N/REF: 0066/2021

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente al Anteproyecto de Ley del mercado de valores y de los servicios de inversión, solicitado, con carácter urgente, de esta Agencia Española de Protección de Datos (AEPD) de conformidad con lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), en relación con el artículo 57.1, letra c), del 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 5 b) del Estatuto de la Agencia, aprobado por Real Decreto 389/2021, de 1 de junio, cúmpleme informarle lo siguiente:

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.

El texto remitido implica una importante reforma sistemática de la actual normativa reguladora de los mercados de valores con el fin de acabar, en la medida de lo posible, con el excesivo carácter reglamentista del vigente texto refundido de la Ley del Mercado de Valores, siguiendo el criterio señalado por el Consejo de Estado en su Dictamen 319/2018, en el que se destacaba cómo una regulación ordenada de los mercado de valores hubiera exigido una ley de nueva planta que contuviera las normas y principios básicos, remitiendo a la vía reglamentaria el desarrollo pormenorizado en tantos reglamentos como fueran necesarios.

De este modo, y con el objetivo de incrementar la seguridad jurídica, el anteproyecto de ley simplifica y reordena el contenido del actual texto refundido de la Ley del Mercado de Valores, deslegalizando cuestiones técnicas de detalle en reglamentos de desarrollo, de tal forma que se faciliten al máximo futuras reformas del texto legal.

Asimismo, el anteproyecto de ley procede a la transposición de las siguientes Directivas:

- Directiva (UE) 2019/2034 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019 relativa a la supervisión prudencial de las empresas de servicios de inversión, y por la que se modifican las Directivas 2002/87/CE, 2009/65/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE y 2014/65/UE.
- Directiva (UE) 2019/2177 del Parlamento Europeo y del Consejo de 18 de diciembre de 2019 por la que se modifica la Directiva 2009/138/CE sobre el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II), la Directiva 2014/65/UE relativa a los mercados de instrumentos financieros y la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo.
- Directiva (UE) 2020/1504 del Parlamento Europeo y del Consejo, de 7 de octubre de 2020, por la que se modifica la Directiva 2014/65/UE relativa a los mercados de instrumentos financieros.
- Directiva (UE) 2021/338 del Parlamento Europeo y del Consejo de 16 de febrero de 2021 por la que se modifica la Directiva 2014/65/UE en lo relativo a los requisitos de información, la gobernanza de productos y la limitación de posiciones, y las Directivas 2013/36/UE y (UE) 2019/878 en lo relativo a su aplicación a las empresas de servicios de inversión con el fin de contribuir a la recuperación de la crisis de la COVID-19.

Por último, se incorpora en el texto el contenido de dos normas vigentes que regulan aspectos parciales de los mercados de valores:
- El Real Decreto-ley 21/2017, de 29 de diciembre, de medidas urgentes para la adaptación del derecho español a la normativa de la Unión Europea en materia del mercado de valores.
- El Real Decreto-ley 14/2018, de 28 de septiembre, por el que se modifica el texto refundido de la Ley del Mercado de Valores, aprobado por el Real Decreto Legislativo 4/2015, de 23 de octubre.

I

Con carácter previo al análisis concreto del texto remitido, deben realizarse unas consideraciones generales respecto de la aplicación de la normativa sobre protección de datos personales, teniendo en cuenta que la finalidad primordial del texto objeto de informe es la de proceder a una deslegalización de gran parte de sus preceptos para incluirlos en los correspondientes reglamentos de desarrollo, introduciendo las correspondientes habilitaciones a favor del Gobierno o de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital o de la Comisión Nacional del Mercado de Valores.

En lo que a la materia de protección de datos personales respecta, la norma a la que debe ajustarse el Anteproyecto de Ley sometido a consulta es 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 por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD), plenamente aplicable desde el 25 de mayo de 2018 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

El RGPD permite a los Estados Miembros, en determinados supuestos, introducir modulaciones en el régimen general de protección de datos personales o regular determinados tratamientos de datos personales. Esta regulación, en el caso de España, siendo el derecho a la protección de datos personales un derecho fundamental reconocido en el artículo 18.4. de la Constitución, debe realizarse por una norma con rango de ley, tal y como resulta del artículo 53 de la misma que prevé que sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades.

Por otro lado, el Tribunal Constitucional ha tenido ocasión de examinar los requisitos para que las leyes que establecen tratamientos de datos personales, en cuanto que restricciones al derecho fundamental a la protección de datos personales del interesado, puedan considerarse conformes a la Constitución.

En este sentido, la **STC 292/2000, de 30 de noviembre**, después de configurar el derecho fundamental a la protección de datos personales 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, analiza los límites del mismo, señalando en su lo siguiente:

> Más concretamente, en las Sentencias mencionadas relativas a la protección de datos, este Tribunal ha declarado que el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, F. 7; 196/1987, de 11 de diciembre [RTC 1987, 196] , F. 6; y respecto del art. 18, la STC 110/1984, F. 5). Esos límites o bien pueden ser restricciones directas del derecho fundamental

mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE. La primera constatación que debe hacerse, que no por evidente es menos capital, es que la Constitución ha querido que la Ley, y sólo la Ley, pueda fijar los límites a un derecho fundamental. Los derechos fundamentales pueden ceder, desde luego, ante bienes, e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido (SSTC 57/1994, de 28 de febrero [RTC 1994, 57] , F. 6; 18/1999, de 22 de febrero [RTC 1999, 18] , F. 2).

Justamente, si la Ley es la única habilitada por la Constitución para fijar los límites a los derechos fundamentales y, en el caso presente, al derecho fundamental a la protección de datos, y esos límites no pueden ser distintos a los constitucionalmente previstos, que para el caso no son otros que los derivados de la coexistencia de este derecho fundamental con otros derechos y bienes jurídicos de rango constitucional, el apoderamiento legal que permita a un Poder Público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, sólo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos. **Por tanto, si aquellas operaciones con los datos personales de una persona no se realizan con estricta observancia de las normas que lo regulan, se vulnera el derecho a la protección de datos, pues se le imponen límites constitucionalmente ilegítimos, ya sea a su contenido o al ejercicio del haz de facultades que lo componen.** Como lo conculcará también esa Ley limitativa si regula los límites de forma tal que hagan impracticable el derecho fundamental afectado o ineficaz la garantía que la Constitución le otorga. Y así será cuando la Ley, que debe regular los límites a los derechos fundamentales con escrupuloso respeto a su contenido esencial, se limita a apoderar a otro Poder Público para fijar en cada caso las restricciones que pueden imponerse a los derechos fundamentales, cuya singular determinación y aplicación estará al albur de las decisiones que adopte ese Poder Público, quien podrá decidir, en lo que ahora nos interesa, sobre la obtención, almacenamiento, tratamiento, uso y cesión de datos personales en los casos que estime convenientes y esgrimiendo, incluso, intereses o bienes que no son protegidos con rango constitucional […]". (Fundamento Jurídico 11)

"De un lado, porque si bien este Tribunal ha declarado que la Constitución no impide al Estado proteger derechos o bienes jurídicos a costa del sacrificio de otros igualmente reconocidos y, por tanto, que el legislador pueda imponer limitaciones al contenido de los derechos fundamentales o a su ejercicio, también hemos precisado que, en tales supuestos, esas limitaciones han de estar justificadas en la protección de otros derechos o bienes constitucionales (SSTC 104/2000, de 13 de abril [RTC 2000, 104] , F. 8 y las allí citadas) y, además, han de ser proporcionadas al fin perseguido con ellas (SSTC 11/1981, F. 5, y 196/1987, F. 6). Pues en otro caso incurrirían en la arbitrariedad proscrita por el art. 9.3 CE.

De otro lado, aun teniendo un fundamento constitucional y resultando proporcionadas las limitaciones del derecho fundamental establecidas por una Ley (STC 178/1985 [RTC 1985, 178]), **éstas pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad en los propios límites que imponen y su modo de aplicación**. Conclusión que se corrobora en la jurisprudencia del Tribunal Europeo de Derechos Humanos que ha sido citada en el F. 8 y que aquí ha de darse por reproducida. Y ha de señalarse, asimismo, que no sólo lesionaría el principio de seguridad jurídica (art. 9.3 CE), concebida como **certeza sobre el ordenamiento aplicable y expectativa razonablemente fundada de la persona sobre cuál ha de ser la actuación del poder aplicando el Derecho** (STC 104/2000, F. 7, por todas), sino que al mismo tiempo dicha Ley estaría lesionando el contenido esencial del derecho fundamental así restringido, dado que la forma en que se han fijado sus límites lo hacen irreconocible e imposibilitan, en la práctica, su ejercicio (SSTC 11/1981, F. 15; 142/1993, de 22 de abril [RTC 1993, 142] , F. 4, y 341/1993, de 18 de noviembre [RTC 1993, 341] , F. 7). De suerte que la falta de precisión de la Ley en los presupuestos materiales de la limitación de un derecho fundamental es susceptible de generar una indeterminación sobre los casos a los que se aplica tal restricción. Y al producirse este resultado, más allá de toda interpretación razonable, la Ley ya no cumple su función de garantía del propio derecho fundamental que restringe, pues deja que en su lugar opere simplemente la voluntad de quien ha de aplicarla, menoscabando así tanto la eficacia del derecho fundamental como la seguridad jurídica […]". (FJ 15).

"Más concretamente, en relación con el derecho fundamental a la intimidad hemos puesto de relieve no sólo la necesidad de que sus posibles limitaciones estén fundadas en una previsión legal que tenga justificación constitucional y que sean proporcionadas (SSTC 110/1984, F. 3, y 254/1993, F. 7) sino que **la Ley que restrinja este derecho debe expresar con precisión todos y cada uno de los presupuestos materiales de la medida limitadora**. De no ser así, mal cabe entender

que la resolución judicial o el acto administrativo que la aplique estén fundados en la Ley, ya que lo que ésta ha hecho, haciendo dejación de sus funciones, es apoderar a otros Poderes Públicos para que sean ellos quienes fijen los límites al derecho fundamental (SSTC 37/1989, de 15 de febrero [RTC 1989, 37], y 49/1999, de 5 de abril [RTC 1999, 49]).
De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concurra algún derecho o bien constitucionalmente protegido. **Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias.** Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación. […] (FJ 16)".

Más recientemente, analizando igualmente los límites al derecho fundamental a la protección de datos personales, la **sentencia núm. 76/2019 de 22 mayo** después de recordar que "A la vista de los potenciales efectos intrusivos en el derecho fundamental afectado que resultan del tratamiento de datos personales, la jurisprudencia de este Tribunal le exige al legislador que, además de cumplir los requisitos anteriormente mencionados, también establezca 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. En este fundamento jurídico precisaremos la naturaleza y el alcance de este específico requisito constitucional", analiza cuál es la norma que debe contener las citadas garantías:

"Por tanto, la resolución de la presente impugnación exige que aclaremos una duda suscitada con respecto al alcance de nuestra doctrina sobre las garantías adecuadas, que consiste en determinar si las garantías adecuadas frente al uso de la informática deben contenerse en la propia ley que autoriza y regula ese uso o pueden encontrarse también en otras fuentes normativas.

La cuestión solo puede tener una respuesta constitucional. 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 art. 53.1 CE (RCL 1978, 2836) para el legislador de los derechos fundamentales: la reserva de ley para la regulación del ejercicio de los derechos fundamentales reconocidos en el capítulo segundo del título primero de la Constitución y el respeto del contenido esencial de dichos derechos fundamentales.

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" (FJ 8).

Por otro lado, y en lo que se refiere al principio de proporcionalidad la **Sentencia del Tribunal Constitucional 14/2003, de 28 de enero**, recuerda lo siguiente:

"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 [RTC 1995, 66] , F. 5; 55/1996, de 28 de marzo [RTC 1996, 55] , FF. 7, 8 y 9; 270/1996, de 16 de diciembre [RTC 1996, 270] , F. 4.e; 37/1998, de 17 de febrero [RTC 1998, 37] , F. 8; 186/2000, de 10 de julio [RTC 2000, 186] , F. 6)."

De acuerdo con la citada doctrina constitucional, 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.

La necesidad de regulación por norma con rango de ley aparece, asimismo, expresamente reconocida en determinados preceptos de la LOPDGDD, como el artículo 8, relativo al tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos, el artículo 9 respecto de las categorías especiales de datos, el artículo 10 respecto del tratamiento de datos de naturaleza penal, el artículo 27 para el tratamiento de datos relativos a infracciones y sanciones administrativas o la disposición adicional decimoséptima sobre tratamientos de datos de salud.

En este caso concreto, en relación con las habilitaciones para el desarrollo reglamentario, esta Agencia considera conveniente recordar expresamente las palabras del Tribunal Constitucional en su sentencia 292/2000, de 30 de noviembre, que declaró inconstitucionales determinados preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

> De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concurra algún derecho o bien constitucionalmente protegido. **Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias.** Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 C.E., esto es, establecer claramente el límite y su regulación.
>
> 17. En el caso presente, el empleo por la L.O.P.D. en su art. 24.1 de la expresión «funciones de control y verificación», abre un espacio de incertidumbre tan amplio que provoca una doble y perversa consecuencia. De un lado, al habilitar la L.O.P.D. a la Administración

> para que restrinja derechos fundamentales invocando semejante expresión está renunciando a fijar ella misma los límites, apoderando a la Administración para hacerlo. Y de un modo tal que, como señala el Defensor del Pueblo, permite reconducir a las mismas prácticamente toda actividad administrativa, ya que toda actividad administrativa que implique entablar una relación jurídica con un administrado, que así será prácticamente en todos los casos en los que la Administración necesite de datos personales de alguien, conllevará de ordinario la potestad de la Administración de verificar y controlar que ese administrado ha actuado conforme al régimen jurídico administrativo de la relación jurídica entablada con la Administración. Lo que, a la vista del motivo de restricción del derecho a ser informado del art. 5 L.O.P.D., deja en la más absoluta incertidumbre al ciudadano sobre en qué casos concurrirá esa circunstancia (si no en todos) y sume en la ineficacia cualquier mecanismo de tutela jurisdiccional que deba enjuiciar semejante supuesto de restricción de derechos fundamentales sin otro criterio complementario que venga en ayuda de su control de la actuación administrativa en esta materia.

Por consiguiente, en el nuevo esquema planteado de una ley marco y reglamentos de desarrollo, los aspectos esenciales que afecten a los tratamientos de datos de carácter personal deberán quedar recogidos en la norma legal, sin perjuicio de su ulterior desarrollo, dentro de los límites legales, por los correspondientes reglamentos, conforme a la doctrina constitucional anteriormente señalada.

Por otro lado, hay que destacar que el RGPD extiende su protección, tal y como establece su artículo 1.2, a los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, definidos en su artículo 4.1 como “toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.”

Quedan, en consecuencia, excluidas de su protección las personas jurídicas, pero su ámbito protector se extiende a las personas físicas que las representan, cuyos datos personales deben ser tratados con sujeción a lo previsto en dicho Reglamento.

La protección conferida por el Reglamento (UE) 2016/679 comprende también a los empresarios individuales, a diferencia de la normativa anterior, en la que el artículo 2.3 del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real decreto 1720/2017, de 21 de diciembre, excluía de su

ámbito de aplicación los datos de los empresarios individuales, cuando el tratamiento de los datos a ellos referentes lo fuera en su calidad de comerciantes, industriales o navieros. El Reglamento (UE) 2016/679 no establece ninguna exclusión en este sentido, de modo que el tratamiento de los datos personales relativos a los empresarios individuales debe someterse a las previsiones contenidas en esta norma.

Por consiguiente, el presente informe se centrará en aquellas cuestiones que impliquen tratamientos de datos de carácter personal de personas físicas.

Por último, para concluir estas consideraciones generales y respecto de las principales novedades introducidas por el RGPD, es preciso recordar, como ya se ha indicado en reiteradas ocasiones por esta Agencia, que la reforma operada por el Reglamento general de protección de datos respecto del régimen contenido en la Ley Orgánica 15/1999 exige un cambio de perspectiva en lo que respecta a los principios articuladores del derecho fundamental a la protección de datos de carácter personal y, en particular, a aquél que hacía del "principio de consentimiento" el eje central del derecho a la protección de datos.

En efecto, si bien la Ley Orgánica y el Reglamento no difieren excesivamente en lo que atañe a la enumeración de las causas legitimadoras del tratamiento, se produce una modificación sumamente relevante en el modo en que dichas causas aparecen recogidas por los textos aplicables: así, mientras del tenor de la Ley Orgánica 15/1999 parecía deducirse que la regla básica de legitimación era, con carácter general, el consentimiento, resultando las restantes causas legitimadoras excepcionales en relación con el consentimiento, que como regla general debía regir el tratamiento, en el texto del artículo 6.1 del Reglamento general de protección de datos el consentimiento se recoge como una de las seis causas de legitimación para el tratamiento, sin ostentar mayor o menor importancia que las restantes que en la norma se enumeran.

A mayor abundamiento, el propio Reglamento general de protección de datos pone de manifiesto que el consentimiento del afectado no debe constituir la base legal del tratamiento en determinados supuestos. Así, el considerando 42 señala en su última frase que "El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno" y el considerando 43 añade que "Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular".

De este modo, no procede recabar en ningún caso el consentimiento del afectado en los supuestos en los que el tratamiento se encuentre amparado por cualquiera de las causas incluidas en las letras b) a f) del artículo 6.1 del reglamento general de protección de datos; es decir cuando:

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

En el presente caso, teniendo en cuenta la intensa regulación legal del Mercado de Valores y de los Servicios de Inversión, los tratamientos de datos personales que sean consecuencia de la aplicación de la presente ley encontrarán su fundamento, generalmente, en el cumplimiento de obligaciones legales conforme al artículo 6.1.c) del RGPD (como ocurre, por ejemplo, respecto de la apreciación de los criterios de honorabilidad, a los que nos referiremos posteriormente, o la evaluación de la idoneidad y la conveniencia de los clientes a la que se refieren los artículo 199 y siguientes) o, en el supuesto de las autoridades competentes, en el ejercicio de potestades públicas conforme al artículo 6.1.e).

No obstante, la existencia de una base jurídica que legitime el tratamiento no exime de cumplir con el resto de principios recogidos en el artículo 5 del RGPD:

> 1. Los datos personales serán:
> a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);
> b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación

científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);
c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);
e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).
2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Por todo ello, y sin perjuicio de su aplicación directa, esta Agencia considera conveniente que en el texto del anteproyecto se introduzca un artículo en el que expresamente se señala que los tratamientos de datos de carácter personal de las personas físicas se realizarán con estricta sujeción a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y el 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 en el resto de la normativa sobre protección de datos personales.

II

El artículo 163 regula los criterios de interpretación de los requisitos de idoneidad requeridos en el Título V, relativo a las “Empresas de servicios de inversión y otras personas y entidades autorizadas para prestar servicios de inversión”

Criterios de interpretación de los requisitos de idoneidad.

1. Se considerará que concurre la honorabilidad, honestidad e integridad requerida en este título en quienes hayan venido mostrando una conducta personal, comercial y profesional que no arroje dudas sobre su capacidad para desempeñar una gestión sana y prudente de la empresa de servicios de inversión o de las empresas a que se refiere el art.124.5.a). La consideración de que concurre la honorabilidad es independiente de la inhabilitación por sanción y su cumplimiento.
Para valorar la concurrencia de honorabilidad, honestidad e integridad deberá considerarse toda la información disponible, de acuerdo con los parámetros que se determinen reglamentariamente. En todo caso, dicha información deberá incluir la relativa a la condena por la comisión de delitos o faltas y la sanción por la comisión de infracciones administrativas.

2. Se considerará que poseen los conocimientos, competencias y experiencia requeridos en este título para ejercer sus funciones en las empresas de servicios de inversión o empresas contempladas en el artículo 124.5.a) quienes cuenten con la formación de nivel y perfil adecuado, en particular, en las áreas de valores y servicios financieros, y experiencia práctica derivada de sus anteriores ocupaciones durante un tiempo suficiente. Reglamentariamente se desarrollará el contenido de estos parámetros.

3. Se tendrán en cuenta a efectos de valorar la disposición de los miembros del órgano de administración para ejercer un buen gobierno exigida en este título, la presencia de potenciales conflictos de interés que generen influencias indebidas de terceros y la capacidad de dedicar el tiempo suficiente para llevar a cabo las funciones correspondientes.

Reglamentariamente se desarrollará el concepto de tiempo suficiente a los efectos del cumplimiento de lo dispuesto en este apartado.

Tal y como ha venido señalando reiteradamente esta Agencia, las obligaciones de verificación de los requisitos de honorabilidad e idoneidad que, en determinado ámbitos, vienen impuestas por las Directivas comunitarias y son debidamente transpuestas a nuestro ordenamiento jurídico por normas con rango de ley, determinan que los correspondientes tratamientos de datos personales dirigidos a dicha verificación se pueden considerar amparados por el artículo 6.1 c) del RGPD, al aparecer la obligación legal de tratamiento recogida en el Derecho de la Unión y debidamente incorporada al derecho interno.

No obstante, esta Agencia ha venido señalando, igualmente, que no es suficiente con la concurrencia de una base jurídica para que el tratamiento sea lícito, sino que será preciso cumplir, igualmente, con el resto de principios recogidos en el artículo 5 del RGPD, interesando destacar, en este punto, el principio de limitación de la finalidad ("Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines") y de minimización ("serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados"). Asimismo, conforme a la doctrina constitucional señalada, será preciso que la ley que legitima el tratamiento de datos personales defina 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, sin que sea suficiente, a estos efectos, una genérica habilitación al desarrollo reglamentario.

Estos principios adquieren singularmente relevancia respecto del tratamiento de los datos personales correspondientes a condenas penales o sanciones administrativas, a los que se refiere el párrafo segundo del apartado 1 del artículo 163:

> Para valorar la concurrencia de honorabilidad, honestidad e integridad deberá considerarse toda la información disponible, de acuerdo con los parámetros que se determinen reglamentariamente. **En todo caso, dicha información deberá incluir la relativa a la condena por la comisión de delitos o faltas y la sanción por la comisión de infracciones administrativas.**

De este modo, la delimitación de la honorabilidad podría implicar el tratamiento de datos relacionados con la comisión de infracciones penales y administrativas.

A estos efectos, el artículo 10 del Reglamento General de Protección de Datos establece que "el tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas".

Esta norma se particulariza por el artículo 10.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales que dispone los siguiente:

1. El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal.

2. El registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas a que se refiere el artículo 10 del Reglamento (UE) 2016/679, podrá realizarse conforme con lo establecido en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

Por otro lado, respecto de los datos referidos a la comisión de infracciones administrativas, el artículo 27 de la misma ley, en correlación con lo establecido por el artículo 15.1 de la Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información y buen gobierno, establece lo siguiente:

1. A los efectos del artículo 86 del Reglamento (UE) 2016/679, el tratamiento de datos relativos a infracciones y sanciones administrativas, incluido el mantenimiento de registros relacionados con las mismas, exigirá:

a) Que los responsables de dichos tratamientos sean los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.

b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.

2. Cuando no se cumpla alguna de las condiciones previstas en el apartado anterior, los tratamientos de datos referidos a infracciones y sanciones administrativas habrán de contar con el consentimiento del interesado o estar autorizados por una norma con rango de ley, en la que se regularán, en su caso, garantías adicionales para los derechos y libertades de los afectados.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a infracciones y sanciones administrativas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

De todo lo que se acaba de indicar se desprende que el tratamiento de datos relacionados con las condenas penales o administrativas sólo resulta posible en caso de que se encuentre previsto por una norma con rango de Ley, en que se establezcan, en su caso, las garantías adicionales para la salvaguarda de los derechos de los afectados.

Debe en este punto señalarse que el derecho español no establece la posibilidad de obtención de certificados parciales de antecedentes penales salvo en los supuestos en que así lo establece expresamente, como sucede en el caso de los que obrasen en el registro de delincuentes sexuales y que hubieran de ser apartados por quienes pretendieran desarrollar actividades que impliquen contacto con menores de edad, tal y como dispone la normativa de atención jurídica del menor. Ello supone que para el conocimiento de la existencia o no de los antecedentes relevantes para la determinación de la existencia de honorabilidad a los efectos establecidos en la Ley sería precisa la recogida de datos contenidos en certificados de antecedentes penales que pueden incluir antecedentes de delitos de distinta naturaleza que no afectasen a la mencionada honorabilidad. Lo mismo sucedería en cuanto al tratamiento de las infracciones administrativas, que podrían incluir otras que tampoco hubieran de ser tomadas en consideración para la apreciación de ese requisito.

De acuerdo con lo señalado, esta Agencia, en los últimos informes emitidos en relación con los tratamientos de datos personales relativos a condenas penales y sanciones administrativas con la finalidad de verificar el cumplimiento de los requisitos de honorabilidad, viene incidiendo en la necesidad de que sea en la propia norma legal en la que se identifiquen los tipos delictivos o las infracciones administrativas que tienen que tomarse en consideración a efectos de la misma.

En este sentido nos hemos pronunciado recientemente en el Informe 8/2021, referente al Anteproyecto de Ley por la que se modifican el Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital, la Ley 26/2013, de 27 de diciembre, de cajas de ahorros y fundaciones bancarias y la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito:

.

> *En este punto, en relación con los requisitos de idoneidad y honorabilidad previstos en dichos preceptos, el criterio que tradicionalmente había venido manteniendo esta Agencia era la existencia de una habilitación legal, derivada de lo establecido en Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, y en la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito la normativa de blanqueo de capitales y de ordenación de las entidades de crédito, para el tratamiento por parte de las entidades de crédito de los*

antecedentes penales de los miembros de su consejo de administración y de sus directores generales o asimilados, y de los responsables de funciones de control interno y otros puestos clave en la entidad, tratamiento que, limitado a las personas y en los términos señalados en el Real Decreto 84/2015, sería conforme a lo previsto en la previsto en la Ley Orgánica 15/1999.

No obstante, con posterioridad a la plena aplicación del RGPD y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, esta Agencia viene insistiendo en la necesidad de que sea la propia norma legal que legitima el tratamiento la que establezca expresamente las garantías necesarias para que el mismo se estime conforme con la normativa de protección de datos de carácter personal, no siendo suficiente, a estos efectos, la mera remisión al desarrollo reglamentario.

En este sentido, si bien referido a las miembros del consejo de administración y de quienes ejerzan la dirección efectiva de las entidades gestoras de los fondos de pensiones, pero cuyos argumentos son plenamente trasladables al presente caso, en el informe 19/2020, reiterando lo que ya se había indicado en el informe 177/2018, se señalaba lo siguiente:

> *Especial referencia debe realizarse a la regulación de los requisitos de honorabilidad que se lleva a cabo en el nuevo artículo 78 bis del Reglamento de planes y fondos de pensiones, que introduce el proyecto.*
>
> *En relación con esta cuestión, en el Informe 177/2018 señalábamos lo siguiente:*
>
> *V*
>
> > *La siguiente cuestión que debe analizarse es la relativa a los requisitos de honorabilidad y aptitud de los miembros del consejo de administración y de quienes ejerzan la dirección efectiva de las entidades gestoras de los fondos de pensiones, aquellas que desempeñen funciones clave previstas en la ley y, en su caso, las personas o entidades a quienes se haya externalizado alguna de las funciones clave, a las que se refiere el artículo 28 de la Ley en la nueva redacción dada por el apartado doce del artículo 1 del Anteproyecto.*
> >
> > *Conforme a lo previsto en el Reglamento (UE) 2016/679 tal tratamiento deberá encontrarse legitimado en*

lo previsto en su artículo 6 y ser respetuoso de los principios recogidos en el artículo 5 del mismo.

Pues bien, las obligaciones de verificación de los requisitos de honorabilidad e idoneidad a las que nos hemos referido aparecen expresamente recogidas en la Directiva (UE) 2016/2341, siendo fiel trasposición de las mismas, por lo que los tratamientos descritos se pueden considerar amparados por el mencionado artículo 6.1 c), al aparecer la obligación legal de tratamiento recogida en el Derecho de la Unión y pretender el proyecto su incorporación al derecho interno.

El considerando 45 del Reglamento 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." En este sentido la Ley Orgánica de protección de datos de carácter personal y garantía de los derechos digitales, dispone en su artículo 8 respecto del tratamiento de datos amparado por la Ley lo siguiente:

"1. El tratamiento de datos de carácter personal sólo 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 de carácter personal sólo 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."

En cuanto al tratamiento de los datos por parte de la Dirección General de Seguros y Fondos de Pensiones, el mismo encuentra su fundamento además, según lo señalado anteriormente, en lo previsto en el artículo 6.1 letra e): el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Sentado lo anterior, es preciso analizar los concretos datos que puedan ser objeto de tratamiento, que deberán cumplir con los principios establecidos en el artículo 5 del RGPD.

En este punto adquiere especial relevancia lo señalado en al apartado 4 del citado artículo 28, que se remite al desarrollo reglamentario para determinar "los supuestos en los que se entiende que se cumplen los requisitos de aptitud y honorabilidad de quienes llevan la dirección efectiva o desempeñan funciones clave…".

Por consiguiente, el citado precepto, después de transcribir literalmente lo previsto en el apartado 1 del artículo 22 de la Directiva (UE) 2016/2341, definiendo el requisito de honorabilidad como "deberán ser personas íntegras y de buena reputación", remite al desarrollo reglamentario la determinación de los supuestos concretos en los que se entiende que se cumplen dichos requisitos.

No obstante, hay que tener en cuenta que la acreditación de dicha honorabilidad puede implicar el tratamiento de datos relativos a condenas penales, posibilidad expresamente contemplada en el artículo 22 de la Directiva, cuyo apartado 3 dispone que "Cuando un Estado miembro de origen exija a las personas mencionadas en el apartado 1 una prueba de honorabilidad, una prueba de que no han sido declaradas anteriormente en quiebra o ambas, ese Estado miembro aceptará como justificación suficiente para los nacionales de otros Estados miembros la presentación de un extracto del registro de antecedentes penales del otro Estado miembro o, si no existe un registro de antecedentes penales en el otro Estado miembro, de un documento equivalente, que acredite que se cumplen esas exigencias, expedido por una autoridad judicial o administrativa

competente bien del Estado miembro del que sea nacional la persona en cuestión o por el Estado miembro de origen".

Asimismo, la acreditación de la misma podría requerir acreditar la ausencia de sanciones en el ámbito administrativo.

De este modo, la delimitación de la honorabilidad podría implicar el tratamiento de datos relacionados con la comisión de infracciones penales y administrativas.

A estos efectos, el artículo 10 del Reglamento General de Protección de Datos establece que "el tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas".

Esta norma se particulariza por el artículo 10.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales que dispone los siguiente:

1. El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal.

2. El registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas a que se refiere el artículo 10 del Reglamento (UE) 2016/679, podrá realizarse conforme con lo establecido en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a

condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

Por otro lado, respecto de los datos referidos a la comisión de infracciones administrativas, el artículo 27 de la misma ley, en correlación con lo establecido por el artículo 15.1 de la Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información y buen gobierno, establece lo siguiente:

1. A los efectos del artículo 86 del Reglamento (UE) 2016/679, el tratamiento de datos relativos a infracciones y sanciones administrativas, incluido el mantenimiento de registros relacionados con las mismas, exigirá:

a) Que los responsables de dichos tratamientos sean los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.

b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.

2. Cuando no se cumpla alguna de las condiciones previstas en el apartado anterior, los tratamientos de datos referidos a infracciones y sanciones administrativas habrán de contar con el consentimiento del interesado o estar autorizados por una norma con rango de ley, en la que se regularán, en su caso, garantías adicionales para los derechos y libertades de los afectados.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a infracciones y sanciones administrativas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

De todo lo que se acaba de indicar se desprende que el tratamiento de datos relacionados con las condenas penales o administrativas sólo resulta posible en caso de que se encuentre amparada por una norma con rango de Ley, en que se establezcan, en su caso, las garantías

adicionales para la salvaguarda de los derechos de los afectados.

Debe en este punto señalarse que el derecho español no establece la posibilidad de obtención de certificados parciales de antecedentes penales salvo en los supuestos en que así lo establece expresamente, como sucede en el caso de los que obrasen en el registro de delincuentes sexuales y que hubieran de ser apartados por quienes pretendieran desarrollar actividades que impliquen contacto con menores de edad, tal y como dispone la normativa de atención jurídica del menor. Ello supone que para el conocimiento de la existencia o no de los antecedentes relevantes para la determinación de la existencia de honorabilidad a los efectos establecidos en la Ley sería precisa la recogida de datos contenidos en certificados de antecedentes penales que pueden incluir antecedentes de delitos de distinta naturaleza que no afectasen a la mencionada honorabilidad. Lo mismo sucedería en cuanto al tratamiento de las infracciones administrativas, que podrían incluir otras que tampoco hubieran de ser tomadas en consideración para la apreciación de ese requisito.

Asimismo, debe tenerse en cuenta que, esta Agencia, ha puesto reiteradamente de manifiesto que la mera previsión de un determinado tratamiento o cesión de datos por un proyecto de disposición con rango de Ley no implica por sí sola la licitud de ese tratamiento o cesión desde el punto de vista de la normativa de protección de datos por cuanto deberá respetar el contenido esencial del derecho fundamental a la protección de datos de carácter personal, tal y como impone el artículo 53.1 de la Constitución. Así lo ha puesto de relieve el Tribunal Constitucional en la Sentencia 17/2013, de 31 de enero, en cuyo fundamento jurídico 4 se señala lo siguiente:

"En conclusión, tal como establece nuestra doctrina, es claro que la LOPD no permite la comunicación indiscriminada de datos personales entre Administraciones Públicas dado que, además, estos datos están, en principio, afectos a finalidades concretas y predeterminadas que son las que motivaron su recogida y tratamiento. Por tanto, la cesión de datos entre Administraciones Públicas sin consentimiento del afectado, cuando se cedan para el ejercicio de competencias

distintas o que versen sobre materias distintas de aquellas que motivaron su recogida, únicamente será posible, fuera de los supuestos expresamente previstos por la propia LOPD, si existe previsión legal expresa para ello [art. 11.2.a) en relación con el 6.1 LOPD] ya que, a tenor de lo dispuesto en el art. 53.1 CE, los límites al derecho a consentir la cesión de los datos a fines distintos para los que fueron recabados están sometidos a reserva de ley. Reserva legal que, como es obvio, habrá de cumplir con los restantes requisitos derivados de nuestra doctrina- esencialmente, basarse en bienes de dimensión constitucional y respetar las exigencias del principio de proporcionalidad- para poder considerar conforme con la Constitución la circunstancia de que la norma legal en cuestión no contemple, por tanto, la necesidad de contar con el consentimiento del afectado para autorizar la cesión de datos."

En particular, será preciso que el tratamiento y comunicación de los datos resulten conformes con el principio de limitación de la finalidad ("Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines") y de minimización ("serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados") recogidos en el artículo 5 del RGPD.

En el presente caso, en cuanto a la información sobre antecedentes penales existe una norma de derecho de la Unión que habilita el tratamiento de "un extracto del registro de antecedentes penales".

De este modo, el derecho de la Unión establece una habilitación para el tratamiento de los datos relacionados con los antecedentes penales cuando los Estados Miembros exijan prueba de la honorabilidad, pero sin concretar los delitos que pueden tener incidencia en dicha honorabilidad.

A diferencia de lo referido a las infracciones penales, y lo previsto para el caso de quiebras (en el caso español, referido a la declaración de concurso e inhabilitación conforme a la Ley Concursal) la Directiva no incorpora referencia alguna a la comisión de infracciones administrativas para valorar la concurrencia de honorabilidad empresarial.

Esta Agencia Española de Protección de Datos ha tenido la oportunidad de analizar la cuestión a la que ahora se está haciendo referencia, incluso dentro del ámbito del sector asegurador que también resulta afectado por la norma objeto de informe, al informar diversos proyectos de disposiciones en las que se establecía la información necesaria para delimitar la concurrencia de honorabilidad. Así, cabe hacer referencia a los informes emitidos al Anteproyecto de Ley de distribución de seguros y reaseguros privados de 5 de diciembre de 2017, al Anteproyecto de Ley de Ordenación, Supervisión y Solvencia de las entidades aseguradoras y reaseguradoras, de fecha 13 de febrero de 2015, a su Reglamento de desarrollo, emitido en fecha 19 de noviembre de 2015 y al Proyecto de Orden por la que se aprueba la lista de información a remitir en supuestos de adquisición o incremento de participaciones significativas en entidades aseguradoras y reaseguradoras y por quienes pretendan desempeñar cargos de dirección efectiva o funciones que integran el sistema de gobierno en entidades aseguradoras, reaseguradoras y en los grupos de entidades aseguradoras y reaseguradoras, de fecha 16 de febrero de 2016.

En el informe de 13 de febrero de 2015 se valoraba la procedencia y conformidad con los principios de finalidad y proporcionalidad del tratamiento de estos datos, señalando lo siguiente:

"Obviamente, la concurrencia de los requisitos adecuados de idoneidad y honorabilidad en los directivos y consejeros de las entidades aseguradoras resulta esencial para garantizar su adecuado funcionamiento y evitar los posibles riesgos que de su actividad, en caso de no reunirse los requisitos, pudieran derivarse en la actividad económica. Sin embargo, la legitimidad de este fin no puede fundamentar por sí sola la recolección de información "disponible" que exceda de la que resulte adecuada, pertinente y no excesiva en relación con el objetivo perseguido, teniendo en cuenta no sólo la normativa sectorial, sino el conjunto del ordenamiento jurídico.

De este modo, como se ha comprobado, la "información disponible" referida a condenas penales

debería quedar limitada a la derivada de los antecedentes penales en vigor y, particularmente, de la situación de inhabilitación del candidato al puesto directivo o de administración. Del mismo modo, en cuanto a las infracciones administrativas, sería preciso el establecimiento de límites similares, tanto en lo referente a la normativa a la que debe referirse la infracción, no acumulándose datos irrelevantes o que no guarden en ninguna medida relación con el puesto que se pretende desempeñar ni aquéllos respecto de los que el tiempo transcurrido determine su irrelevancia para la toma de decisiones."

De lo que acaba de transcribirse, trasladado al supuesto ahora estudiado, se desprende que, efectivamente, el conocimiento del requisito de honorabilidad por parte de quienes intervienen en la actividad de gestión de los fondos de pensiones constituye una finalidad legítima que garantiza el adecuado funcionamiento y transparencia en el mercado de planes de pensiones.

No obstante, con el fin de habilitar el tratamiento de los datos relativos a las condenas penales y a las infracciones administrativas, se considera necesario que así se establezca expresamente en el Anteproyecto de ley, delimitándose, conforme al principio de minimización, los supuestos concretos de infracciones penales y administrativas que se consideran relevantes a efectos de valorar la honorabilidad.

En todo caso, el tratamiento de los datos, tanto relativos a la comisión de infracciones penales como de ilícitos administrativos únicamente debería llevarse a cabo con la finalidad de evaluar la honorabilidad exigida por los preceptos del Anteproyecto a los que se ha hecho exhaustiva referencia en un lugar anterior de este informe y para su comunicación a la Dirección General de Seguros y Fondos de Pensiones.

A título de ejemplo, entre las normas más recientemente informadas por esta Agencia, puede citarse el Anteproyecto de Ley de distribución de seguros y reaseguros privados, cuyo artículo 2.19 definía la «Honorabilidad comercial y profesional» como la "cualidad aplicable a aquellas personas que hayan venido observando una trayectoria personal de respeto a las leyes

mercantiles u otras que regulen la actividad económica y la vida de los negocios, así como a las buenas prácticas comerciales, financieras y de seguros. Dicha condición será aplicable a aquellas personas que no tengan antecedentes penales por haber cometido infracciones penales relativas al ejercicio de actividades financieras, y que no hayan sido sancionadas en el ámbito administrativo en materia aseguradora, bancaria, de mercado de valores, Hacienda Pública, Seguridad Social, defensa de la competencia, movimiento de capitales, transacciones económicas con el exterior, blanqueo de capitales y financiación del terrorismo y protección de consumidores y usuarios por la comisión de infracciones tipificadas como muy graves o graves. La inhabilitación para el ejercicio de cargos públicos o de administración y dirección de entidades financieras, así como la declarada conforme a la Ley 22/2003, de 9 de julio, Concursal, mientras no haya concluido el periodo de inhabilitación fijado, o el estado de quebrado o concursado no rehabilitado en el caso de procedimientos concursales anteriores a la entrada en vigor de la referida ley, se considerarán circunstancias que no permiten cumplir el requisito de honorabilidad".

VI

A los efectos anteriores, y para recalcar la insuficiencia de la remisión a la normativa reglamentaria para determinar los supuestos en los que se entiende que se cumplen los requisitos de honorabilidad, procede traer a colación la doctrina sentada por el Tribunal Constitucional en su reciente sentencia de 22 de mayo de 2019, en la que se comienza realizando una síntesis de la doctrina recogida en otras sentencias anteriores:

"6. A la vista de los potenciales efectos intrusivos en el derecho fundamental afectado que resultan del tratamiento de datos personales, la jurisprudencia de este Tribunal le exige al legislador que, además de cumplir los requisitos anteriormente mencionados, también establezca 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. En este fundamento jurídico precisaremos la naturaleza y el alcance de este específico requisito constitucional.

a) La necesidad de establecer las garantías adecuadas para procurar el respeto del contenido esencial del derecho fundamental a la protección de datos personales fue señalada específicamente en el FJ 10 de la STC 292/2000, que ha sido correctamente invocado por el Defensor del Pueblo. Del mencionado fundamento jurídico se extraen las siguientes conclusiones:

- La previsión legal y la legitimidad del fin perseguido son requisitos necesarios pero no suficientes para fundamentar la validez constitucional de una regulación del tratamiento de datos personales, pues para ello se requieren también "garantías adecuadas frente al uso potencialmente invasor de la vida privada del ciudadano a través de su tratamiento informático".

- Esas garantías son necesarias "para el reconocimiento e identidad constitucionales del derecho fundamental a la protección de datos" y "para que los intereses jurídicamente protegibles, que constituyen la razón de ser del aludido derecho fundamental, resulten real, concreta y efectivamente protegidos".

- La mera inexistencia de "garantías adecuadas" o de las "mínimas exigibles a la Ley" constituye de por sí una injerencia en el derecho fundamental, de gravedad similar a la que causarían intromisiones directas en su contenido nuclear.

- La exigencia de "garantías adecuadas" se fundamenta, por tanto, en el respeto del contenido esencial del derecho fundamental.

Asimismo, del examen conjunto de los FFJJ 7 y 10 de la STC 292/2000 se deduce que las "garantías adecuadas" o "garantías mínimas exigibles a una Ley sometida al insoslayable respeto al contenido esencial del derecho fundamental cuyo ejercicio regula" deben diferenciarse también del "haz de facultades que componen el contenido del derecho fundamental a la protección de datos de carácter personal", que, como se indicó antes, son aquellas que otorgan al titular del derecho fundamental "un poder de disposición y de control sobre los datos personales".

b) Esta doctrina sobre las garantías adecuadas es también la que sigue la jurisprudencia del Tribunal de Justicia de la Unión Europea. En la Sentencia de la Gran Sala de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland Ltd, apartado 54, el Tribunal de Justicia señaló lo siguiente: "la normativa de la Unión de que se trate debe establecer reglas claras y

precisas que regulen el alcance y la aplicación de la medida en cuestión y establezcan unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos respecto de tales datos (véanse, por analogía, en lo que respecta al artículo 8 del CEDH, las sentencias TEDH, Liberty y otros c. Reino Unido de 1 de julio de 2008, nº 58243/00, §§ 62 y 63; Rotaru c. Rumanía, antes citada, §§ 57 a 59, y S y Marper c. Reino Unido, antes citada, §§ 99).”

En la citada sentencia, la constatación de la carencia de, por un lado, reglas claras y precisas que regulasen el alcance de la injerencia en los derechos fundamentales reconocidos en los arts. 7 y 8 de la Carta de Derechos Fundamentales y de, por otro lado, garantías suficientes que permitieran una protección eficaz de los datos conservados fundamentó la declaración de invalidez de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

c) La necesidad de disponer de garantías adecuadas es especialmente importante cuando el tratamiento afecta a categorías especiales de datos, también llamados datos sensibles, pues el uso de estos últimos es susceptible de comprometer más directamente la dignidad, la libertad y el libre desarrollo de la personalidad.”

Para añadir, resolviendo la cuestión objeto de debate, que:

“Por tanto, la resolución de la presente impugnación exige que aclaremos una duda suscitada con respecto al alcance de nuestra doctrina sobre las garantías adecuadas, que consiste en determinar si las garantías adecuadas frente al uso de la informática deben contenerse en la propia ley que autoriza y regula ese uso o pueden encontrarse también en otras fuentes normativas.

La cuestión solo puede tener una respuesta constitucional. 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 art. 53.1 CE para el legislador de los derechos fundamentales: la reserva de ley para la regulación del ejercicio de los derechos fundamentales reconocidos en el capítulo segundo del título primero de la Constitución y el respeto del contenido esencial de dichos derechos fundamentales".

Por consiguiente, correspondiendo a los Estados Miembros definir los supuestos en los que se entiende que se cumplen los requisitos de honorabilidad, en la medida en que afectan al derecho fundamental a la protección de datos y conforme a la doctrina constitucional citada, dicha definición deberá contenerse en el propio Anteproyecto al menos en sus elementos esenciales".

Dicha observación fue recogida en la modificación realizada por el Real Decreto Ley 3/2020, en la que ya se identificaron, al regular la información a facilitar en el caso de personas no residentes en España, concretos tipos delictivos, procediendo el nuevo artículo 78 bis a regular más detalladamente los supuestos en los que se entiende que se cumplen los requisitos de honorabilidad, identificando las conductas y tipos delictivos que deben ser objeto de valoración, dando cumplimiento, de este modo, al principio de minimización de datos. Asimismo, y de acuerdo con el principio de limitación de la finalidad, se señala expresamente que "El tratamiento de los datos que las entidades lleven a cabo en el marco de lo dispuesto en este precepto deberá limitarse a la exclusiva finalidad de suministro de la información a la Dirección General de Seguros y Fondos de Pensiones, quedando expresamente limitado el número de personas de la entidad que dentro de su organización pueda tener acceso a dichos datos".

Por consiguiente, aun cuando no es propiamente objeto de modificación en virtud de la transposición directa de la Directiva, teniendo en cuenta que la apreciación del cumplimiento de los requisitos de idoneidad y honorabilidad puede implicar el tratamiento de datos relativos a condenas penales y sanciones administrativas, y al objeto de adecuar la regulación contenida en la Ley 10/2014 a los requisitos normativos y jurisprudenciales señalados, esta Agencia considera necesario que se

modifique el artículo 24 de la Ley 10/2014, de manera que se recoja, de manera expresa, el tratamiento de dichos datos, precisando, asimismo, las conductas y tipos delictivos que deben ser objeto de valoración y el uso de los mismos, de acuerdo con los principios de minimización y limitación de la finalidad, incorporando en el texto legal las previsiones contenidas en el artículo 30.2.b) del Real Decreto 84/2015, de 13 de febrero, por el que se desarrolla la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito. De este modo, dichos tratamientos se encontrarían amparados por lo previsto en la letra c) del artículo 6.1. del RGPD (el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento), de acuerdo con lo previsto en el artículo 10 del RGPD y en los artículos 10 y 27 de la LOPDGDD.

En virtud de lo expuesto, esta Agencia considera que debería modificarse el segundo párrafo del apartado 1 del artículo 163, con el objeto de incluir en el mismo, respecto de la información relativa a la condena por la comisión de delitos o faltas y la sanción por la comisión de infracciones administrativas que deben valorarse para la apreciación del cumplimiento de los requisitos de idoneidad y honorabilidad, la identificación de las conductas y tipos delictivos que deben ser objeto de valoración y el uso de los mismos, de acuerdo con los principios de minimización y limitación de la finalidad, trasladando a dicho artículo el contenido que para su aplicación, se establece actualmente a nivel reglamentario.

III

El artículo 173 recoge la regulación de los registros que actualmente se contiene en el artículo 194 del texto refundido de la Ley del Mercado de Valores.

A la importancia de armonizar la normativa de registros hace referencia el Considerando 57 de la Directiva 2014/65/UE:

"La Directiva 2006/73/CE de la Comisión (1) permite que los Estados miembros exijan, en el contexto de los requisitos organizativos que deben cumplir las empresas de servicios de inversión, el registro de conversaciones telefónicas o de comunicaciones electrónicas ligadas a órdenes de clientes. El registro de conversaciones telefónicas o de comunicaciones electrónicas ligadas a órdenes de clientes es compatible con la Carta de los Derechos Fundamentales de la Unión Europea (la Carta) y se justifica por la necesidad de reforzar la protección del inversor, mejorar la vigilancia del mercado y aumentar la seguridad jurídica en beneficio de las empresas de servicios de inversión y sus clientes. La recomendación técnica a la Comisión, emitida por el Comité de Responsables Europeos de Reglamentación de Valores el 29 de julio de 2010, resalta también la importancia de dichos registros. Estos registros deben garantizar que haya pruebas que permitan demostrar las condiciones de las órdenes dadas por los clientes y su correspondencia con las operaciones realizadas por las empresas de servicios de inversión, así como detectar cualquier conducta que pueda ser relevante en materia de abuso de mercado, en particular cuando las empresas negocian por cuenta propia.

A tal fin, es necesario conservar registros de todas las conversaciones en las que participen representantes de la empresa cuando negocien o se propongan negociar por cuenta propia. Cuando los clientes comuniquen sus órdenes por otros canales distintos al teléfono, tales comunicaciones deben hacerse en un soporte duradero, como correo postal, fax, correo electrónico, o documentación de órdenes de clientes formuladas en reuniones. Por ejemplo, el contenido de conversaciones pertinentes directas con un cliente podría registrarse por escrito en actas o notas. Esas órdenes deben considerarse equivalentes a las recibidas por teléfono. Cuando se levanten actas de conversaciones directas con clientes, los Estados miembros deben asegurar que existen las salvaguardias adecuadas, a fin de garantizar que el cliente no se vea perjudicado debido a que el acta no reproduce con exactitud la comunicación entre las partes. Dichas salvaguardias no implicarán la asunción de responsabilidad por parte del cliente.

Para garantizar la seguridad jurídica en lo que se refiere al alcance de esta obligación, es conveniente, por una parte, que la obligación se aplique a todo material facilitado por la empresa de servicios de inversión o cuya utilización esta permita, y, por otra, exigir a las empresas de servicios de inversión que tomen medidas razonables para garantizar que no se utilice material privado en relación con las operaciones de la empresa. Los mencionados registros deben estar a disposición de las autoridades competentes cuando desempeñen sus funciones de supervisión o apliquen medidas ejecutivas de conformidad con la presente Directiva y con el Reglamento (UE) n o 600/2014, el Reglamento (UE) n o 596/2014 y la Directiva 2014/57/UE del Parlamento Europeo y del Consejo (1), con el fin de que puedan identificar toda conducta que no se ajuste al marco jurídico por el que se rigen las actividades de las empresas de servicios de inversión. También deben estar a disposición de las empresas de servicios de inversión y los clientes, para demostrar el desarrollo de su relación en lo que atañe a las órdenes dadas por los clientes y las operaciones realizadas por las empresas. Por tales razones, es conveniente consignar en la presente Directiva los principios de un régimen general relativo al registro de conversaciones telefónicas o comunicaciones electrónicas ligadas a órdenes de clientes".

Y el Considerando 144 añade los siguiente:

"Los registros telefónicos y de tráfico de datos procedentes de empresas de servicios de inversión en los que se ejecutan y documentan las operaciones, así como los registros telefónicos y de tráfico de datos procedentes de empresas de telecomunicaciones, constituyen una prueba crucial, a veces la única, para detectar y demostrar la existencia de prácticas de abuso de mercado, así como para comprobar si las empresas cumplen su obligación de proteger a los inversores y otros requisitos establecidos en la presente Directiva o en el Reglamento (UE) n o 600/2014. Por tanto, las autoridades competentes deben poder exigir los registros de conversaciones telefónicas, de comunicaciones electrónicas o de tráfico de datos mantenidos por una empresa de servicios de inversión o una entidad de crédito. El acceso a los registros telefónicos es necesario para poder detectar y sancionar las prácticas de abuso de mercado o el incumplimiento de los requisitos establecidos en la presente Directiva o en el Reglamento (UE) n o 600/2014.

Para introducir unas condiciones equitativas en la Unión en relación con el acceso a registros telefónicos y de tráfico de datos mantenidos por empresas de telecomunicaciones o a registros telefónicos y de tráfico de datos mantenidos por una empresa de servicios de inversión, las autoridades competentes deben poder exigir, de conformidad con el Derecho nacional, los registros existentes sobre el tráfico de datos mantenidos por una empresa de telecomunicaciones en la medida en que lo permita el Derecho nacional y los registros existentes sobre conversaciones telefónicas y tráfico de datos mantenidos por una empresa de servicios de inversión, cuando exista una sospecha razonable de que dichos registros, relacionados con el objeto de la inspección o la investigación, puedan ser pertinentes para demostrar conductas que están prohibidas por el Reglamento (UE) n o 596/2014 o los requisitos establecidos en la presente Directiva o en el Reglamento (UE) n o 600/2014. El acceso a los registros telefónicos y de tráfico de datos que mantiene una empresa de telecomunicaciones no debe incluir el contenido de las comunicaciones telefónicas vocales".

Partiendo de lo anterior, el artículo 16 de la Directiva legitima dichos registros al disponer lo siguiente:

> "6. Toda empresa de servicios de inversión llevará un registro de todos los servicios, actividades y operaciones que realice. Dicho registro deberá ser suficiente para permitir que la autoridad competente desempeñe sus funciones de supervisión y aplique las medidas ejecutivas oportunas al amparo de la presente Directiva, del Reglamento (UE) n o 600/2014, de la Directiva 2014/57/UE y del Reglamento (UE) n o 596/2014, y en particular para que pueda determinar si la empresa de servicios de inversión ha cumplido todas sus obligaciones, incluidas las relativas a sus clientes o posibles clientes y a la integridad del mercado.
>
> 7. El registro incluirá las grabaciones de las conversaciones telefónicas o comunicaciones electrónicas relativas, al menos, a las operaciones realizadas cuando se negocia por cuenta propia y la prestación de servicios que estén relacionados con la recepción, transmisión y ejecución de órdenes de clientes.
>
> Entre tales conversaciones telefónicas y comunicaciones electrónicas figurarán también aquellas cuya intención sea dar lugar a operaciones realizadas en el marco de una negociación por cuenta propia o en la prestación de servicios que estén relacionados con la recepción, transmisión y ejecución de órdenes de clientes, incluso si esas conversaciones o comunicaciones no den lugar a la realización de tales operaciones o a la prestación de tales servicios.

A tal fin, la empresa de servicios de inversión tomará todas las medidas razonables para grabar las conversaciones telefónicas y comunicaciones electrónicas pertinentes realizadas, enviadas o recibidas a través de material facilitado por la propia empresa a un empleado o una persona contratada o cuya utilización por estos haya aceptado o autorizado la empresa de servicios de inversión.

Las empresas de servicios de inversión notificarán a sus clientes nuevos y actuales que se grabarán las comunicaciones o conversaciones telefónicas entre ellas y sus clientes a resultas de las cuales se realicen o puedan realizarse operaciones.

Dicha notificación podrá realizarse una sola vez, antes de la prestación de servicios de inversión a clientes nuevos y actuales.

Las empresas de servicios de inversión no prestarán por teléfono servicios ni ejercerán actividades de inversión con aquellos clientes a los que no hayan notificado por adelantado la grabación de sus comunicaciones o conversaciones telefónicas en caso de que dichos servicios y actividades estén relacionadas con la recepción, transmisión y ejecución de órdenes de clientes.

Los clientes podrán comunicar sus órdenes por otros canales, si bien tales comunicaciones deberán hacerse en un soporte duradero, como correo postal, fax, correo electrónico, o documentación de órdenes de clientes formuladas en reuniones. En particular, el contenido de conversaciones pertinentes cara a cara con un cliente podrá registrarse por escrito en actas o notas. Esas órdenes se considerarán equivalentes a las recibidas por teléfono.

La empresa de servicios de inversión tomará todas las medidas razonables para impedir que un empleado o una persona contratada realice, envíe o reciba llamadas telefónicas o comunicaciones electrónicas en materia de su propiedad que la empresa no pueda registrar o copiar.

Los registros conservados con arreglo a lo dispuesto en este apartado se pondrán a disposición de los clientes si así lo solicitan, y se conservará durante un período de cinco años y, cuando la autoridad competente así lo solicite, durante un período de hasta siete años".

Por lo tanto, dicho registro encuentra igualmente en el artículo 6.1.c) del Reglamento general de protección de datos su base jurídica, al tratarse de una obligación impuesta por el Derecho comunitario que ha sido debidamente incorporada al derecho interno.

Además, la propia norma establece determinadas garantías que son conformes con el Reglamento general de protección de datos, como la obligación de informar sobre la grabación (información que deberá completarse en todo caso con los previsto en el artículo 13 del RGPD) o la de conservar los datos no más tiempo del necesario para los fines del tratamiento.

Por consiguiente, se considera que la regulación contenida en el citado precepto, sin perjuicio de su posterior desarrollo reglamentario, es conforme con la normativa sobre protección de datos personales.

IV

Procede analizar, a continuación, el régimen jurídico aplicable a los tratamientos de datos personales que pueda realizar la CNMV en el ejercicio de sus facultades de supervisión e inspección.

En relación con las bases jurídicas contenidas en el artículo 6 del RGPD y a las que nos referíamos al principio del presente informe, y en cuanto al tratamiento de datos por parte de las Administraciones Públicas, es criterio reiterado de esta Agencia que el fundamento del mismo debe encontrarse en las letras c) y e) del artículo 6.1 del RGPD. En este sentido, en el informe 175/2018 ya se señalaba lo siguiente:

> *"Como CONCLUSIÓN en este punto, cabe decir que, con carácter general, la base jurídica del tratamiento en las relaciones con la Administración, en aquellos supuestos en que existe una relación en la que no puede razonablemente predicarse que exista una situación de equilibrio entre el responsable del tratamiento (la Administración), y el interesado (el administrado) no sería el consentimiento (art. 6.1.a) RGPD), sino, según los casos, el cumplimiento de una obligación legal (art. 6.1.c) RGPD) o el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos (art. 6.1.e) RGPD).*
>
> *Por otro lado, respecto de los tratamientos de datos personales realizados al amparo de las letras c) y e) del artículo 6.1 del RGPD, es preciso realizar las siguientes matizaciones:*
>
> *En primer lugar, que tal y como prevén los apartados 2 y 3 del artículo 6 del RGPD, las normas jurídicas que habiliten dichos tratamientos podrán establecer disposiciones específicas en relación con los mismos:*
>
> *"2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.*
>
> *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".

En segundo lugar, y tal y como se indicaba en el ya citado informe 175/2018: "En cuanto al sentido de la expresión "obligación legal" contenida en el artículo 6.1.c) RGPD, dicha expresión equivale, en la regulación española de protección de datos, a "obligación establecida en una norma con rango de ley". El art. 53.1 de la Constitución (CE) establece que [l]os derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos. Sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, que se tutelarán de acuerdo con lo previsto en el artículo 161.1.a). El derecho fundamental a la protección de datos personales se contiene en el art. 18.4 CE, y por tanto le es aplicable la necesidad de una ley para limitar el mismo".

Por otro lado, conforme a lo razonado en nuestro Informe 74/2019, debe concluirse que la licitud de los tratamientos de datos de carácter personal *"encontrará su fundamento en la base jurídica del artículo 6.1.c) del RGPD (el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento) únicamente en aquellos casos en los que una norma con rango de ley imponga a la Administración una obligación específica de dar, hacer o no hacer, que implique el tratamiento de datos de carácter personal, y diferente del deber jurídico genérico de la Administración de ejercer las potestades que el ordenamiento jurídico le atribuye para servir con objetividad al interés público".*

Asimismo, y en cuanto a la base de la letra e) del artículo 6 del RGPD, el citado informe señalaba que *"la Administración está vinculada por el principio de legalidad, de manera que, a diferencia de los particulares, tan sólo puede llevar a cabo aquello para lo que el ordenamiento jurídico le permite expresamente. Este es el sentido de lo dispuesto en los artículos 9.1 y 103 de la Constitución, de suerte que cuando la ley y el derecho no han atribuido a la Administración las potestades correspondientes para actuar ante una determinada situación, esa actuación no podrá llevarse a cabo sin que previamente el ordenamiento le atribuya dichas potestades. No existe por tanto un espacio vacío donde a falta de ley pueda la Administración actuar. Es lo que se ha denominado la doctrina de la vinculación positiva de la Administración a la legalidad (García de Enterría). En consecuencia, para que la Administración pueda actuar necesita de una previa habilitación legal (entendida aquí legalidad como habilitación normativa). Y ello tanto si la Administración actúa en el ámbito del derecho público como el ámbito del derecho privado"*. Por lo tanto, en este caso, será igualmente necesario que dicha habilitación legal se contenga en una norma con rango de ley, por exigirlo el citado artículo 53 de la Constitución.

En este sentido se recoge en el artículo 8 de la LOPDGDD, que lleva por rúbrica "Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos":

> 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.

No obstante, no todo tratamiento que lleve a cabo una Administración pública podrá legitimarse en el artículo 6.1.e) del RGPD, sino que solo lo será en la medida en que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, tal y como señalaba el informe 175/2018:

"En cuanto a la extensión de la expresión del art. 6.1.e) RGPD como base jurídica del tratamiento de datos personales, la consulta inquiere si "todo tratamiento de datos personales por una Administración pública estaría en todo caso amparado por la letra e)", la respuesta ha de ser negativa, pero no en el sentido que propugna la pregunta sino en un sentido más general puesto que el art. 6.1.e) RGPD tan sólo considera lícito un tratamiento de datos personales sobre la base de dicho precepto si el mismo es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Por ello, si un determinado tratamiento no es "necesario" para el cumplimiento de la misión realizada en interés público o en el ejercicio de los poderes públicos conferidos por el ordenamiento, dicho tratamiento no sólo carecería de base jurídica suficiente legitimadora prevista en el apartado e), sino que, además, infringiría el principio de minimización de datos contenido en el artículo 5.1.c) RGPD, aplicable igualmente a los tratamientos de datos llevados a cabo por la Administración pública.

CONCLUSIÓN: los tratamientos de datos que lleve a cabo la Administración están sujetos a los principios establecidos en el RGPD, y entre ellos, el principio de minimización (art. 5.1.c) RGPD), por lo que sólo están amparados los tratamientos de datos personales que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que dichos datos son tratados".

Por lo tanto, los tratamientos de datos de carácter personal que se lleven a cabo por las Administraciones públicas encontrarán su legitimación, con carácter general, en las letras c) y e) del artículo 6.1 del RGPD y quedan sujetos al principio de minimización de datos establecido en el artículo 5.1.c) del mismo, pudiendo establecerse por la normativa nacional que tenga rango de ley especificaciones respecto de dichos tratamientos conforme a los apartados 6.2 y 6.3 del RGPD.

Asimismo, mediante norma con rango de ley podrán establecerse las limitaciones a las que se refiere el artículo 23 del RGPD:

Artículo 23 Limitaciones

1.El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;

e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;

f) la protección de la independencia judicial y de los procedimientos judiciales; g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;

h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);

i) la protección del interesado o de los derechos y libertades de otros;

j) la ejecución de demandas civiles.

2.En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a:

a) la finalidad del tratamiento o de las categorías de tratamiento;

b) las categorías de datos personales de que se trate; c) el alcance de las limitaciones establecidas;

d) las garantías para evitar accesos o transferencias ilícitos o abusivos;

e) la determinación del responsable o de categorías de responsables;

f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento;

g) los riesgos para los derechos y libertades de los interesados, y

h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.

Dicha norma legal, en la medida en que establezca especificaciones o limitaciones respecto del tratamiento de datos personales por las Administraciones públicas y siempre que sean conformes con el RGPD, que goza de efecto directo y ha desplazado la normativa nacional que se oponga al mismo, podrá tener la consideración de ley especial.

Así lo ha venido considerando esta Agencia en relación, por ejemplo, con el tratamiento de los datos tributarios (Informes 131/2013, 423/2013 y 430/2014, entre otros) considerando que el carácter reservado de los datos tributarios implica que los mismos solo pueden ser cedidos en los términos previstos en su normativa específica, actuando según lo dicho la Ley General Tributaria como ley especial, que legitima el tratamiento y al mismo tiempo fija en su artículo 95 “las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación”, previsión expresamente contemplada en el artículo 6.3 del RGPD. En este sentido, la disposición adicional decimoséptima de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público señala que “el acceso, la cesión o la comunicación de información de naturaleza tributaria se regirán en todo caso por su legislación específica”.

También se establecen normas específicas respecto al tratamiento de datos personales en otras leyes sectoriales, como ocurre en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, cuyo artículo 32.3 excluye de su ámbito el cumplimiento del deber de información así como el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, estableciendo que “En caso de ejercicio de los citados derechos por el interesado, los sujetos obligados se limitarán a ponerle de manifiesto lo dispuesto en este artículo”; o en el artículo 59 de la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, que regula la Central de Información de Riesgos del Banco de España, cuyo apartado 3 señala que “No habrá lugar al derecho de oposición de los afectados al tratamiento, realizado conforme a lo previsto en la presente Ley, de sus datos de carácter personal”; en el artículo 16.11 de la Ley 23/2015, de 21 de julio, Ordenadora del Sistema de Inspección de Trabajo y Seguridad Social, según el cual “la obtención de datos de carácter personal no recabados del interesado por los funcionarios de la Inspección en el ejercicio de sus competencias, no requerirá la información expresa e inequívoca a los interesados prevista en el artículo 5.4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal”.

Partiendo de lo anterior, debe analizarse el contenido del artículo 234 del anteproyecto de ley, similar al vigente artículo 234.12 del texto refundido de la Ley del Mercado de Valores:

> Artículo 234. Recogida y tratamiento de datos de carácter personal.
> 1. El acceso, tratamiento y cesión de los datos personales recabados por la CNMV en el ejercicio de sus funciones de inspección y supervisión se encuentra amparado por la normativa de protección de datos de carácter personal. Los datos únicamente se emplearán para el ejercicio de las mencionadas potestades en los términos previstos en esta ley.

> 2. Los derechos de los interesados regulados en la normativa de protección de datos de carácter personal quedarán limitados, de acuerdo con lo dispuesto en dicha normativa, durante el tiempo que la CNMV considere necesario para salvaguardar el buen fin de sus actuaciones inspectoras y supervisoras.

En cuanto al tratamiento de los datos por parte de la Comisión Nacional del Mercado de Valores, el mismo encuentra su fundamento, con carácter general, en lo previsto en el artículo 6.1 letra e): el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Asimismo, encontrará su fundamento en el artículo 6.1.c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, en lo supuestos en los que la ley impone obligaciones específicas como las resultantes del deber de colaboración regulado en el artículo 241 del anteproyecto, del acceso a los registros telefónicos y de tráfico de datos del artículo 233. 3 d) del anteproyecto.

Por consiguiente, se considera conveniente que se modifique el apartado 1 del artículo 234 para incluir la referencia expresa a los apartados c) y e) del artículo 6.1. del RGPD.

Por otro lado, el apartado 2 recoge la limitación de los derechos de los interesados en términos genéricos, estableciéndose con carácter general respecto de todos los derechos regulados en la normativa de protección de datos y durante el tiempo que la CNMV considere necesario para salvaguardar el buen fin de sus actuaciones inspectoras y supervisoras, señalando expresamente que quedarán limitados *“de acuerdo con lo dispuesto en dicha normativa”.*

A este respecto, debe señalarse que el RGPD no limita directamente los derechos de los afectados, sino que admite, excepcionalmente y en los supuestos tasados en el artículo 23, que pueda procederse a su limitación por el Derecho de la Unión o de los Estados miembros, lo que requerirá en el caso de norma nacional que tenga rango de ley y que cumpla con los requisitos del apartado 2 del citado artículo 23:

> 2.En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a:
> a) la finalidad del tratamiento o de las categorías de tratamiento;
> b) las categorías de datos personales de que se trate;
> c) el alcance de las limitaciones establecidas;
> d) las garantías para evitar accesos o transferencias ilícitos o abusivos;
> e) la determinación del responsable o de categorías de responsables;

> f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento;
> g) los riesgos para los derechos y libertades de los interesados, y
> h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.

En el texto remitido y a lo largo de su articulado, se recogen determinadas garantías que adquieren especial relevancia desde la perspectiva de protección de datos personales, como las correspondientes a la obligación de secreto profesional del artículo 250, las garantías de confidencialidad del artículo 273 o la adopción de medidas que garanticen la seguridad y confidencialidad de las comunicaciones a las que se refiere el artículo 275, a las que habría que añadir las garantías de conocimiento e intervención que resultan de la aplicación de la normativa reguladora del correspondiente procedimiento administrativo, que de este modo tiene la consideración de ley especial al amparo de lo señalado en el artículo 12.5 de la LOPDGDD:

> 5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquellas.

A este respecto, el artículo 266 del anteproyecto señala lo siguiente:

> Artículo 266. Legislación aplicable al procedimiento sancionador.
>
> 1. En materia de procedimiento sancionador, resultará de aplicación la Ley 39/2015, de 1 de octubre y la Ley 40/2015, de 1 de octubre y su desarrollo reglamentario, con las especialidades recogidas en los artículos 108, 110 y 112 de la Ley 10/2014, de 26 de junio, así como lo dispuesto en esta ley y su desarrollo reglamentario.
> 2. Igualmente, en el ejercicio de la potestad sancionadora atribuida a la CNMV, será aplicable a las entidades comprendidas en el artículo 228 [ámbito de la supervisión, inspección y sanción].a) lo dispuesto en el artículo 106 de la Ley 10/2014, de 26 de junio.

Por consiguiente, se considera que, si bien se establecen determinadas garantías dirigidas a proteger el derecho fundamental, para el adecuado cumplimiento del artículo 23.2. del RGPD se debería precisar más respecto de

las limitaciones que el precepto prevé, en función de los concretos derechos afectados.

A este respecto, en el Informe 74/2019, analizando los procedimientos que se tramitaban por la Dirección de Competencia de la CNMC y de acuerdo con su normativa específica, se alcanzaban las siguientes conclusiones que resultarían igualmente aplicables a los procedimientos tramitados por la CNMV:

> *"Comenzando con el derecho de acceso regulado en el artículo 15 del RGPD el mismo se define como el derecho del interesado a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la información que el precepto detalla, incluyendo como novedad el RGPD la obligación del responsable del tratamiento de facilitar una copia de los datos personales objeto de tratamiento. En el presente caso, tratándose de la tramitación de procedimientos administrativos, y conforme a lo previsto en el citado artículo 12.5. de la LOPDGDD, deberá atenderse a la normativa común de procedimiento administrativo que desarrolla, con trámites específicos, el derecho de los interesados en un procedimiento administrativo a conocer, en cualquier momento, el estado de la tramitación de los procedimientos en los que tengan la condición de interesados y a acceder y a obtener copia de los documentos contenidos en los citados procedimientos recogido en el artículo 53.1.a) de la Ley 39/2015, lo que incluye el acceso a los datos personales que figuren en el procedimiento..*
>
> *Por lo tanto, el acceso al expediente administrativo y la obtención de copias de los documentos deberá sujetarse a lo previsto en la normativa reguladora de los correspondientes procedimientos, al igual que la rectificación de los datos inexactos o incompletos deberá instarse en los trámites previstos por la citada normativa.*
> *[…]*
>
> *En cuanto al derecho de supresión, no resultará de aplicación conforme al artículo 17.3.b del RGPD, al ser el tratamiento necesario para para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.*
> *[…]*
>
> *Respecto del derecho de oposición, en principio resultará de aplicación con carácter general, al tratarse de tratamientos legitimados en la letra e) del artículo 6.1. del RGPD, salvo en los supuestos concretos en que el tratamiento se fundamente en la letra c) de dicho precepto, según lo*

analizado anteriormente. No obstante, podrá denegarse el mismo por "motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado" conforme al artículo 21.1 del RGPD, al perjudicar el ejercicio de la potestad sancionadora e impedir la tramitación de los correspondientes procedimientos, tal y como específicamente ha reconocido el legislador al modificar, mediante la disposición final duodécima de la LOPDGDD el artículo 28.2 de la Ley 39/2015:

"Los interesados tienen derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración. La administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello. No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección".

Por consiguiente, el derecho de acceso y el derecho de rectificación queda sometido a la normativa sobre procedimiento administrativo; el de supresión, queda excluido por el propio RGPD; y el de oposición, se puede denegar, si bien podría valorarse introducir expresamente su exclusión en el artículo 234.2.

Por lo tanto, a juicio de esta Agencia, las principales limitaciones que derivan de la previsión del artículo 234.2 del anteproyecto afectarían al derecho de información al afectado, respecto del cual, en nuestro informe 74/2019 indicábamos lo siguiente:

Por consiguiente, siempre que los datos personales se obtengan directamente del interesado, deberá informarse al mismo en los términos señalados anteriormente, (por ejemplo, en los formularios de denuncia o en las actas en las que se documente la correspondiente actuación), salvo que el interesado ya disponga de dicha información.

Por el contrario, en los casos en que los datos no se obtengan del interesado, que como se señala en la consulta, es la situación que se produce con más frecuencia, como consecuencia de las denuncias recibidas, inspecciones y requerimientos de información, resultará de aplicación lo previsto en el artículo 14 del RGPD, cuyo apartado 5 incluye mayores supuestos de limitación respecto al deber de informar, ya que no deberá de cumplirse con el mismo, además de en los supuestos en que el interesado ya disponga de la información, cuando "la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al

responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado" o "cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria" (artículo 14.5 letras c y d). Asimismo, el artículo 23 del RGPD, ya transcrito, prevé la posibilidad de que el Derecho de la Unión o de los Estados Miembros puedan limitar este derecho por razón de "g) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social" y "h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g)".

En este sentido, estando prevista la comunicación de la información en la LDC y en la Ley 3/2013 y las limitaciones derivadas del tratamiento de la información confidencial, del deber de secreto y de la tramitación de la información reservada con carácter previo a la incoación del procedimiento sancionador, implican que no resulte de aplicación el deber de información previsto en el artículo 14 del RGPD con carácter previo a la incoación del correspondiente procedimiento sancionador, siendo el acuerdo de incoación la primera actuación que la DC tiene obligación de notificar al interesado conforme al artículo 49.1 de la LDC y el artículo 64.1 de la Ley 39/2015. Una vez incoado el correspondiente procedimiento sancionador, deberá darse cumplimiento al deber de informar salvo que dicha información hubiera sido facilitada con anterioridad. En este sentido se pronunció ya esta Agencia en el Informe 201/2016:

Cierto es, en respuesta concreta a la pregunta realizada, que el artículo 5.4 LOPD no requiere expresamente que la información que ha de darse en virtud de dicho artículo lo sea en el acuerdo de inicio expediente sancionador, por cuanto, como bien apunta la consulta, dicho artículo tan sólo establece que el interesado habrá de ser informado del contenido del tratamiento, de la procedencia de los datos, y de lo previsto en las letras a), d) y e) del apartado 1 del artículo 5, si no hubiese sido ya informado con anterioridad (y siempre en el plazo de los tres meses siguientes al momento del registro de los datos). Ello supone que si con anterioridad un tercero (por ejemplo la Guardia Civil, como expone la consulta) o el propio responsable del fichero –a través de la Inspección- han informado al interesado de las circunstancias previstas en dicho apartado 5.4 LOPD, no es necesario una nueva información a este respecto. Por ello, si ya ha existido dicha información previa no será necesaria una nueva información, ya sea en el acuerdo

de inicio del procedimiento sancionador o mediante una notificación específica al respecto.

Todo ello sin perjuicio de que a las personas que faciliten los datos se les deba informar, respecto del tratamiento de sus datos personales, en los términos del artículo 13 del RGPD, según lo visto anteriormente.

En cuanto a la información a los interesados que deben facilitar los responsables del tratamiento de las empresas o entidades que faciliten información a la DC, y sin perjuicio de que las mismas han debido cumplir con el deber de información a los interesados en el momento en que obtuvieron los datos en los términos de los artículos 13 y 14, en el momento en que se procede a su comunicación a la DC es cuando resulta de aplicación lo previsto en el artículo 4.9) del RGPD al definir el concepto de destinatario: "la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento". Como hemos visto anteriormente, se trata de una previsión que ya se contenía en el artículo 2, letra g) de 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos: "g) «destinatario»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios".

Dicho precepto despliega toda su virtualidad en relación con el deber de informar conforme a los artículos 13 y 14 del RGPD, que impone la obligación al responsable de informar sobre "los destinatarios o las categorías de destinatarios de los datos personales, en su caso", no teniendo esta consideración la DC.

La aplicación de dicha regla, unida a las limitaciones derivadas del tratamiento de la información confidencial, del deber de secreto y el carácter reservado de la información previa suponen que las empresas o entidades que faciliten información a la DC no deban suministrar al afectado la información prevista en los artículos 13 y 14 del RGPD.

Por todo ello, teniendo en cuenta que el artículo 23.2 del RGPD prevé que en la norma limitadora se fije un contendido específico, incluyendo, entre otros supuestos, el alcance de las limitaciones establecidas, debería recogerse expresamente en el artículo 234.2 qué derechos se considera que deben quedar limitados y en qué forma se produce esa limitación (exclusión total, o un aplazamiento, limitación u omisión parcial). Singularmente, teniendo en cuenta que la salvaguarda del buen fin de las actuaciones inspectoras y supervisoras incide directamente en el derecho/deber de información, debería recogerse específicamente, señalando el momento a partir del cual se deberá facilitar la información correspondiente.

Asimismo, deberían incluirse garantías adicionales a las ya señaladas, como puede ser, en su caso, el deber de informar al afectado sobre su solicitud en el plazo de un mes, conforme al artículo 12.3 del RGPD o el derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, de conformidad con el artículo 77 del RGPD.

V

El Capítulo II del Título IX regula las “Relaciones de cooperación entre la CNMV y otras autoridades nacionales, europeas y de terceros estados”.

En relación con los diferentes supuestos de intercambio o suministro de información previstos en el citado capítulo, en la medida en que pueden suponer transferencias de datos personales a terceros países, será de aplicación lo dispuesto en el Título V del Reglamento general de protección de datos que, como regla general, establece en su artículo 44 que “Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado”.

Pues bien, el régimen regulador de las transferencias internacionales de datos en el Reglamento establece una serie de reglas que deberán ser adecuadamente cumplidas para que proceda la transmisión a la que se refiere el Anteproyecto.

En primer lugar, será posible la colaboración en caso de que sea aplicable el artículo 45.1 del Reglamento, a cuyo tenor “Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica”.

Si el Estado de destino no tuviese el citado nivel adecuado, seguiría siendo posible la transferencia si se diera cumplimiento a lo dispuesto en el artículo 46.1, cuyo apartado 1 dispone que “A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas”.

En particular, en lo que afecta a la colaboración entre organismos con potestades de derecho público, el artículo 46.2 a) del Reglamento establece que “Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por (…) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos.

De no existir dicho instrumento, el artículo 46.3 b) aún permite la transferencia, si bien en ese caso sometida a autorización de la autoridad de control. Así se indica que “Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante (…) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados”.

En este mismo sentido, el artículo 42.1 b) de la LOPDGDD dispone que “Las transferencias internacionales de datos a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en el artículo anterior y en el artículo 46.2 del Reglamento (UE) 2016/679, requerirán una previa autorización de la Agencia Española de Protección de Datos o, en su caso, autoridades autonómicas de protección de datos, que podrá otorgarse (…) cuando la transferencia se lleve a cabo por alguno de los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento”.

Por otro lado, a falta de los instrumentos anteriores y en supuestos excepcionales, la transferencia podría basarse en la excepción de interés público contemplada en el artículo 49.1.d) del RGPD: la transferencia sea necesaria por razones importantes de interés público.

Por último, deberán tenerse en consideración los criterios establecidos por el Tribunal de Justicia de la Unión Europea en su sentencia de 16 julio 2020, asunto C-311/18, Caso Data Protection Commissioner contra Facebook Ireland Ltd y Otros (más conocida como SCHREMS II), que ha declarado inválida la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-EE. UU.

Estas disposiciones deberán ser respetadas todos los supuestos de suministro de información a terceros países, circunstancia que ha sido expresamente prevista en el Considerando 17 de la Directiva (UE) 2019/2034:

> A efectos de la presente Directiva, el tratamiento de datos personales debe llevarse a cabo de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (9) y el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo (10). En particular, cuando la presente Directiva permita los intercambios de datos personales con terceros países, deben aplicarse las disposiciones pertinentes del capítulo V del Reglamento (UE) 2016/679 y capítulo V del Reglamento (UE) 2018/1725.

Y, consecuentemente, se ha introducido dicha previsión en el artículo 248 del anteproyecto informado, que señala que “La CNMV podrá transferir datos personales a Estados no miembros de la Unión Europea de conformidad con la normativa de protección de datos de carácter personal”.

No obstante, aunque debe interpretarse que dicha previsión, contenida en el artículo 248, se aplicará a todo supuesto de transferencias internacionales de datos por parte de la CNMV, el artículo 250, al regular las excepciones a la obligación de secreto, incluye otro supuesto que puede implicar transferencias internacionales de datos y para el que establece reglas específicas en su letra j):

> j) Las informaciones que la CNMV tenga que facilitar, para el cumplimiento de sus funciones, a la ABE, AEVM, a la Junta Europea de Riesgo Sistémico, a los organismos o autoridades de otros países en los que recaiga la función pública de supervisión de las entidades de crédito, de las entidades aseguradoras o reaseguradoras, de otras instituciones

financieras y de los mercados financieros, o la gestión de los sistemas de garantía de depósitos o indemnización de los inversores, siempre que exista reciprocidad, y que los organismos y autoridades estén sometidos a secreto profesional en condiciones que, como mínimo, sean equiparables a las establecidas por las leyes españolas.

En el caso de que dichas informaciones contengan datos personales, además de la existencia de reciprocidad y de secreto profesional, será en todo caso de aplicación el régimen de trasferencias internacionales de datos previsto en el Capítulo V del Reglamento (UE) 2016/679, por lo que sería conveniente que en este apartado se recogiera, igualmente, la necesidad de cumplir con normativa de protección de datos de carácter personal.

VI

El Capítulo V regula la Comunicación de infracciones, dando cumplimiento a lo previsto en el artículo 22 de la Directiva, que prevé determinadas garantías de protección de los afectados, tanto de los que comuniquen la posible infracción como de los presuntos infractores, incluida la "protección de los datos personales relativos tanto a las personas que informen del incumplimiento como a la persona física presuntamente responsable de dicho incumplimiento, de conformidad con el Reglamento (UE) 2016/679".

A este respecto, el artículo 273 establece unas garantías de confidencialidad que se estiman adecuadas a la normativa sobre protección de datos personales:

> 1. La CNMV mantendrá un registro con la totalidad de la información recibida a través de los canales señalados en el artículo 271 [Tipos y contenido mínimo de las comunicaciones].3 El registro asegurará la plena confidencialidad de la información recibida, con acceso limitado exclusivamente al personal especializado responsable del tratamiento y gestión de estas comunicaciones.
> Las comunicaciones recibidas no tendrán valor probatorio y no podrán ser incorporadas directamente a las diligencias judiciales o administrativas.
> 2. Cualquier transmisión de la comunicación, dentro o fuera de la CNMV, se realizará sin revelar, directa o indirectamente, los datos personales del comunicante de la infracción, si fuesen conocidos, ni de las personas físicas presuntamente responsables de dicha infracción incluidas en la comunicación, de conformidad con el Reglamento (UE) n.º 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; excepto en los siguientes casos:
a) Los datos personales de la persona presuntamente infractora que resulten necesarios para la realización de actuaciones previas, la iniciación, instrucción y resolución de un procedimiento administrativo sancionador, o bien de un proceso judicial, que tendrán en todo caso un nivel de protección equivalente al de las personas objeto de investigación o de sanción por parte del órgano competente;
b) los datos personales del comunicante cuando fuesen conocidos y así sea expresamente requerido por un órgano judicial competente del orden penal en el curso de diligencias de investigación o proceso penal, cuando constituya un elemento esencial para dicho proceso; y
c) todos los datos personales incluidos en la comunicación que resulten necesarios a autoridades equivalentes a autoridades nacionales competentes en el ámbito de la Unión Europea, previo cumplimiento de los requisitos establecidos en las normas comunitarias o nacionales que resulten de aplicación, o de terceros Estados, siempre que el nivel de protección de la confidencialidad de los datos personales resulte equivalente al vigente en España.

No obstante, en relación con esta última excepción, referida a la comunicación de datos personales a terceros países, se recuerda que deberá garantizarse, además de que existe un nivel de protección de la confidencialidad equivalente, que la transferencia internacional de datos personales cumple con los requisitos establecidos en el Capítulo V del Reglamento (UE) 2016/679, por lo que debería incluirse también dicha referencia, al igual que se ha indicado en el apartado anterior.

Por otro lado, el artículo 272 prevé la posibilidad de que las comunicaciones se formulen de forma anónima y la protección de dicho anonimato, lo que se estima adecuado, atendiendo al interés público tutelado y la admisión de este tipo de denuncias al amparo de lo previsto en la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo de 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (pendiente de transposición), siendo igualmente, el criterio del Tribunal Supremo favorable a este tipo de denuncias, tal y como se recoge en la Sentencia del Tribunal Supremo (Sala Segunda) 272/2020, de 6 de febrero de 2020.

VII

El Capítulo IX del Título IX regula la publicidad de sanciones. A este respecto, hay que diferenciar entre la publicación en el Boletín Oficial del Estado, existente en nuestro ordenamiento jurídico desde la modificación del

artículo 103 de la Ley del Mercado de Valores, de 29 de julio de 1988, por la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, y la publicación en la página web de la CNMV como consecuencia de la transposición del artículo 20 de la Directiva 2019/2034.

La finalidad de la publicidad de las sanciones es, como ha señalado nuestro Tribunal Supremo en su sentencia de 21 de julio de 2009, "reforzar el general conocimiento de los operadores económicos y de los inversores de aquellas prácticas o conductas dirigidas a falsear la libre formación de los precios en el mercado de valores e impedir el flujo de informaciones privilegiadas, con el fin de proteger al inversor, y trata, por ello, de garantizar que la Comisión Nacional del Mercado de Valores desarrolle eficientemente la función legalmente atribuida de informar de aquellos hechos que puedan contribuir a distorsionar el adecuado funcionamiento del mercado bursátil y que resulten necesarios para asegurar la consecución de sus fines". De acuerdo con el Alto Tribunal, esta publicación no tiene la naturaleza de una sanción pese a su carácter aflictivo y disuasorio.

El artículo 326 recoge una serie de garantías, previstas en el artículo 20 de la Directiva, dirigidas a garantizar la proporcionalidad de dicha medida y que se han hecho extensivas a la publicidad en el BOE prevista en el artículo 327, acabando con el automatismo que existía en dicha publicación, lo que, en relación con la protección de datos personales y las competencias de esta Agencia, se valora positivamente.

No obstante, el artículo 328 del proyecto, que se corresponde con el actual artículo 313 quinquies del texto refundido de la Ley del Mercado de Valores, introducido por el Real Decreto-ley 14/2018, de 28 de septiembre, contempla la publicidad de los acuerdos de iniciación de los procedimientos sancionadores, señalando lo siguiente:

> La CNMV podrá hacer públicos los acuerdos de iniciación de procedimientos sancionadores una vez notificados a los interesados, tras resolver, en su caso, sobre los aspectos confidenciales de su contenido y previa disociación de los datos de carácter personal a los que se refiere el artículo 4.1 del Reglamento (UE) n.º 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016; salvo en lo que se refiere al nombre de los infractores. La publicación se decidirá previa ponderación, suficientemente razonada, entre el interés público, atendiendo a los efectos favorables que, en conjunto, genere sobre la mejor transparencia y funcionamiento de los mercados de valores y la protección de los inversores, y el perjuicio que cause a los infractores.

La incorporación de dicho artículo no se corresponde con la transposición de la Directiva, por lo que debe entenderse que es una posibilidad más dentro de las potestades que corresponde a la CNMV

introducida por la legislación nacional, teniendo la norma rango adecuado pero debiendo cumplir, en todo caso, con el principio de proporcionalidad, a cuyo efecto se establece la imprescindible ponderación entre el interés público y los intereses de los afectados.

No obstante, en lo que se refiere a la posible publicación de datos personales, se observa una contradicción en el texto, ya que por un lado prevé su disociación, lo que implicaría que no se aplicara la normativa sobre protección de datos, y por otro se excluye de la disociación el "nombre de los infractores", por lo que sí resulta de aplicación. **En este caso, hay que tener en cuenta que se trata de acuerdos de inicio en los que todavía no se ha acreditado plenamente la existencia de responsabilidad administrativa, por lo que la publicación del nombre de los presuntos infractores debería recogerse, por aplicación de los principios de limitación de la finalidad, minimización de datos y proporcionalidad, con carácter excepcional, solo en los supuestos en los que la finalidad de interés público pretendida, consistente en la mejor transparencia y funcionamiento de los mercados de valores y la protección de los inversores, no pueda conseguirse sin la publicación del nombre de los presuntos infractores.**

Por último, conviene recordar que esta Agencia ha tenido ocasión de pronunciarse en otras ocasiones sobre la publicidad de las sanciones en otros ámbitos en que la normativa comunitaria o internacional así lo prevé, como ocurre en el dopaje, pudiéndose citar al efecto los informes 288/2012 y 455/2010, en los que se destacaba que no obstante la existencia de una base legal que legitime dicho tratamiento, el mismo debe ser conforme al resto de principios de la protección de datos de carácter personal, debiéndose informar sobre esa publicación en el momento de la notificación de la resolución sancionadora y estableciendo las garantías adecuadas que permitan respetar los principios que actualmente se recogen en el artículo 5 del RGPD, en particular los de limitación de la finalidad, minimización, exactitud y limitación del plazo de conservación. Estas garantías aparecen previstas en el artículo 20 de la Directiva y se han recogido adecuadamente en el artículo 326 del proyecto, distinguiendo entre sanciones y medidas provisionales firmes y aquellas que estén pendiente de recurso, debiendo informarse en este último caso sobre el mismo. Asimismo, se recogen diferentes supuestos en los que no procederá la publicación, garantizando, de este modo, la proporcionalidad de la medida.

En cuanto al plazo en el que se mantendrá publicada la información, el precepto, recogiendo lo dispuesto en la Directiva, que prevé en su artículo 20.4 que "Los datos de carácter personal solo podrán mantenerse en el sitio web oficial de la autoridad competente, cuando lo permitan las normas aplicables en materia de protección de datos, establece que "Los datos de carácter personal

solo podrán mantenerse en el sitio web oficial, cuando lo permita la Ley Orgánica 3/2018, de 5 de diciembre".

A este respecto, la citada Ley Orgánica 3/2018 no contiene previsión al respecto, sino que debe atenderse al principio de limitación del plazo de conservación establecido en el artículo 5.1.f) del RGPD, de modo que los datos personales serán "mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»)". **Por ello, debería fijarse en el artículo 326.6 el plazo máximo por el que los datos personales podrán mantenerse en el sitio web oficial, que será el necesario para cumplir la finalidad prevista**.