

**N/REF: 0075/2025**

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, tal y como efectivamente se indica en el apartado de Análisis y contenidos jurídicos de la Memoria de Análisis de Impactos Normativos que acompaña a este borrador sometido a consulta.

# I

En primer lugar, debe partirse de la naturaleza reglamentaria del proyecto informado y de la vigencia, en relación con las limitaciones al derecho fundamental de protección de datos personales, del principio de reserva de ley exigido por el artículo 53.1 de la Constitución y el artículo 8 de la LOPDGDD, que, conforme a reiterada jurisprudencia del Tribunal Constitucional, requiere, por un lado, la necesaria intervención de la *ley* para habilitar la injerencia; y, por otro lado, esa norma legal ***“ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica”***, esto es, ***“ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención”*** (STC 49/1999, FJ 4). En otras palabras, *“no sólo excluye apoderamientos a favor de las normas reglamentarias [...], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites”* (STC 292/2000, FJ 15). Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero.

En este sentido, la **sentencia TC 292/2000 de 30 de noviembre** señala, en su Fundamento Jurídico 14, y se pronuncia respecto del alcance de las normas reglamentarias en los siguientes términos:

*14. Pese a la importancia que para garantizar el ejercicio del derecho fundamental poseen los derechos del interesado a ser informado y a consentir la cesión de sus datos personales, como antes se ha declarado, sin embargo, es suficiente según el art. 21.1 LOPD [norma cuya constitucionalidad se estaba discutiendo en el proceso ante el TC] que la comunicación de tales datos entre Administraciones Públicas, para el ejercicio de competencias diferentes o que versen sobre materias distintas, sea autorizada por una norma reglamentaria. Al respecto, ya hemos dicho [STC 127/1994, FJ 5, con remisión a la STC*

83/1984, FJ 4, y 99/1987, FJ 3 a)] que incluso en los ámbitos reservados por la Constitución a la regulación por Ley no es imposible una intervención auxiliar o complementaria del Reglamento, pero siempre que estas remisiones restrinjan efectivamente el ejercicio de esa potestad reglamentaria a un complemento de la regulación legal que sea indispensable por motivos técnicos o para optimizar el cumplimiento de las finalidades propuestas por la Constitución o por la propia Ley. De tal modo que esa remisión no conlleve una renuncia del legislador a su facultad para establecer los límites a los derechos fundamentales, transfiriendo esta facultad al titular de la potestad reglamentaria, sin fijar ni siquiera cuáles son los objetivos que la reglamentación ha de perseguir, pues, en tal caso, el legislador no haría sino "deferir a la normación del Gobierno el objeto mismo reservado" (STC 227/1993, de 9 de julio, FJ 4, recogiendo la expresión de la STC 77/1985, de 27 de junio, FJ 14).

La remisión a la regulación reglamentaria de materia ligada a la reservada a la Ley es preciso, pues, que se formule en condiciones tales que no contraría materialmente la finalidad de la reserva, de la cual se derivan, según la STC 83/1984, "ciertas exigencias en cuanto al alcance de las remisiones o habilitaciones legales a la potestad reglamentaria, que pueden resumirse en el criterio de que las mismas sean tales que restrinjan efectivamente el ejercicio de esa potestad a un complemento de la regulación legal que sea indispensable por motivos técnicos o para optimizar el cumplimiento de las finalidades propuestas por la Constitución o por la propia Ley". Es en este segundo plano en el que se encuentra el núcleo argumental del recurso interpuesto por el Defensor del Pueblo que es acogido en esta Sentencia, el cual considera que al establecer el art. 21.4 LOPD que esas cesiones no requieren del previo consentimiento del afectado permite al reglamento imponer un límite al derecho fundamental a la protección de datos personales, que como se ha dicho ya, defrauda la previsión del art. 53.1 de la Constitución (STC 101/1991, de 13 de mayo, FJ 3).

El artículo 6.1 del RGPD considera que un tratamiento es lícito cuando cumpla al menos una serie de supuestos, y, asimismo, el apartado 3 del citado artículo 6 RGPD, ahonda en los requisitos legales de la norma que dé cobertura al tratamiento y propone elementos que podrán ser tenidos en cuenta en dicha regulación, al indicar que:

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por: a) el Derecho de la Unión, o b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento. **La finalidad del tratamiento deberá quedar determinada en dicha base jurídica** o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha

*base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.*

El Considerando 45 del RGPD señala que “Cuando se realice en cumplimiento de una obligación legal aplicable al responsable del tratamiento, o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, el tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros.”

Por su parte la LOPDGDD establece en su artículo 8, bajo la denominación “Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos”, lo siguiente:

- 1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o **una norma con rango de ley**, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.*
- 2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, **cuando derive de una competencia atribuida por una norma con rango de ley.***

## **II**

A estos requisitos, referidos en general a cualesquiera tratamientos de datos personales (sean o no estos datos pertenecientes a categorías especiales) debemos

añadir los exigidos **para poder someter a tratamiento datos personales incluidos en dichas categorías especiales. En estos supuestos deben darse las especiales exigencias y reserva de ley de las restricciones al derecho de protección de datos que se derivan de la jurisprudencia constitucional y europea y que expresa también el artículo 23 RGPD.**

Es decir, **respecto de estas categorías especiales de datos personales, el art. 9.1 RGPD, y el art. 9.1 LOPDGDD prohíben su tratamiento.** Se prevén, sin embargo, determinados requisitos que permiten levantar dicha prohibición de tratamiento a la que hace referencia el apartado 1 del citado artículo 9 del RGPD, para lo que debemos aplicar alguna de las excepciones que se recogen en el apartado 2 del citado precepto.

A ello hay que añadir la doctrina de nuestro Tribunal Constitucional contenida en la **Sentencia 76/2019, de 22 de mayo** respecto de la norma en la que deben recogerse dichas garantías (F.J.8):

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

De manera más extensa, y como ya ha venido recordando esta AEPD reiteradamente en sus informes:

*[...] debe tenerse igualmente en cuenta que, en el caso de que la obligación venga impuesta por una norma de derecho interno, **la misma deberá tener rango de ley**, por exigirlo el artículo 53.1 de la Constitución, tal y como expresamente recoge el artículo 8.1 de la LOPDGDD, añadiendo que “podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo, así como las cesiones que procedan como consecuencia del*

cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679” y deberá tenerse en cuenta la doctrina constitucional recogida, fundamentalmente, en las sentencias 292/2000 de 30 noviembre y 76/2019 de 22 de mayo, conforme a **la cual los límites al derecho fundamental a la protección de datos personales deben establecerse por una norma con rango de ley**, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, definiendo todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías adecuadas, siendo la propia ley la que habrá de contener las garantías adecuadas frente a la recopilación de datos personales que autoriza. El Tribunal Constitucional (TC) ha sido claro en cuanto a que la previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. **Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado.** Solo ese entendimiento es compatible con la doble exigencia que dimana del artículo 53.1 CE (...). **Es evidente que, si la norma incluyera una remisión para la integración de la ley con las garantías adecuadas establecidas en normas de rango inferior a la ley, sería considerada como una deslegalización que sacrifica la reserva de ley ex artículo 53.1 CE, y, por este solo motivo, debería ser declarada inconstitucional y nula.** (...)

Se trata, en definitiva, de “garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental”. **Tampoco sirve por ello que para el establecimiento de dichas garantías adecuadas y específicas la ley se remita al propio RGPD o a la LOPDGD.**

Como gráficamente expone el TC en su STC 76/2019, FJ 8 y 9:

Por último, debemos recordar que el Reglamento general de protección de datos establece las garantías mínimas, comunes o generales para el tratamiento de datos personales que no son especiales. **En cambio, no establece por sí mismo el régimen jurídico aplicable a los tratamientos de datos personales especiales**, ni en el ámbito de los Estados miembros ni para el Derecho de la Unión. Por ende, **tampoco fija las garantías que deben observar los diversos tratamientos posibles de datos sensibles**, adecuadas a los riesgos de diversa probabilidad y gravedad que existan en cada caso; tratamientos y categorías especiales de datos que son, o pueden



*ser, muy diversos entre sí. El reglamento se limita a contemplar la posibilidad de que el legislador de la Unión Europea o el de los Estados miembros, cada uno en su ámbito de competencias, prevean y regulen tales tratamientos, y a indicar las pautas que deben observar en su regulación. Una de esas pautas es que el Derecho del Estado miembro establezca “medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado” [art. 9.2 g) RGPD] y que “se ofrezcan garantías adecuadas” (considerando 56 RGPD). Es patente que ese establecimiento de medidas adecuadas y específicas solo puede ser expreso. Si la norma interna que regula el tratamiento de datos personales relativos a opiniones políticas, no prevé esas garantías adecuadas, sino que, todo lo más, se remite implícitamente a las garantías generales contenidas en el Reglamento general de protección de datos, no puede considerarse que haya llevado a cabo la tarea normativa que aquel le exige.*

*9. De lo anterior se concluye que la ley no ha identificado la finalidad de la injerencia para cuya realización se habilita a los partidos políticos, ni ha delimitado los presupuestos ni las condiciones de esa injerencia, ni ha establecido las garantías adecuadas que para la debida protección del derecho fundamental a la protección de datos personales reclama nuestra doctrina, por lo que se refiere a la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de sus actividades electorales.*

*De esta forma, se han producido tres vulneraciones del art. 18.4 CE en conexión con el art. 53.1 CE, autónomas e independientes entre sí, todas ellas vinculadas a la insuficiencia de la ley y que solo el legislador puede remediar, y redundando las tres en la infracción del mandato de preservación del contenido esencial del derecho fundamental que impone el art. 53.1 CE, (...).*

La misma doctrina sostiene el Tribunal de Justicia de la Unión Europea (TJUE). Así, si el art. 8 de la Carta Europea de los Derechos Fundamentales reconoce el derecho de toda persona a la protección de los datos de carácter personal que le conciernan, el art. 52.1 reconoce que ese derecho no es ilimitado y permite la limitación del ejercicio de esos derechos y libertades reconocidos por la Carta, limitación que deberá ser establecida por la ley y respetar el contenido esencial de los mismos.

Pues bien, la **STJUE de 6 de octubre de 2020**, en los **casos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros**, en su apartado 175, recuerda que:

*En cuanto a la justificación de dicha injerencia, cabe precisar que el requisito, previsto en el artículo 52, apartado 1, de la Carta, de que cualquier limitación del ejercicio de los derechos fundamentales **deba ser establecida por ley** implica que la base legal que la permita **debe definir ella misma el alcance***

**de la limitación del ejercicio del derecho** de que se trate (véase, en este sentido, la sentencia de 16 de julio de 2020, *Facebook Ireland y Schrems*, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).

Igualmente, el apartado 65 de la **Sentencia (STJUE) de la misma fecha 6 de octubre de 2020 (C-623/17)**, *Privacy International contra Secretary of State for Foreign and Commonwealth Affairs* y otros, dice:

*Cabe añadir que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida **por ley** implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (sentencia de 16 de julio de 2020, *Facebook Ireland y Schrems*, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).*

Es pues, la misma ley que establece la injerencia en el derecho fundamental la que ha de determinar las condiciones y garantías, esto es, el alcance y la limitación, que han de observarse en dichos tratamientos de datos sensibles.

Y en dicha **STJUE de 16 de julio de 2020**, se añade (y se reitera posteriormente en las citadas sentencias de 6 de octubre de 2020):

*176 Finalmente, para cumplir el requisito de proporcionalidad según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario, la normativa controvertida que conlleve la injerencia debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. En particular, **dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario.** La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado*

Aún más recientemente, en relación con este principio de legalidad, el TJUE, en sentencia de 21 de marzo de 2024, C-61/22, apartado 77, establece:

a) *Respeto del principio de legalidad*

*77 En lo que se refiere al requisito, establecido en el artículo 52, apartado 1, primera frase, de la Carta, de que cualquier limitación del ejercicio de los derechos reconocidos por ella debe ser establecida por **la ley**, ha de recordarse que este requisito implica que **el propio acto que permita la***

*injerencia en dichos derechos debe definir el alcance de la limitación del ejercicio del derecho de que se trate, con la precisión de que, por un lado, este requisito **no excluye** que la limitación en cuestión se formule en **términos lo suficientemente abiertos** como para poder adaptarse a supuestos distintos, así como a los cambios de situación, y de que, por otro lado, el Tribunal de Justicia, en su caso, puede precisar, por vía de interpretación, el alcance concreto de la limitación en relación tanto con los propios términos de la normativa de la Unión de que se trate como con su estructura general y los objetivos que persigue, interpretados a la luz de los derechos fundamentales garantizados por la Carta (sentencia de 21 de junio de 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, apartado 114).*

La ya citada STJUE de 6 de octubre de 2020, en el caso C-623/17, añade la mención de las **categorías especiales de datos**:

*68 (...) Estas consideraciones son aplicables **en particular cuando está en juego la protección de esa categoría particular de datos personales que son los datos sensibles** [véanse, en este sentido, las sentencias de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 54 y 55, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 117; dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 141].*

Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, tal y como recuerda la **Sentencia del Tribunal Constitucional 14/2003, de 28 de enero**:

*“En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; SSTC 66/1995, de 8 de mayo F. 5; 55/1996, de 28 de marzo, FF. 7, 8 y 9; 270/1996, de 16 de diciembre, F. 4.e; 37/1998, de 17 de febrero, F. 8; 186/2000, de 10 de julio, F. 6).”*

En consecuencia, los límites referidos con carácter general a cualesquiera tratamientos de datos personales son todavía más estrictos cuando se trata de datos



de categorías especiales (también conocidos como datos sensibles), los cuales necesariamente deben establecerse por una norma con rango de ley, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, definiendo todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías adecuadas.

### III

Entrando al análisis del proyecto normativo objeto de este informe desde la perspectiva de la normativa de protección de datos personales, que es lo que compete a esta Agencia, y de acuerdo con la Memoria Justificativa recibida, el presente borrador de Real Decreto pretende desarrollar y concretar los requisitos que debe tener un registro de jornada eficaz, al amparo de la habilitación que el artículo 34.7 y el apartado primero de la disposición final segunda del Estatuto de los Trabajadores (en adelante ET) otorga al Gobierno. A tal fin se proyecta una norma que consta de 9 artículos y seis disposiciones finales.

En cuanto a la tramitación de esta norma se refiere se observa que se autorizó por el Consejo de Ministros con fecha de 30 de septiembre de 2025 la tramitación administrativa urgente del procedimiento de elaboración y aprobación de este Real Decreto, habiendo sido recabados de conformidad con el artículo 26.5 de la Ley 50/1997, de 27 de noviembre, además del informe preceptivo de la Secretaría General Técnica del Ministerio de Trabajo y Economía Social, informe del Ministerio de Economía, Comercio y Empresa, informe del Ministerio de Transformación Digital y Función Pública, e informe de esta Agencia Española de Protección de Datos. Todo ello sin perjuicio del informe de la Oficina de Coordinación y Calidad Normativa ex artículo 26.9 de la Ley 50/1997, de 27 de noviembre, y del informe del Consejo de Estado en cumplimiento del artículo 26.7 de la Ley 50/1997, de 27 de noviembre. Asimismo, en cuanto al análisis de impactos se refiere, se observa la evaluación de los impactos en cuanto a la adecuación al orden de competencias, al impacto económico y presupuestario, al impacto de género, así como a los impactos en materia de infancia y adolescencia, en la familia, por razón del cambio climático, en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.

Sin embargo, no se ha realizado ningún informe acerca del análisis de riesgos o evaluación de impacto en materia de protección de datos (EIPD) 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.

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.*

No resulta dudoso, sino evidente del propio texto del proyecto informado, que el contenido del registro de jornada al que se refiere este borrador tratará datos personales. Siendo ésta, además, una cuestión pacífica a la vista de la sentencia del TJUE de fecha de 30 de mayo de 2013, en cuyo párrafo 22 expresa que: “(...) el artículo 2, letra a), de la Directiva 95/46 debe interpretarse en el sentido de que un registro del tiempo de trabajo, como el controvertido en el litigio principal, que incluye la indicación de las horas en que cada trabajador inicia y finaliza la jornada, así como de las pausas o períodos de descanso correspondientes, queda comprendido en el concepto de «datos personales» a efectos de dicha disposición”.

En esta misma línea, cabe recordar que 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.*

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

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.***

Dicho análisis de riesgos o la EIPD no parece haberse llevado a cabo por el órgano proponente de este proyecto normativo. Ello no obstante, esta Agencia considera de la mayor importancia en una norma como la proyectada la realización de un análisis de riesgos y la evaluación de los impactos en materia de protección de datos, pues precisamente el objeto central de esta norma, no meramente indirecto o derivado, es regular la recogida, registro, organización, consulta y utilización de tales datos por el empleador, así como su puesta a disposición de las autoridades competentes en materia de supervisión de las condiciones de trabajo, y de los representantes de los trabajadores en la empresa.

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 (art. 24 y 25 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, cabe recordar, 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 la este borrador normativo.

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”**<sup>1</sup>, 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 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:***

<sup>1</sup> <https://www.aepd.es/es/documento/orientaciones-evaluacion-impacto-desarrollo-normativo.pdf>



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.**

#### **IV**

Sentada pues esta ausencia de análisis de riesgos (artículos 24 y 25 RGPD) y evaluación de impacto relativa a la protección de datos personales (artículo 35 RGPD), cuestión sobre la que volveremos más tarde, hemos de volver a recordar, tal y como dijimos al principio de este informe que, de conformidad con el artículo 6 RGPD, con carácter previo al establecimiento de una intromisión en este derecho fundamental a la protección de datos, procede comprobar la existencia de una base reguladora habilitante del tratamiento de datos que se desea realizar.

En este sentido, el TJUE en su sentencia de 30 de mayo de 2013, en respuesta a las cuestiones prejudiciales segunda y tercera acerca de si un Estado Miembro (en dicho caso el portugués) estaba obligado en virtud del artículo 17, apartado 1, de la Directiva 95/46, a prever medidas técnicas y de organización adecuadas para la protección de los datos personales contra la destrucción accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red; y acerca de si, en caso de respuesta afirmativa a la cuestión anterior, podía interpretarse el principio de primacía del Derecho de la Unión en el sentido de que el Estado Miembro no podía sancionar a la entidad empleadora por dicho comportamiento, cuanto el Estado Miembro no hubiera adoptado ninguna medida en cumplimiento del citado artículo 17.1 y cuando la entidad empleadora, responsable del tratamiento de los datos, hubiera adoptado un sistema de acceso restringido a tales datos que no permita el acceso automático de la autoridad nacional competente para la supervisión de las condiciones de trabajo, dictamina lo siguiente (el subrayado es nuestro):

*“En el presente asunto, corresponde al órgano jurisdiccional remitente examinar si la obligación del empleador de dar acceso a la autoridad nacional competente para la supervisión de las condiciones de trabajo al registro del tiempo de trabajo, de forma que se permita su consulta inmediata, puede considerarse necesaria para el cumplimiento por esta autoridad de la misión de supervisión que le incumbe, contribuyendo a una mayor eficacia en la aplicación de la normativa sobre condiciones de trabajo y, especialmente, de la relativa al tiempo de trabajo. 44 A este respecto, debe precisarse que en cualquier caso, aun cuando esta obligación se considere necesaria para alcanzar tal objetivo, las sanciones impuestas para garantizar la aplicación efectiva de las exigencias establecidas en la Directiva 2003/88 han de respetar el principio de proporcionalidad, circunstancia que debe verificar también el órgano jurisdiccional remitente en el litigio principal (véase, por analogía, la sentencia de 6 de noviembre de 2003, Lindqvist, C-101/01, Rec. p. I-12971, apartado 88). Por consiguiente, procede responder a las cuestiones segunda y tercera que los artículos 6, apartado 1, letras b) y c), y 7, letras c) y e), de la Directiva 95/46 deben interpretarse en el sentido de que no se oponen a una normativa nacional, como la controvertida en el litigio principal, que impone al empleador la obligación de poner a disposición de la autoridad nacional competente para la supervisión de las condiciones de trabajo el registro del tiempo de trabajo, de forma que se permita su consulta inmediata, siempre que esta obligación sea necesaria para el cumplimiento por esta autoridad de la misión de supervisión que le incumbe en relación con la aplicación de la normativa sobre condiciones de trabajo y, especialmente, de la relativa al tiempo de trabajo”.*

En lo que se refiere a este proyecto normativo son varias las disposiciones legales que han contemplado el registro de jornada y que, con acierto, son citadas tanto en el texto de la MAIN como en el propio articulado del mismo, cuyo artículo 1 que lleva por rúbrica *Objeto* dispone:

*“Este real decreto tiene por objeto desarrollar los artículos 12.4.c), 34.7 y 9 y 35.5 del texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre, en particular, en materia de registro de jornada”.*

Entre tales bases legales cabe traer a colación la que se contiene en el artículo 34.9 ET en cuya virtud se establece que (el subrayado es nuestro):

*“La empresa garantizará el registro diario de jornada, que deberá incluir el horario concreto de inicio y finalización de la jornada de trabajo de cada persona trabajadora, sin perjuicio de la flexibilidad horaria que se establece en este artículo.*

*Mediante negociación colectiva o acuerdo de empresa o, en su defecto, decisión del empresario previa consulta con los representantes legales de los trabajadores en la empresa, se organizará y documentará este registro de jornada.*

*La empresa conservará los registros a que se refiere este precepto durante cuatro años y permanecerán a disposición de las personas trabajadoras, de sus representantes legales y de la Inspección de Trabajo y Seguridad Social".*

En consecuencia, la existencia de diferentes previsiones legales permitirá al legislador desarrollar la regulación del registro de jornada por tratarse de una obligación legalmente impuesta al empresario. No obstante, resulta igualmente importante recordar que, como indica el precepto ut supra transcrito también es posible el desarrollo, complemento y organización de dicho registro de jornada mediante *negociación colectiva o acuerdo de empresa* de conformidad con el artículo 34.9 apartado segundo ut supra transcrito. Dicho lo cual, sin perjuicio de la conveniencia de regular la eventual coexistencia de normativa estatal y convencional a propósito de esta materia, corresponde a este Servicio Jurídico centrarse en el alcance que deba tener la regulación del registro de jornada a través de esta norma reglamentaria.

A este respecto no cabe duda de que **ninguna de las habilitaciones legales existentes refiere el tratamiento de datos de categorías especiales**, lo que determina la imposibilidad de que el registro de jornada incluya la recogida y tratamiento de datos sensibles o especialmente protegidos (art. 9 RGPD). En este sentido, tal y como se acaba de explicar en el fundamento segundo de este informe, el tratamiento de datos sensibles solo resulta admisible cuando concurre alguna de las causas excepcionales por las que se levanta la prohibición general de realizar su tratamiento previstas en el artículo 9.2 RGPD. La habilitación legal actualmente existente permite la recogida y tratamiento de los datos personales mínimos y necesarios para el fin perseguido (registro de jornada) pero no habilita en modo alguno la recogida y tratamiento de datos sensibles, los cuales habrán de quedar en todo caso excluidos de su alcance y contenido.

Asimismo, cabe añadir que en el artículo 3 de este proyecto normativo, el cual lleva por rúbrica *Contenido mínimo del registro de jornada* no se ha detectado que haya sido prevista la recogida y tratamiento de este tipo de datos sensibles; sin detrimento de lo cual, se considera oportuno reiterar que **de ningún modo podrá considerarse el registro de jornada habilitado para el tratamiento de datos sensibles por faltar la habilitación legal específica para ello**; dicha recogida y tratamiento de datos sensibles a través del registro de jornada sería ilícita e inadmisibles al no contar con la mencionada cobertura de rango legal.

## **V**

Como se ha explicado en los fundamentos de derecho primero y segundo de este informe, cuando se trate de tratamientos derivados de una obligación legal o de la atribución de competencias o misiones de interés público ex artículo 6.1.c) y e) RGPD, la regulación de desarrollo debe contar necesariamente, como punto de partida, con dicha norma legal, sin que sea suficiente con la mera existencia de ley formal para dar

cobertura a tales tratamiento de datos; dicha ley meramente formal, por sí sola no será suficiente, sino que la misma deberá cumplir con los requisitos establecidos por la doctrina reiterada del TJUE y de nuestro Tribunal Constitucional.

Teniendo presente la doctrina expuesta en los fundamentos de derecho primero y segundo de este informe, resulta posible en el supuesto que ahora nos ocupa llegar a considerar que los *mínimos imprescindibles* relativos al registro de jornada han quedado incluidos en las diversas normas legales que lo regulan, las cuales, como hemos dicho antes, han sido convenientemente citadas en el artículo 1 de este proyecto normativo; siendo, por lo tanto, ésta la base legal sobre la que procede ubicar el marco de actuación del actual proyecto normativo.

Centrado así el marco de habilitación legal de la norma reglamentaria objeto de estudio resulta apropiado, por su importancia a la hora de delimitar su alcance y contenido, traer a colación el artículo 6.3 RGPD en cuya virtud se dispone que:

*“3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:*

*a) el Derecho de la Unión, o*

*b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.*

*La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. **Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.***

El precepto que acabamos de transcribir establece la posibilidad de que determinadas “*disposiciones específicas*” relativas al alcance y contenido del tratamiento que se habilita en la ley se contengan en dicha base jurídica, es decir en la norma que lo habilita utilizando el término potestativo “*podrá contener*”, lo que a su vez hace posible admitir que tales “*desarrollos específicos concretos*” no se contengan en las normas legales habilitantes del tratamiento (en este caso habilitantes del registro de jornada), sino en el desarrollo reglamentario que se habrá de realizar respecto de tales tratamientos; los cuales habrán necesariamente de recogerse en la norma jurídica de rango inmediatamente inferior.



En cuanto al registro de jornada se refiere, dichos “desarrollos específicos concretos” habrán de contenerse en este proyecto normativo, siendo pues indispensable analizar su alcance y contenido a fin de verificar la presencia o ausencia de los mismos. A este respecto, se observa que el artículo 2, *Obligación de disponer de un registro de jornada*, dispone en su apartado primero: “*Todas las empresas garantizarán el registro diario de la jornada de trabajo realizada por cada persona trabajadora en su lugar de trabajo, por medios digitales*”. Sin embargo, la imposición de llevanza del registro de jornada no resulta directamente de las habilitaciones legales de continua referencia; el citado artículo 34.9 ET no especifica cuál deba ser la forma o formas de llevanza del registro, por lo que la previsión de una forma específica y excluyente de otras posibles implicaría una restricción que podría resultar contraria no solo a la ley, sino también a la norma convencional que pudiera eventualmente desarrollarse en un sentido distinto. Por todo lo cual, la previsión de esta llevanza del registro digital de manera excluyente de otras modalidades de llevanza del mismo resulta carente de fundamento y de justificación, toda vez que al no haberse realizado el correspondiente análisis de riesgos, ni tampoco la evaluación de impacto prevista en el artículo 35 RGPD no se conocen las razones, ni las justificaciones, caso de haberlas, que pudieran permitir o incluso aconsejar la adopción de esta forma de llevanza como la más adecuada para la tuición de este derecho y cumplimiento de los fines de estos tratamientos.

El mismo artículo 2 en su apartado 3 dispone que: “*El sistema de registro de jornada garantizará adecuadamente el derecho a la intimidad y a la protección de datos, en los términos previstos en la normativa aplicable en materia de protección de datos, de acuerdo con los principios de minimización, idoneidad, necesidad y proporcionalidad*”. Lamentablemente, a pesar de ser correcta esta redacción debe objetarse su insuficiencia dado que corresponde a este proyecto normativo no solo afirmar la obligación de cumplir sino concretar las medidas técnicas y organizativas, así como las garantías previstas para preservar dicho cumplimiento, y no solo de los citados principios sino de todos y cada uno de los principios generales previstos en el artículo 5 RGPD en materia de protección de datos personales. Del mismo modo, corresponde a este Real Decreto especificar quién o quiénes serán en cada caso los responsables de los tratamientos, y las medidas técnicas y organizativas necesarias para evitar la destrucción accidental o ilícita de estos datos personales, la difusión o acceso no autorizados etc.

El artículo 3, *Contenido mínimo del registro de jornada*, prevé que: “*El sistema permitirá, como mínimo, el registro de la siguiente información: (...)*”, debiendo hacerse notar que no resulta admisible que la norma de desarrollo de estos tratamientos establezca un contenido mínimo susceptible de ulterior desarrollo a través de cierto tipo de normativa que tampoco se llega a explicitar en este borrador. Siendo pacífico que de ningún modo podrá este registro contener datos sensibles, corresponde a este borrador de Real Decreto especificar con carácter taxativo los datos personales que podrán ser recogidos por resultar imprescindibles para el cumplimiento de la finalidad perseguida por el mismo (principio de minimización y de finalidad, artículo 5 RGPD). Razonamiento que resulta igualmente aplicable a la letra a) de este artículo 3:

*Identificación de la persona trabajadora que realiza el asiento, con los datos personales imprescindibles para la finalidad del registro, volviéndose a reiterar la necesidad de que este borrador delimite el contenido mínimo de los datos que podrán ser tratados al amparo de este registro de jornada, no siendo posible su remisión a normativa posterior que no resulta especificada ni justificada. Análogamente, se desconocen las razones por las que se ha considerado razonable o justificado a los fines de este registro incluir dentro del contenido mínimo la referencia al carácter retribuido o no de las horas extraordinarias realizadas en la letra f) del artículo 3. Como decimos, todas estas cuestiones precisan de la elaboración previa de un análisis de riesgos (artículos 24 y 25 RGPD) y de una evaluación de impacto (artículo 35 RGPD) que arroje una panorámica clara no solo de los contenidos, fines y demás medidas necesarias en relación con los tratamientos, sino también de todos los riesgos posibles, y de las medidas y garantías técnicas y organizativas necesarias para paliarlos.*

De igual manera, la previsión contenida en el artículo 4.e): *La empresa garantizará que el registro no se ubique en zonas de acceso público ni encontrarse accesible a personas distintas de las que deban realizar cada asiento*, adolece de falta de justificación técnica y jurídica, pues parece contemplar única y exclusivamente la realización del registro en la empresa *in situ*, obviando la realidad del teletrabajo, cada vez más presente en todas las empresas de nuestro país. Asimismo, si el asiento debe realizarse por cada persona trabajadora respecto de su jornada, tal y como prevé la letra a) de este artículo, se observa falta de justificación técnica y jurídica acerca de cómo se garantizará la limitación de accesos a personas distintas a las que deban realizar el asiento.

En relación con el artículo 6.2 en cuya virtud: *El sistema de registro permitirá que la representación legal de las personas trabajadoras pueda consultar y obtener copia de todos asientos y modificaciones, en cualquier momento y de forma inmediata, en el centro de trabajo*; siendo esta previsión de accesos conforme con la habilitación legal existente y alineada con la jurisprudencia del TJUE anteriormente comentada, se aprecia, nuevamente, ausencia de referencia a cuestiones esenciales para garantizar la adecuada protección de este derecho a la protección de datos personales. Determinadas cuestiones tales como si será posible el acceso por personas legitimadas fuera del centro de trabajo o no, toda vez que la llevanza del registro será digital, o en qué circunstancias y para qué finalidades quedará justificado y habilitado el acceso por las personas legitimadas, no se especifican en este borrador.

Las limitaciones que venimos comentado con detalle en este informe a propósito de la remisión reglamentaria ligada a la materia reservada a la ley, dirigidas a que se formule en condiciones tales que no contraría materialmente la finalidad de la reserva resultan igualmente aplicables respecto del artículo 8 sobre *Requisitos Técnicos*, por el que se dispone que: *Sin perjuicio de lo establecido en el artículo 9, las empresas deberán adoptar un sistema de registro que cumpla con los requisitos técnicos que se establezcan en las disposiciones de desarrollo.*

A modo de conclusión, tal y como se ha expuesto a lo largo de este informe, la norma de desarrollo de una habilitación legal relativa a un tratamiento de datos personales (excluidos los datos de categorías especiales) debe ser el complemento de la regulación legal indispensable por motivos técnicos o para optimizar el cumplimiento de las finalidades propuestas por la Constitución o por la propia Ley, sin que dicha remisión pueda enmascarar una renuncia del legislador a la facultad de establecer los límites al derecho fundamental. A tales efectos el artículo 6.3 RGPD constituye la referencia esencial en cuanto a la determinación del contenido mínimo que dicha norma de desarrollo deberá regular, para el caso se no haber sido previsto previamente en la normativa legal habilitante dicho contenido mínimo.

En consecuencia, la ausencia en este proyecto normativo del análisis de riesgos (artículo 24 y 25 RGPD) y evaluación de impacto en materia de datos personales (artículo 35 RGPD), junto con la falta de regulación de los “desarrollos específicos concretos” referidos en el citado artículo 6.3 RGPD, tales como, a título meramente ejemplificativo, las concretas condiciones de licitud de los tratamientos, los tipos de datos que serán objeto del tratamiento, los plazos de conservación de los datos, o las operaciones y procedimientos del tratamiento, determinan que el contenido de este proyecto normativo no pueda considerarse suficiente a efectos de considerar colmada la reserva legal existente.