial protección (personas con enfermedades mentales, solicitantes de asilo, personas mayores, pacientes, etc.), y cualquier caso en el que se pueda identificar un desequilibrio en la relación entre la posición del interesado y el responsable del tratamiento."

Es de recordar que el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, de aplicación a todo el sector público (art. 2), establece que:

> *1.* ***Cuando un sistema de información trate datos personales*** *le será de aplicación lo dispuesto en 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) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, 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, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto.*
>
> *2.* ***En estos supuestos****, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos,* ***realizarán un análisis de riesgos*** *conforme al artículo 24 del Reglamento General de Protección de Datos* ***y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.***
>
> *3. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el presente real decreto.*

Desde un punto de vista práctico, esta Agencia ha publicado su **Guía** denominada **"*Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo*"** [1], que 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 normativas de las Administraciones Públicas implican el tratamiento de datos personales. 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 RGPD, así

[1] https://www.aepd.es/es/documento/orientaciones-evaluacion-impacto-desarrollo-normativo.pdf

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.

En esta "Guía" se contienen, con profundidad y rigor, los pasos o el método a seguir para determinar la necesidad y el contenido de la Evaluación de Impacto, y entre ellos esta AEPD desea resaltar en este momento el apartado D del epígrafe II del mismo, relativo a las características de la norma que ampara el tratamiento:

> ***"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, el TJUE y el Tribunal Constitucional (TC). Por lo tanto,* ***en la norma han de estar claramente definidos, con precisión y apropiadamente:***
>
> *1.- La finalidad o finalidades del tratamiento.*
>
> *2.- La legitimidad del tratamiento.*
>
> *3.- La descripción de la implementación 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.*
>
> *4.- El ámbito y extensión del tratamiento con relación a las categorías de datos personales tratados (especialmente si son categorías especiales), las categorías de interesados afectados, 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.*
>
> *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.*

7.- La justificación de la solución adoptada para el acceso 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.

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.*

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.

Por su parte, el art. 25 RGPD establece la necesidad de la protección de datos "desde el diseño" de los tratamientos, y la necesidad de tener en cuenta los **riesgos** que se derivan de estos:

"Artículo 25. Protección de datos desde el diseño y por defecto

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los ***riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas,*** *el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados."*

En el marco del principio de responsabilidad proactiva consagrado en el art. 25 del RGPD, resulta necesario distinguir entre el análisis de riesgos y la evaluación de impacto en protección de datos, instrumentos ambos orientados a garantizar la protección de los derechos y libertades de las personas físicas, pero con distinto alcance y régimen jurídico.

El análisis de riesgos constituye una obligación general inherente a todo tratamiento de datos personales, derivada de lo dispuesto en los artículos 24, 25 y 32 del RGPD. A través de este proceso, el responsable y, en su caso, el encargado, identifican y valoran los riesgos asociados al tratamiento, determinando las medidas técnicas y organizativas apropiadas para mitigarlos

en función de su probabilidad y gravedad. Se trata, por tanto, de un instrumento de carácter continuo y transversal, aplicable a cualquier tratamiento con independencia de su naturaleza.

Por su parte, la evaluación de impacto en protección de datos, regulada en el artículo 35 del RGPD, constituye un mecanismo específico que debe llevarse a cabo únicamente en aquellos supuestos en los que el tratamiento pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas. A diferencia del análisis de riesgos, la evaluación de impacto presenta un carácter formalizado y reforzado, exigiendo una descripción sistemática del tratamiento, una evaluación detallada de su necesidad y proporcionalidad, así como la identificación de los riesgos específicos y las medidas previstas para afrontarlos.

En consecuencia, ambos instrumentos no son alternativos, sino complementarios, de modo que el análisis de riesgos actúa como presupuesto general del que puede derivarse, en caso de apreciarse un alto riesgo, la obligación de realizar una evaluación de impacto.

Dicho análisis de riesgos no parece haberse llevado a cabo por el órgano proponente de este proyecto normativo. En el caso del proyecto analizado, atendiendo a la naturaleza del tratamiento, caracterizado por su alcance masivo, la posible inclusión de datos de carácter sensible y la interconexión de múltiples Administraciones públicas, cabe concluir que no solo resulta exigible la realización de un análisis de riesgos, sino también la elaboración de una EIPD, de conformidad con el artículo 35 del RGPD.

Esta Agencia viene recomendando repetidamente en sus informes que el prelegislador, en aquellos casos, como el presente, en que los tratamientos puedan tener como base jurídica el art. 6.1.c) o e) del RGPD (esto es, tratamientos cuya base es una obligación legal o una misión de interés público), y venga establecida por el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento y tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, **haga uso de la posibilidad que establece el art. 35.10 RGPD de modo que sea el propio órgano proponente de la disposición general, -en vez de a posteriori los responsables de los tratamientos- quien realice en el curso del procedimiento de creación de la norma una evaluación de impacto relativa a la protección de datos (EIPD) como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica.**

Dicha EIPD habrá de incorporarse tal y como establece el art. 2.1, letra g), del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo. Este precepto es suficientemente

expresivo de la voluntad del legislador de incluir en las Memorias justificativas de los proyectos normativos, (en el caso del Estado, la Memoria de Análisis de Impacto Normativo, MAIN), dentro del concepto “Otros impactos”, el análisis del “*impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma*”:

> *g) Otros impactos:* ***La memoria*** *del análisis de impacto normativo* ***incluirá*** *cualquier otro extremo que pudiera ser relevante a criterio del órgano proponente, prestando especial atención a los* ***impactos de carácter social*** *y medioambiental, al impacto en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y al* ***impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma.***

Esta Agencia recuerda, asimismo, que el reiterado Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) establece que la política de seguridad del sistema de información deberá examinar y tener en cuenta “*los riesgos que se derivan del tratamiento de los datos personales*” (art. 12.1.f)), así como que en caso de que los sistemas de información traten datos personales (como es el caso), en todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto en caso de resultar agravadas respecto de las previstas en el citado Real Decreto (art. 3.3), análisis de riesgos y evaluación de impactos en protección de datos que, al no haberse realizado, o no constar haberlos realizados, no permiten saber si las medidas a implantar serían o no las correctas, ni tampoco la suficiencia de las mismas.

En definitiva, esta AEPD recomienda que se lleven a cabo, y se incorporen a la Memoria justificativa del proyecto el análisis de riesgos (arts. 25 y 32 del RGPD) y la evaluación de impacto relativa a la protección de datos (art. 35 RGPD). Ello permitirá al propio prelegislador, determinar no sólo las medidas de seguridad necesarias en los sistemas de información, sino las garantías específicas que se requieran para afrontar los riesgos derivados del tratamiento de los datos que el proyecto de Real Decreto establece (ver art. 35.7.d) RGPD). Como hemos mencionado más arriba, al no constar la existencia de una EIPD en el presente caso, no se conocen cuáles son esos riesgos susceptibles de derivarse de los tratamientos de datos personales que establece la norma, por lo que tampoco en la norma es posible recoger las posibles medidas y garantías que paliarían esos riesgos, ni tampoco valorar su corrección y suficiencia.

Corresponde al responsable del tratamiento, en virtud del principio de responsabilidad proactiva (art. 24.1 RGPD) el establecimiento de las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD, teniendo en cuenta la naturaleza, el ámbito, 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, y que ello habrá de hacerlo "desde el diseño" del tratamiento (art. 25.1 RGPD), integrando las garantías en el tratamiento; todo lo cual aconseja que las garantías para minimizar los riesgos, una vez conocidos y ponderados en la EIPD tras el correspondiente análisis de riesgos, se incorporasen a este borrador normativo.

Dicho análisis de riesgos y evaluación de impacto deberían de llevarse a cabo con la ayuda del Delegado de Protección de datos correspondiente.

La ausencia de EIPD resulta especialmente relevante habida cuenta de las características del tratamiento previsto, que incluye la gestión de un sistema de información de alcance masivo, la posible incorporación de categorías de datos especialmente protegidas y la interconexión de múltiples Administraciones públicas, factores todos ellos que, conforme a las directrices del Comité Europeo de Protección de Datos, determinan la concurrencia de un alto riesgo para los derechos y libertades de las personas físicas.

En este sentido, la inexistencia de una evaluación de impacto o la falta de referencia a la misma en el proyecto normativo impide verificar adecuadamente la necesidad y proporcionalidad del tratamiento, así como la idoneidad de las medidas previstas para mitigar los riesgos identificados, lo que podría comprometer el cumplimiento de las exigencias derivadas del RGPD.

Aunque el artículo 6 dispone que la TSD observará las **garantías de seguridad**, integridad, confidencialidad y disponibilidad previstas en el RGPD, en la LOPDGDD, en el Esquema Nacional de Seguridad (ENS) y en el Esquema Nacional de Interoperabilidad (ENI), conviene recordar que esta Agencia ya ha señalado anteriormente, por ejemplo, en su Informe 170/2018, de 12 de noviembre, que, con independencia de lo dispuesto en normas de rango superior, cuando el análisis de riesgos ponga de manifiesto la necesidad de adoptar medidas más exigentes que las previstas en el Anexo II del ENS, deberán aplicarse en todo caso las medidas adicionales que resulten necesarias para garantizar la protección de los datos personales.

Así, según se señaló en el citado Informe y ahora se reitera:

"Con carácter previo a analizar la concreta cuestión que planteada en la consulta este Gabinete Jurídico estima conveniente hacer una referencia previa a la diferenciación, sustantiva y competencial, que existe entre el ámbito de la seguridad de información y el de la protección de datos de carácter personal.

Por lo que se refiere a la seguridad de la información, la misma comprende el conjunto de técnicas y medidas orientadas a garantizar la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para cualquier organización, independientemente del formato que tengan. En el ámbito de las Administraciones Públicas españolas y en relación con los sistemas que manejan información en formato electrónico (comúnmente denominados "Tecnologías de la Información y las Comunicaciones (TIC)"), el artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, actualmente sustituido por el artículo 156.2 de la Ley 40/2015, de régimen jurídico del sector público, creó el Esquema Nacional de Seguridad, que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la citada Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

Dicho precepto encuentra su desarrollo reglamentario en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, cuyo Preámbulo señala que "la finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios" añadiendo que "en este contexto se entiende por seguridad de las redes y de la información, la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles".

En este ámbito, son múltiples los órganos que ostentan competencias, pudiendo destacarse, conforme a lo recogido en el reciente Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, al Centro Criptológico Nacional (CCN) responsable del citado ENS, el Instituto Nacional de Ciberseguridad (INCIBE) y el Ministerio de Defensa.

Por el contrario, la protección de datos de carácter personal de las personas físicas se configura como un auténtico derecho fundamental que encuentra su fundamento en el artículo 18.4 de la Constitución Española, conforme al cual "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Así lo ha reconocido nuestro Tribunal Constitucional, destacando en la Sentencia 94/1998, de 4 de mayo que el citado artículo 18.4 "no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la «privacidad» según el neologismo que reza en la Exposición de Motivos de la LORTAD- pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos".

Así se recoge en el Preámbulo del Proyecto de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, que por su claridad se transcribe a continuación:

"La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Se hacía así eco de los trabajos desarrollados desde finales

de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno.

El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención. Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que 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.

A nivel legislativo, la concreción y desarrollo del derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales tuvo lugar en sus orígenes mediante la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD. La Ley Orgánica 5/1992 fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, a fin de trasponer a nuestro derecho a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta ley orgánica supuso un segundo hito en la evolución de la regulación del derecho fundamental a la protección de datos en España y se complementó con una cada vez más abundante jurisprudencia procedente de los órganos de la jurisdicción contencioso-administrativa.

Por otra parte, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. Anteriormente, a nivel europeo, se había adoptado la Directiva 95/46/CE citada, cuyo objeto era procurar que la garantía del derecho a la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un espacio común de garantía del derecho que, al propio tiempo, asegurase que en caso de transferencia internacional de los datos, su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a las previstas en la propia directiva".

Y en este mismo sentido se pronuncia 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 sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD), que tiene por objeto "proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales" (artículo 1.2.), destacando en su Considerando 1 que "la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental" y en su Considerando 10 que "para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos deber ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogéneo".

Consecuentemente, el derecho a la protección de datos de carácter personal de las personas físicas es un derecho fundamental y, por tanto, situado en el máximo nivel de

protección jurídica, que actualmente se encuentra regulado directamente por la normativa comunitaria, estableciendo el citado RGPD un conjunto de principios, derechos, obligaciones y una estructura organizativa tendentes a garantizar dicho derecho fundamental. Dentro de los mismos, la seguridad de la información aparece como una obligación más de los responsables y encargados del tratamiento quienes deberán aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que incluirán, entre otros factores "la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento" y "la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico" (artículo 32.2. b) y c) del RGPD).

Por lo tanto, no cabe duda de que la garantía de la seguridad de los datos personales adquiere una especial trascendencia en cuanto a su protección, pero sin que ésta se limite exclusivamente al ámbito de la seguridad de dicha información, en cuanto que la protección de datos personales tiene un ámbito mucho más extenso que abarca, como decíamos, a un conjunto de principios, derechos y obligaciones mucho más amplio.

Y todo ello bajo la garantía administrativa de las "autoridades de control", funciones que en España asume, sin perjuicio de las competencias que corresponde a las autoridades de las Comunidades Autónomas en su ámbito competencial, la Agencia Española de Protección de Datos, que actúan con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes (Artículo 52 RGPD) y son las únicas competentes para "asesorar sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento" (artículo 57.1.c) RGPD)".

En síntesis, tal y como ha venido informando esta Agencia, las medidas a implantar como consecuencia del análisis de riesgos previsto en los artículos 25 y 32 del RGPD, en caso de resultar agravadas respecto de las previstas en el ENS deberán prevalecer aquellas sobre éstas últimas, a fin de dar adecuado cumplimiento a lo exigido por el RGPD.

III

El artículo 7 del Reglamento de la TSD, que regula el **Protocolo de intercambio de ficheros** para la carga y actualización de datos en el sistema, establece las bases técnicas y organizativas para la creación de una base de datos integrada que contendrá información completa y detallada sobre las prestaciones sociales, sus complementos y pagos, así como las situaciones subjetivas que afectan a los ciudadanos, como el grado de discapacidad, la dependencia, la condición de familia numerosa o los niveles de renta. Este artículo es clave para garantizar la interoperabilidad y eficiencia en la gestión de las políticas sociales, pero también introduce riesgos significativos en materia de protección de datos, especialmente debido a la automatización del intercambio, el elevado volumen de datos tratados y la interconexión permanente entre sistemas de distintas administraciones públicas.

En este contexto, las "*Orientaciones de la AEPD para tratamientos que implican comunicación de datos entre Administraciones Públicas ante el riesgo de brechas masivas*"[II] resultan fundamentales para complementar y reforzar lo

[II]https://www.aepd.es/guias/orientaciones-riesgo-brechas-masivas-aapp.pdf

dispuesto en el artículo 7 del Reglamento de la TSD. Estas orientaciones, dirigidas a responsables del tratamiento en el sector público y a sus Delegados de Protección de Datos (DPD), abordan los riesgos específicos que surgen en entornos de interoperabilidad e intercambio masivo de datos, donde la materialización de una brecha de seguridad podría tener un impacto no solo individual, sino también social. Esta Agencia subraya que, en estos casos, las medidas de seguridad tradicionales, como el control de acceso básico o el cifrado genérico, son insuficientes para gestionar los riesgos asociados a brechas que afecten a un gran número de personas y a categorías sensibles de datos.

El Protocolo de intercambio de ficheros previsto en el artículo 7 del Reglamento de la TSD no detalla las medidas técnicas y organizativas específicas que deben aplicarse para garantizar que este intercambio cumpla plenamente con el RGPD. Esto es especialmente crítico porque los ficheros intercambiados contienen datos sensibles, como información sobre prestaciones sociales, salud o situación económica, que están sujetos a requisitos reforzados de seguridad según el artículo 9 del RGPD (categorías especiales de datos) y el artículo 32 del RGPD (seguridad del tratamiento). Además, la automatización y el volumen masivo de datos aumentan la probabilidad de que un incidente en un punto del sistema se propague rápidamente, afectando a la totalidad de los datos integrados.

El análisis de las **funcionalidades** previstas en el Capítulo IV pone de manifiesto que, si bien las mismas pueden considerarse en abstracto coherentes con la base jurídica del artículo 6.1.e) del RGPD, en cuanto responden a fines de interés público vinculados a la gestión y coordinación de las prestaciones sociales, su configuración concreta presenta deficiencias desde la perspectiva de la protección de datos.

Las funcionalidades previstas en los artículos 12, 13 y 15 del Reglamento plantean riesgos específicos en materia de protección de datos que no derivan tanto de la licitud abstracta del tratamiento examinada anteriormente como de la intensidad y modalidad de los accesos y usos habilitados por el sistema.

En primer lugar, las funcionalidades de consulta ciudadana y actualización de datos del artículo 12, aun respondiendo a objetivos legítimos de transparencia y simplificación administrativa, introducen riesgos asociados a la exposición permanente de información sensible en canales digitales, especialmente si el proyecto no explicita con mayor detalle salvaguardas relativas a autenticación reforzada, gestión de sesiones, trazabilidad de accesos o prevención de usos indebidos derivados de canales remotos de acceso. Tratándose de información relativa a prestaciones y situaciones

subjetivas de especial sensibilidad social, el diseño funcional debería incorporar una lógica de privacidad desde el diseño y por defecto conforme al artículo 25 del RGPD.

En segundo término, las funcionalidades del artículo 13 relativas a consulta y actualización por las entidades responsables presentan riesgos vinculados a la ampliación del círculo de acceso a datos y a la posible desalineación entre el principio de necesidad de acceso y la operativa real del sistema. En particular, un entorno en el que intervienen diversas administraciones públicas como el previsto puede generar riesgos de accesos excesivos, reutilización funcional de información más allá de la finalidad inicial o consultas masivas no suficientemente justificadas, especialmente si la norma no concreta suficientemente perfiles de acceso, reglas funcionales de segmentación o condiciones de uso ligadas al principio de minimización.

Especial atención merece el artículo 15 y la previsión de servicios web síncronos y asíncronos, cuyas funcionalidades, en particular en modalidad masiva, intensifican significativamente los riesgos para los derechos y libertades de los afectados. El acceso automatizado o masivo a información social consolidada puede elevar los riesgos de utilización extensiva de datos, consultas desproporcionadas o generación de usos secundarios no previstos inicialmente. En este punto, la amplitud funcional del sistema puede proyectar dudas sobre si todas las funcionalidades habilitadas quedan suficientemente delimitadas por las finalidades definidas en la norma.

Asimismo, la habilitación de accesos por terceros amparados en disposición legal o, en aquellos supuestos excepcionales en que el consentimiento resulte jurídicamente válido, presenta una formulación amplia que podría beneficiarse de mayor concreción, a fin de evitar que esa cláusula opere como título excesivamente abierto para nuevas comunicaciones de datos.

Con relación al artículo 16, se valora positivamente que el proyecto contemple expresamente el régimen aplicable a las **transferencias internacionales de datos** y remita, respecto de terceros países u organizaciones internacionales, a lo dispuesto en el Capítulo V del RGPD.

No obstante, cabe realizar dos observaciones. En primer lugar, bajo el título de transferencia internacionales de datos se incluye una referencia a transferencias de datos con destino a Estados miembros de la Unión Europea, lo cual supone cierta imprecisión conceptual, al no tratarse, en sentido estricto, de transferencias internacionales sometidas al régimen del Capítulo V del RGPD.

En segundo lugar, la previsión relativa a transferencias derivadas de tratados o convenios en los que sea parte España podría requerir una

formulación más precisa, a fin de evitar que dicha referencia pueda interpretarse como habilitación autónoma al margen de las condiciones y garantías exigidas por los artículos 45 a 49 del RGPD, por lo que debería precisarse su articulación conforme a las garantías y mecanismos previstos en el Capítulo V.

IV

El Reglamento de la TSD reconoce el **ejercicio de los derechos** de acceso, rectificación, supresión, limitación, oposición y a no ser objeto de decisiones automatizadas. No obstante, la regulación proyectada no delimita de manera suficiente cómo se articula su ejercicio en un sistema en el que intervienen múltiples responsables del tratamiento, cada uno de ellos competente respecto de los datos que aporta, genera o gestiona en el ámbito de sus respectivas competencias.

Esta cuestión presenta especial relevancia en el modelo de la TSD, en el que el INSS asume funciones de gestión del sistema centralizado, mientras que otras Administraciones y entidades participantes actúan, con carácter general, como responsables independientes respecto de los datos cuya incorporación al sistema les corresponde. En este contexto, la efectividad de los derechos reconocidos en el RGPD no puede quedar condicionada a que el ciudadano identifique qué entidad ostenta la condición de responsable respecto de cada dato concreto.

Desde esta perspectiva, se aprecia la necesidad de que el Reglamento establezca expresamente un mecanismo de ejercicio de derechos que no traslade al interesado la complejidad organizativa del sistema. En particular, debería preverse que las solicitudes puedan presentarse ante cualquiera de las entidades intervinientes y, singularmente, a través del punto de acceso que representa el propio sistema, debiendo la entidad receptora tramitar la solicitud en el ámbito de su competencia o remitirla, mediante mecanismos internos de coordinación, al responsable materialmente competente, garantizando en todo caso una respuesta unitaria, eficaz y dentro de los plazos previstos en el artículo 12 del RGPD.

La ausencia de una regulación expresa sobre esta coordinación interadministrativa genera incertidumbre respecto de cuestiones esenciales como la tramitación de solicitudes relativas a datos aportados por terceros responsables, la gestión de derechos de rectificación u oposición sobre información no generada por el INSS, o la forma en que se articularía la respuesta cuando concurrieran varios responsables implicados en un mismo flujo de tratamiento. Estas carencias podrían comprometer la efectividad práctica de los derechos de los interesados y deberían ser objeto de desarrollo específico en la norma.

Particularmente, en relación con los derechos de acceso, rectificación y supresión, se echa en falta una regulación más detallada sobre los cauces de respuesta, los mecanismos de colaboración entre entidades y la información que debe facilitarse al interesado en caso de denegación total o parcial de su solicitud, incluyendo la motivación de dicha decisión y la posibilidad de acudir a la autoridad de control, conforme al artículo 12.4 del RGPD.

Por último, dada la obtención indirecta de datos que articula el sistema, cabría considerar la incidencia del artículo 14 del RGPD, si bien, en principio, estos tratamientos podrían quedar amparados por la excepción prevista en el artículo 14.5.c) del RGPD. No obstante, podría valorarse reforzar las garantías de transparencia del sistema mediante una mayor explicitación de los flujos de información interadministrativos y de los mecanismos mediante los cuales los interesados puedan conocer los accesos y comunicaciones efectuadas respecto de sus datos.

V

El tratamiento de datos personales previsto en el proyecto de Reglamento de la Tarjeta Social Digital encuentra, con carácter general, cobertura en el artículo 6.1.e) del RGPD, en la medida en que se vincula al ejercicio de competencias públicas en materia de gestión y coordinación de prestaciones sociales. Asimismo, la disposición adicional centésima cuadragésima primera y la disposición transitoria tercera de la Ley 6/2018 proporcionan una habilitación legal suficiente para la creación del sistema y para el intercambio de determinada información entre Administraciones públicas.

No obstante, **la existencia de una habilitación legal general no excluye la necesidad de que el desarrollo reglamentario concrete adecuadamente los elementos esenciales del tratamiento, de conformidad con el artículo 6.3 del RGPD y con las exigencias derivadas del principio de calidad normativa en materia de limitaciones al derecho fundamental a la protección de datos**, toda vez que dichos elementos y garantías esenciales del tratamiento no han sido previstos en la dicha habilitación legal general.

Se recomienda reforzar la delimitación normativa de las finalidades y funcionalidades del sistema, especificando de manera expresa los distintos supuestos de acceso, cesión e intercambio de datos entre Administraciones, así como su concreta vinculación con fines determinados, explícitos y legítimos. En particular, debería precisarse, para cada flujo de datos y modalidad de acceso, especialmente en los tratamientos masivos o automatizados, la

finalidad perseguida, las categorías de datos estrictamente necesarias y los sujetos habilitados, de modo que pueda verificarse de forma efectiva el cumplimiento de los principios de necesidad, minimización y proporcionalidad.

Asimismo, se considera conveniente incorporar en la norma o en sus desarrollos instrumentos de gobernanza del dato (como políticas de acceso basadas en perfiles, registros de trazabilidad y controles periódicos), que permitan garantizar que los accesos interadministrativos se producen únicamente en los casos justificados y dentro de los límites legalmente establecidos, evitando configuraciones excesivamente abiertas o genéricas que puedan comprometer la suficiencia de la base jurídica prevista en el Reglamento General de Protección de Datos.

Resulta asimismo conveniente hacer notar la **insuficiente delimitación de los sujetos intervinientes y de la gobernanza del tratamiento**

Si bien puede considerarse que el INSS ostenta la condición de responsable del tratamiento respecto de los tratamientos vinculados a la gestión y funcionamiento de la TSD, en la medida en que determina fines y medios esenciales de dichos tratamientos, persisten insuficiencias en la delimitación de la posición jurídica de las restantes Administraciones y entidades participantes.

Como se ha señalado, no parece que estas deban configurarse, con carácter general, como encargados del tratamiento, ni concurra automáticamente un supuesto de corresponsabilidad del artículo 26 RGPD; más bien se aprecia una pluralidad de responsables independientes conectados a través de una infraestructura común. Precisamente por ello, sería conveniente reforzar normativamente:

- las reglas de distribución funcional de responsabilidades;
- los mecanismos de cooperación entre responsables;
- la gobernanza del sistema en materia de seguridad, incidencias y cumplimiento;
- y el papel coordinador de los Delegados de Protección de Datos de las entidades intervinientes.

La ausencia de esta arquitectura de gobernanza constituye una carencia relevante en un sistema de interconexión administrativa de esta complejidad. Se hace necesario definir el estatus de las entidades colaboradoras, estableciendo sus obligaciones en materia de protección de datos.

Tal y como se ha anticipado en fundamentos de derecho anteriores resulta necesaria la realizaciñon de **una Evaluación de Impacto en Protección de Datos.**

Aunque el proyecto contempla referencias a la aplicación del Esquema Nacional de Seguridad y del Esquema Nacional de Interoperabilidad, no se recoge referencia expresa a la realización de una evaluación de impacto en protección de datos.

La ausencia de referencia a una EIPD constituye una carencia relevante, al impedir verificar adecuadamente la necesidad y proporcionalidad del tratamiento, así como la suficiencia de las medidas previstas para mitigar riesgos. Se considera, por ello, necesaria su realización con carácter previo a la implantación efectiva del sistema, debido a la concurrencia de varios de los supuestos que el art. 35 del RGPD y las directrices del GT 29. La EIPD es obligatoria en este caso, debiendo realizarse con carácter previo a la implantación efectiva del sistema y debe incluir:

- Descripción sistemática de las operaciones de tratamiento.
- Evaluación de la necesidad y proporcionalidad de las medidas de protección.
- Análisis de riesgos para los derechos y libertades de los interesados.
- Medidas previstas para mitigar los riesgos identificados.

Además, conforme al Considerando 78 del RGPD "*La evaluación de impacto relativa a la protección de datos debería ser un proceso continuo, que se revise siempre que haya cambios en el tratamiento que puedan afectar a la protección de los datos personales*". Este "*proceso continuo*" conlleva que la EIPD deba actualizarse, especialmente cuando cambien las circunstancias del tratamiento o surjan nuevos riesgos.

Como consecuencia de lo anterior es posible apreciar insuficiencias en las medidas técnicas y organizativas contenidas en este proyecto normativo.

En cuanto a las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo cuya adopción exige el art. 32 del RGPD, el Reglamento contiene referencias al ENS, ENI y a medidas de seguridad. Debería incluirse una previsión conforme a la cual, si el análisis de riesgos exige medidas agravadas respecto del ENS, deberán aplicarse dichas medidas reforzadas; no obstante, ello podría complementarse con una mayor explicitación normativa de salvaguardas concretas. Y ello sin perjuicio de revisión periódica de la TSD para evaluar su impacto en la protección de datos y ajustar las medidas de seguridad. Del mismo modo que en la EIPD, respecto

a las medidas de seguridad, el RGPD exige que los responsables del tratamiento revisen y actualicen las medidas de protección de datos de forma continua (art. 24 y 32 RGPD).

En quinto lugar se sugiere la **necesidad de protocolizar los intercambios de información entre Administraciones públicas**

Las "*Orientaciones de la AEPD para tratamientos que implican comunicación de datos entre Administraciones Públicas ante el riesgo de brechas masivas*" destacan que, en tratamientos complejos como el de la TSD, donde múltiples entidades actúan (INSS, comunidades autónomas, mutualidades), es esencial adoptar un enfoque proactivo y coordinado para gestionar los riesgos. La AEPD insiste en la importancia de establecer medidas de detección temprana, como sistemas de monitorización continua y alertas automáticas, así como protocolos de respuesta coordinados entre todas las entidades intervinientes, para garantizar una gestión ágil y unificada en caso de incidencia.

Además, las orientaciones de la AEPD subrayan la necesidad de fortalecer la coordinación entre los Delegados de Protección de Datos (DPD) de las entidades implicadas, asegurando que las medidas de privacidad y seguridad sean coherentes y efectivas en todas las administraciones. Esto incluye la participación activa de los DPD en el diseño y supervisión del Protocolo de intercambio de ficheros, así como la creación de canales de comunicación ágiles para notificar y gestionar incidentes, evitando que la responsabilidad se diluya entre los distintos actores.

A continuación, se muestran algunas de las medidas preventivas, de detección, de respuesta y de revisión y supervisión que se podrían implementar, según se establecen en la Guía, la cual aclara que esta lista no es exhaustiva ni exigible en su totalidad, pero sí son medidas a valorar:

"*Algunos ejemplos de medidas preventivas son:*

• Disponer de un marco de coordinación de los DPD de las entidades involucradas.
• Realizar un análisis conjunto de las implicaciones de los tratamientos que involucran a distintas entidades.
• Disponer de políticas de protección de datos, en el sentido indicado anteriormente, coordinadas entre los intervinientes en el tratamiento.
• Realizar ejercicios conjuntos en el que se planteen escenarios de brechas de datos personales.
• Categorizar datos que en un momento dado puedan ser considerados de especial sensibilidad.
• Identificar conjuntos de datos de mayor impacto que no deban ser accesibles por medios exclusivamente automatizados.
• Aumentar la intervención humana en la gestión de los accesos.

• Implementar políticas de cancelación o bloqueo de datos que no deben estar en los sistemas de producción.

• Estudiar estrategias de minimización de datos accesibles por Internet: anonimización, seudonimización, disminución de la granularidad o precisión de los datos, restricción de campos/atributos, agregación, adición de ruido, etc.

• Atendiendo a las políticas de acceso, establecer estrategias de minimización en el sentido anterior.

• Implementar estrategias de "mínimo privilegio", con protección contra posibles ataques desde los sistemas interconectados basados también en la estrategia de "mínimo privilegio".

• Establecer parámetros de monitorización o que impliquen requisitos de acceso adicional para la consulta de datos cuyas características personales puedan suponer un daño social adicional.

• Disponer en los planes de continuidad de negocio y resiliencia, que incluyan copias de seguridad de datos y también de continuidad de los tratamientos.

• Proteger las copias de seguridad con el mismo nivel de protección que sea aplicable a los datos y sistemas en producción

• Disponer de copias de seguridad en sistemas independientes y separados de los de producción.

• Aplicar estrategias de segmentación de redes y sistemas, incluyendo protección de servicios expuestos, mediante DMZ u otras medidas adecuadas.

• Implementar estrategias de aislamiento entre sistemas que impidan la extensión de ransomware a toda la organización.

• Tener los sistemas de la infraestructura de servicios e interoperabilidad

actualizados sin vulnerabilidades conocidas (servidores, máquinas virtuales, acceso a la nube, etc.)

• Evitar la utilización de nombres de usuario significativos, con patrones predecibles y/o otros identificadores como el NIF, DNI o correos electrónicos que puedan ser igualmente predecibles.

• Tener redactada e implementada una política de gestión de contraseñas actualizada, incluyendo la imposibilidad de utilizar contraseñas débiles y/o comprometidas en otras brechas de datos personales.

• Prohibir el uso de credenciales organizacionales genéricas (el mismo para múltiples usuarios de una organización). El usuario final que accede a datos, junto a la finalidad/justificación del acceso/consulta debe permear hasta el servicio que expone datos para que pueda aplicar políticas de acceso restrictivas.

• Tener y aplicar políticas de acceso a los datos diferenciadas por categorías de responsables, usuarios y tratamientos.

• Añadir un segundo y/o tercer factor de autenticación, sin que eso implique necesariamente tratamientos biométricos o en dispositivos móviles.

Algunos ejemplos de medidas de detección son:

• Establecimiento de cuotas o límites de consulta por usuario/cuenta y también por organización, acordes al uso legítimo de los mismos, incluyendo la monitorización de tales accesos.

• Gestionar de forma específica las consultas/accesos desde IP geolocalizadas en áreas geográficas fuera del ámbito de las organizaciones o no habituales, IP basadas en redes de anonimización o IP comprometidas.

• Implementación de sistemas que permitan la detección y mitigación de ataques de enumeración/fuerza fruta.

• Implementación de sistemas que detecten intentos fallidos de acceso a datos, como por ejemplo consultas sistemáticas a DNI u otros datos que den como resultados intentos fallidos.

• Sistemas de detección de situaciones de exfiltración de datos.

• Implementar sistemas de alerta temprana que permitan conocer el ataque lo antes posible y en sus primeras fases a aquellos que tienen las obligaciones de actuar.

• Utilizar sistemas de detección basados en honey-pots.

Algunas medidas de respuesta que tienen que estar previstas:

• Disponer de planes de respuesta a incidentes que incluyan la gestión y rápida respuesta a brechas de datos personales.

• Disponer de procedimientos que permitan que los incidentes de seguridad escalen de forma rápida tanto al DPD como a los círculos de decisión de la organización.

• Establecimiento de canales ágiles, efectivos y probados de comunicación de brechas entre las entidades intervinientes.

• Procedimiento de notificación de brechas de datos personales a las autoridades competentes que concrete todos los aspectos fundamentales. Por ejemplo, el responsable debe saber de antemano cuál es la Autoridad de Control a la que se debe notificar, qué sucesos motivarán la ejecución del procedimiento, qué persona debe realizar la notificación a la autoridad de control, aprovisionar los medios técnicos o de cualquier índole necesarios para notificar.

• Procedimiento y recursos para la comunicación a los afectados, que adelante en cada situación cómo se va a comunicar una brecha masiva a los interesados afectados, en qué situaciones se producirá tal comunicación, medio para comunicar, plazos para proteger de forma efectiva los derechos de los interesados, recomendaciones para los interesados en función de los distintos escenarios de brechas, situaciones que pueden justificar el retraso de la comunicación, etc.

• En situaciones de gran impacto social, puede estar justificado la utilización de un comunicado público que podría ser un comunicado conjunto entre todos los responsables implicados en la brecha. En algunas situaciones podría ser ampliado a posteriori con comunicaciones individuales si fuera necesario.

• Notificación, en caso de ciberincidente, al CERT correspondiente y respuesta al ciberincidente siguiendo las indicaciones del CERT.

• Denuncia de los hechos a autoridades policiales/judiciales en caso de ilícitos.

Algunas medidas de supervisión y revisión son:

• Procedimientos establecidos para determinar cambios de contexto en responsables y tratamientos de similar naturaleza: brechas producidas, cambios tecnológicos, novedades normativas nacionales, europeas e internacionales, evolución social o política, factores geoestratégicos, etc.

• Establecimiento de canales de comunicación efectivos entre las entidades intervinientes sobre los eventos anteriores.

• Reuniones periódicas entre los DPD y responsables de seguridad de las entidades intervinientes.

• Auditorias de privacidad (en función de cambios en la naturaleza, contexto, extensión, fines y riesgos del tratamiento art. 24.1) y de seguridad (estas últimas regulares art. 32.1d) en servicios que exponen datos personales a nivel de:

o Evaluación de impacto del punto común de comunicación de datos.
o Reevaluación de riesgo para los derechos y libertades individuales y sociales.
o Grado de implementación de garantías de privacidad y medidas de seguridad.
o Test de penetración.
o Ataques por ingeniería social.
o Nivel de respuesta de las medidas organizativas.
o Procedimientos de gestión de incidentes de seguridad y brechas de datos personales (preventivos y reactivos).”

VI

Seguidamente centraremos nuestro análisis en las **observaciones y propuestas de mejora de las funcionalidades de la TSD en el Capítulo IV del Reglamento,**

De acuerdo con lo expuesto en el apartado II, se considera conveniente reforzar normativamente el diseño de estas funcionalidades incorporando mayores garantías sobre su arquitectura de funcionamiento, no necesariamente mediante un desarrollo técnico exhaustivo impropio de una norma reglamentaria, pero sí mediante una delimitación más precisa de condiciones, límites y salvaguardas.

En particular, respecto del artículo 12, podría valorarse introducir previsiones adicionales que refuercen el principio de privacidad desde el diseño en relación con los canales digitales de acceso ciudadano, incluyendo una referencia expresa a garantías reforzadas para funcionalidades móviles, mecanismos de trazabilidad accesibles al propio interesado y controles preventivos frente a accesos indebidos.

En relación con el artículo 13, resultaría conveniente precisar con mayor claridad el principio de acceso basado en necesidad de conocimiento (“need to know”), delimitando funcionalmente los accesos de las entidades participantes, así como prever expresamente mecanismos de supervisión y auditoría de los accesos realizados en el sistema. Asimismo, podría valorarse incorporar una remisión expresa a protocolos de intercambio de información o reglas comunes de operación entre Administraciones, en línea con las recomendaciones formuladas por la Agencia Española de Protección de Datos sobre comunicaciones de datos entre Administraciones públicas.

Respecto del artículo 15, sería recomendable reforzar la delimitación material de los servicios web, especialmente en modalidad asíncrona, precisando supuestos de uso, límites funcionales, condiciones para accesos masivos y salvaguardas específicas aplicables a estos tratamientos de mayor riesgo. Podría valorarse asimismo una referencia expresa a la necesidad de someter estas funcionalidades a revisión periódica desde la perspectiva de gestión de riesgos y proporcionalidad.

Finalmente, con carácter general, cabría sugerir que las funcionalidades del Capítulo IV se formulen de manera más estrechamente conectada con las finalidades del tratamiento definidas por la norma, reforzando así la coherencia entre diseño funcional, principio de minimización y exigencias de necesidad derivadas del RGPD.

Respecto a las **transferencias internacionales de datos**, la inclusión en el apartado 1 del artículo 16 de las transferencias a Estados miembros de la Unión Europea debe corregirse al no tratarse en sentido estricto de transferencias internacionales de datos sujetas al Capítulo V del RGPD; y la referencia a tratados o convenios en los que sea parte España debería ajustarse su redacción para reforzar su coherencia con el régimen del Capítulo V, especificando las garantías adicionales para transferencias a terceros países, como el uso de cláusulas contractuales tipo o la verificación de decisiones de adecuación.

En relación con las mencionadas **carencias en la articulación del ejercicio de derechos** se aprecia una insuficiente regulación del ejercicio efectivo de derechos en un entorno con multiplicidad de responsables. Se considera necesario incorporar una regulación más precisa del ejercicio de derechos en este entorno con diversos intervinientes, articulando protocolos de cooperación entre responsables, reglas claras de remisión y gestión de solicitudes, y un modelo de ventanilla funcional que garantice que la distribución interna de responsabilidades no menoscabe el ejercicio sencillo y efectivo de los derechos reconocidos en el RGPD.

Aunque el proyecto reconoce formalmente los derechos de los interesados, no articula de manera suficientemente precisa los mecanismos de ejercicio cuando los datos provengan de distintas Administraciones, ni evita plenamente trasladar al ciudadano la complejidad organizativa del sistema.

Se considera conveniente incorporar:

- un modelo funcional de “ventanilla única operativa” para el ejercicio de derechos;
- reglas de remisión y coordinación entre responsables;
- una regulación más detallada sobre respuesta, motivación de denegaciones y coordinación interadministrativa.

Ello reforzaría la efectividad práctica de los artículos 12 a 22 del RGPD.

El ejercicio de derechos deberá dirigirse, en última instancia, al responsable del dato, esto es, la Administración que lo haya generado, si bien el interesado podrá presentar su solicitud ante cualquiera de las entidades intervinientes, las cuales deberán garantizar su tramitación o remisión al responsable competente, sin trasladar al ciudadano la complejidad organizativa del sistema.

El diseño del sistema no puede implicar que el interesado deba identificar al responsable originario del dato, debiendo establecerse mecanismos de coordinación interadministrativa que aseguren un ejercicio efectivo y sencillo de los derechos reconocidos en el RGPD.

En conclusión, definir un protocolo de colaboración entre el INSS y las entidades colaboradoras para gestionar las solicitudes de derechos de los interesados, especialmente cuando los datos no sean competencia directa del INSS, que incluya cómo se informará al interesado cuando su solicitud de supresión o rectificación sea denegada, indicando los motivos y la posibilidad de reclamar ante la AEPD.

VII

Recopilando lo explicado en los apartados anteriores de este informe, el proyecto de Real Decreto por el que se regula la Tarjeta Social Digital (TSD) se enmarca en el desarrollo de lo dispuesto en la disposición adicional centésima cuadragésima primera y la disposición transitoria tercera de la Ley 6/2018, de Presupuestos Generales del Estado. No obstante, el tratamiento de datos personales que implica este sistema, especialmente cuando afecta a categorías especiales de datos, como los relativos a discapacidad, dependencia u otras situaciones subjetivas susceptibles de revelar información sobre la salud o circunstancias socioeconómicas especialmente sensibles, exige el cumplimiento estricto de las exigencias derivadas del artículo 6.3 del Reglamento General de Protección de Datos, así como de la doctrina consolidada del Tribunal Constitucional y del Tribunal de Justicia de la Unión Europea en materia de protección de datos personales, calidad normativa y proporcionalidad de las injerencias en derechos fundamentales.

La Disposición Adicional de continua referencia permite el tratamiento de datos personales (incluyendo en algunos casos datos sensibles) en el ámbito de la protección social, siempre que se cumplan determinadas condiciones y garantías legales. El tratamiento de datos sensibles (tales como discapacidad, dependencia, familia numerosa, etc.) deberá realizarse de acuerdo con las bases jurídicas del RGPD y la normativa española, y será posible siempre que se ajuste a alguno de los supuestos de levantamiento de la prohibición previstos en el artículo 9.2 RGPD, tales como, por citar algunos ejemplos, el previsto en la letra b) "*El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral, la seguridad social y la protección social*", o g) "*El tratamiento es necesario por razones de interés público esencial, con sujeción a garantías adecuadas".*

Del artículo 8 del Reglamento, datos integrados en la TSD, no se desprende un tratamiento de datos sensibles directamente, pero sí de manera

indirecta cuando lleguen a tratarse datos sensibles vinculados a determinadas prestaciones sociales (discapacidad o dependencia), estos tratamientos podrían encontrar amparo bien en el artículo 9.2.b) o 9.2.g) RGPD, siempre y cuando así se justificara en el texto del proyecto normativo objeto de este informe tal y como se ha indicado en fundamentos anteriores, y todo ello teniendo en cuenta la redacción contenida en el apartado seis de la disposición adicional centésima cuadragésima primera de la Ley 6/2018:

"El tratamiento de datos previsto en la Tarjeta Social Digital se basa en el interés público que representa disponer de un sistema informático integrado en el que se recojan todas las prestaciones sociales públicas de contenido económico y situaciones subjetivas relevantes que afecten a los ciudadanos. La información contenida en la Tarjeta se someterá a la normativa vigente en materia de protección de datos de las personas físicas".

En este sentido, aunque la Ley 6/2018 proporciona una habilitación legal suficiente, en términos generales, para la creación y funcionamiento de la Tarjeta Social Digital y para el intercambio de determinada información entre Administraciones públicas, el desarrollo reglamentario debe ajustarse a las exigencias reforzadas de predeterminación normativa, necesidad, proporcionalidad y garantías adecuadas derivadas del artículo 53.1 de la Constitución Española y de la normativa europea de protección de datos. El artículo 6.3 del RGPD permite que la base jurídica del tratamiento determine de manera suficientemente precisa los elementos esenciales del mismo, incluyendo las condiciones generales de licitud, los fines perseguidos, las categorías de datos objeto de tratamiento, los sujetos afectados, las entidades destinatarias de la información, las condiciones de comunicación, los plazos de conservación y las garantías aplicables. En esta misma línea, la Sentencia del Tribunal Constitucional 76/2019 recuerda que las garantías adecuadas y los elementos esenciales de los tratamientos limitativos de derechos fundamentales deben incorporarse a la propia regulación legal, sin que puedan quedar deferidos de forma abierta a un ulterior desarrollo reglamentario.

No obstante, el proyecto normativo analizado presenta insuficiencias en la delimitación de diversos elementos esenciales del tratamiento, lo que dificulta verificar plenamente su conformidad con los principios de necesidad, minimización, proporcionalidad y limitación de la finalidad. En particular, se observan las siguientes carencias:

i) Aunque el Instituto Nacional de la Seguridad Social aparece configurado como responsable del tratamiento respecto de la gestión y funcionamiento del sistema TSD, el proyecto no delimita con suficiente precisión el papel de las comunidades autónomas, mutualidades, entidades gestoras y restantes organismos

participantes. Estas entidades no parecen actuar, con carácter general, como encargados del tratamiento en el sentido del artículo 28 RGPD, al tratar los datos en ejercicio de competencias propias legalmente atribuidas, ni tampoco puede apreciarse de forma inequívoca una situación de corresponsabilidad plena conforme al artículo 26 RGPD.

ii) El modelo diseñado se aproxima más bien a un sistema de pluralidad de responsables interconectados mediante mecanismos de interoperabilidad administrativa, circunstancia que exigiría una regulación más detallada sobre distribución funcional de responsabilidades, reglas de acceso, flujos de información y mecanismos de coordinación. La ausencia de una arquitectura clara de gobernanza puede generar incertidumbres relevantes desde la perspectiva del principio de responsabilidad proactiva y del adecuado cumplimiento de las obligaciones derivadas del RGPD.

iii) El proyecto no incorpora referencia expresa a la realización de una Evaluación de Impacto en Protección de Datos (EIPD), pese a que el sistema previsto presenta múltiples elementos que, conforme al artículo 35 RGPD y a las directrices europeas y nacionales aplicables, apuntan claramente hacia la necesidad de efectuarla. Entre ellos cabe destacar el tratamiento a gran escala de categorías especiales de datos, la concentración e interconexión de información procedente de múltiples Administraciones públicas, la utilización de servicios de acceso automatizado y la amplitud funcional del sistema.

iv) La ausencia de referencia a dicha evaluación resulta particularmente relevante en un sistema caracterizado por tratamientos masivos y continuados de información social especialmente sensible, en el que la identificación y mitigación previa de riesgos constituye una garantía esencial desde la perspectiva del principio de protección de datos desde el diseño y por defecto.

v) Aunque el proyecto establece que la TSD deberá ajustarse a las exigencias del Esquema Nacional de Seguridad (ENS) y del Esquema Nacional de Interoperabilidad (ENI), no incorpora una regulación suficientemente detallada sobre los riesgos específicos asociados al sistema ni sobre las medidas técnicas y organizativas concretas destinadas a mitigarlos. Tal y como ha venido señalando la Agencia Española de Protección de Datos en diversos informes, la mera remisión al ENS y al ENI no excluye la necesidad de adoptar medidas adicionales derivadas del análisis

específico de riesgos en materia de protección de datos personales.

vi) Las funcionalidades previstas en los artículos relativos a consultas ciudadanas, accesos interadministrativos y servicios web síncronos y asíncronos incrementan notablemente la superficie de exposición del sistema y los riesgos asociados a accesos excesivos, reutilización funcional de información o consultas masivas no suficientemente justificadas, lo que exigiría una mayor explicitación normativa de salvaguardas, mecanismos de auditoría y controles de acceso basados en el principio de necesidad de conocimiento.

vii) El proyecto contempla un protocolo de intercambio de información entre Administraciones y entidades participantes, si bien su regulación resulta limitada desde la perspectiva de las garantías exigibles en materia de protección de datos. La comunicación sistemática e interoperable de información entre múltiples responsables exige mecanismos particularmente rigurosos de delimitación de accesos, trazabilidad, supervisión y control de usos secundarios de la información.

En este sentido, la doctrina del Tribunal Constitucional y las recomendaciones formuladas por la Agencia Española de Protección de Datos en materia de comunicación de datos entre Administraciones públicas vienen insistiendo en la necesidad de que estos intercambios se articulen conforme a protocolos suficientemente definidos, limitados a los datos estrictamente necesarios y acompañados de garantías efectivas de control y supervisión.

viii) Aunque el proyecto incorpora cobertura general para el tratamiento de datos personales, la insuficiencia de garantías anteriormente expuesta junto con la ausencia de delimitación detallada sobre los concretos datos objeto de intercambio dificultan verificar plenamente la aplicación efectiva del principio de minimización previsto en el artículo 5.1.c) RGPD. Todo ello, sin perjuicio de la necesidad de fundamentar la concurrencia de alguno de los supuestos de levantamiento de la prohibición previstos en el artículo 9.2 RGPD cuando se trate de datos personales, como es el caso de información vinculada a discapacidad, dependencia y otras situaciones subjetivas ligadas a datos especialmente protegidos.

En consecuencia, la ausencia en el proyecto normativo de referencias expresas al análisis de riesgos y a la evaluación de impacto en protección de datos, unida a la insuficiente concreción de diversos elementos esenciales del tratamiento exigidos por el artículo 6.3 RGPD —entre ellos, la delimitación precisa de finalidades, categorías de datos, condiciones de acceso, operaciones de tratamiento, garantías aplicables o reglas de intercambio de información— dificulta considerar plenamente satisfechas las exigencias de predeterminación normativa y calidad de la ley derivadas del artículo 53.1 de la Constitución Española y de la doctrina constitucional y europea en materia de protección de datos personales.