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

I

El Anteproyecto remitido tiene por objeto garantizar los derechos fundamentales de los niños, niñas y adolescentes a su integridad física, psíquica, psicológica y moral frente a cualquier forma de violencia, asegurando el libre desarrollo de su personalidad y estableciendo medidas de protección integral, que incluyan la sensibilización, la prevención, la detección precoz, la protección y la reparación del daño en todos los ámbitos en los que se desarrolla su vida.

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), 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.

El citado Reglamento 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.”

Asimismo, el artículo 4.1 define “tratamiento” como “cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción”.

La ejecución de actos de violencia contra los niños, niñas y adolescentes pueden implicar, especialmente cuando se realizan a través de las tecnologías de la información y la comunicación, tratamientos ilícitos de datos personales, razón por la cual esta Agencia ha puesto en marcha un Canal prioritario para comunicar la difusión ilícita de contenido sensible, un sistema que tiene como objetivo dar una respuesta rápida en situaciones excepcionalmente delicadas, como aquellas que incluyen la difusión de contenido sexual o violento.

A pesar de las ventajas que proporcionan las nuevas tecnologías y los servicios que estas ofrecen, en ocasiones se utilizan como vía para extender formas de violencia que fomentan la humillación pública de las víctimas, dañando de forma grave su privacidad. Las características de las TIC han dado lugar a nuevas amenazas para los menores y la mujer víctima de violencia, derivadas, entre otras, de la velocidad con la que la información se difunde en este entorno, la posibilidad de acceder a la información gracias a los motores de búsqueda y las dificultades para su eliminación. La facilidad para viralizar y la perdurabilidad y falta de olvido en el entorno en línea entrañan nuevas situaciones de riesgo, como pueden ser el acceso y la divulgación sin consentimiento de información sensible, de fotografías o vídeos de carácter íntimo; la vigilancia y monitoreo de actividades en línea; daños a la reputación de la mujer; las conductas conocidas como «sextorsión» o el acoso sexual en línea.

La extensión y el uso intensivo de dispositivos móviles e Internet, redes sociales y servicios como los de mensajería instantánea o de geolocalización, han servido de cauce para la proliferación de conductas violentas, comprobándose que, en muchas ocasiones, Internet y sus servicios y aplicaciones se han utilizado con la finalidad de controlar, amedrentar, acosar, humillar y chantajear a mujeres y a menores de edad. La grabación y difusión de imágenes personales es uno de los instrumentos más utilizados en los casos de acoso escolar -bullying y su versión a través de Internet, cyberbullying- y de acoso sexual a menores -grooming o sexting-, en ocasiones con trágicas consecuencias.

Por ello, esta Agencia considera necesario que en el Anteproyecto objeto de informe se recoja dicha circunstancia en su Exposición de Motivos y se haga

una especial referencia a la “violencia digital” y las nuevas formas de violencia contra los menores derivadas del uso de Internet y las redes sociales, atendiendo, de este modo, a las recomendaciones contenidas en el Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos de 18 de junio de 2018, proponiéndose la siguiente redacción del artículo 1.2:

«Artículo 1. *Objeto.*

2. A los efectos de esta ley, se entiende por violencia toda acción, omisión o trato negligente que priva a las personas menores de edad de sus derechos y bienestar, que amenaza o interfiere su ordenado desarrollo físico, psíquico o social, con independencia de su forma y medio de comisión incluida la realizada a través de las tecnologías de la información y la comunicación, **especialmente la violencia digital.**

En todo caso, se entenderá por violencia el maltrato físico, psicológico o emocional, los castigos físicos, humillantes o denigrantes, el descuido o trato negligente, **las amenazas, injurias y calumnias**, la explotación, las agresiones y los abusos sexuales, la corrupción, el acoso escolar, el acoso sexual, **el ciberacoso,** la violencia de género, la mutilación genital, la trata de seres humanos con cualquier fin, el matrimonio infantil, **la pornografía no consentida o no solicitada, la extorsión sexual, la difusión pública de datos privados** así como la presencia de cualquier comportamiento violento en su ámbito familiar».

II

Asimismo, y atendiendo a la finalidad preventiva perseguida por el Anteproyecto, esta Agencia considera necesario garantizar una adecuada formación en un uso responsable de internet. Internet y las redes sociales han experimentado un avance sin precedentes en los últimos años. La facilidad de uso y de difusión expone a los ciudadanos, especialmente a los menores, a múltiples riesgos que afectan a su privacidad y derechos, siendo necesaria una formación específica en esta materia.

Por ello se propone que el artículo 5, relativo a la formación, incluya la necesaria respecto al uso responsable de internet, de modo que la letra c) del apartado 1 tenga la siguiente redacción:

«Artículo 5. *Formación.*

1. Las Administraciones Públicas, en el ámbito de sus respectivas competencias, promoverán y garantizarán una formación especializada, inicial

y continua en materia de derechos fundamentales de la infancia y la adolescencia a los y las profesionales que tengan un contacto habitual con las personas menores de edad. Dicha formación comprenderá como mínimo:

[…]

c) Formación específica en seguridad y uso seguro **y responsable** de Internet.

[…]».

Por la misma razón se propone incluir, en el artículo 32, la formación en materia de derechos y responsabilidad digital, en consonancia con lo previsto en el artículo 83 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales:

> «Artículo 32. *Formación en materia de* ***derechos,*** *seguridad y* ***responsabilidad*** *digital.*
>
> **Las Administraciones Públicas garantizarán la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales, conforme a lo previsto en el artículo 83 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.**
>
> **Asimismo,** las Administraciones Públicas deberán incorporar contenidos obligatorios y específicos para la capacitación de las personas menores de edad en materia de seguridad digital. Dicha formación se incluirá tanto en los bloques de contenidos como con carácter transversal, y deberá implantarse desde la etapa de educación primaria».

III

De acuerdo con reiterada doctrina constitucional, el derecho fundamental a la protección de datos personales consagrado en el artículo 18.4 de la

Constitución, es un derecho independiente del derecho a la intimidad. En este sentido se pronunciaba la sentencia 292/2000:

> "…el Tribunal ya ha declarado que el art. 18.4 C.E. contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo «un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama ´la informática»´, lo que se ha dado en llamar «libertad informática» (F.J. 6, reiterado luego en las SSTC 143/1994, F.J. 7, 11/1998, F.J. 4, 94/1998, F.J. 6, 202/1999, F.J. 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 C.E.), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada «libertad informática» es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, F.J. 5, 94/1998, F.J. 4).
>
> Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 C.E., con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 C.E. debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 C.E.), bien regulando su ejercicio (art. 53.1 C.E.). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.
>
> La función del derecho fundamental a la intimidad del art. 18.1 C.E. es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, F.J. 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, F.J. 5; 144/1999, F.J. 8; 98/2000, de 10 de abril, F.J. 5; 115/2000, de 10

de mayo, F.J. 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.

De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 C.E., sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre, F.J. 4), como el derecho al honor, citado expresamente en el art. 18.4 C.E., e igualmente, en expresión bien amplia del propio art. 18.4 C.E., al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.

De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 C.E. otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 C.E. Dicha peculiaridad radica

en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (SSTC 73/1982, de 2 de diciembre, F.J. 5; 110/1984, de 26 de noviembre, F.J. 3; 89/1987, de 3 de junio, F.J. 3; 231/1988, de 2 de diciembre, F.J. 3; 197/1991, de 17 de octubre, F.J. 3, y en general las SSTC 134/1999, de 15 de julio, 144/1999, de 22 de julio, y 115/2000, de 10 de mayo), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, F.J. 7).”

Partiendo de lo anterior, se considera necesario incluir en los protocolos de actuación regulados en el artículo 33, la necesaria protección del derecho fundamental a la protección de datos:

«Artículo 33. *Protocolos de actuación.*

2. Entre otros aspectos, los protocolos determinarán las actuaciones a desarrollar, los sistemas de comunicación y la coordinación de los y las profesionales responsables de cada actuación.

Asimismo, deberán contemplar actuaciones específicas cuando el acoso tengan como motivación la discapacidad, el origen racial o nacional, la orientación sexual, la identidad o expresión de género. De igual modo, dichos protocolos deberán contemplar actuaciones específicas cuando el acoso se lleve a cabo a través de las nuevas tecnologías o dispositivos móviles y se haya menoscabado la intimidad**,** ~~y~~ reputación **o el derecho a la protección de datos personales** de las personas menores de edad».

IV

La Agencia Española de Protección de Datos es una autoridad administrativa independiente a la que le corresponde la función de supervisar la aplicación de la normativa vigente en materia de protección de datos personales con el fin de proteger los derechos y libertades de las personas físicas en lo que respecta al tratamiento y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 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 éstos y por el que se deroga la Directiva 95/46/CE (en adelante, Reglamento General de Protección de Datos o RGPD) en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) y en sus disposiciones de desarrollo.

Con la aplicación efectiva del RGPD el 25 de mayo de 2018, se pretende hacer frente a los nuevos retos que para la protección de los datos personales han planteado la rápida evolución tecnológica y la globalización derivados del aumento significativo de la magnitud de su recogida e intercambio, tal y como se expone en su Considerando segundo.

El RGPD, en su considerando 38, señala que “Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales…)”. En el considerando 75 se recoge que los riesgos para los derechos y libertades de las personas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que se traten datos de personas vulnerables, como los niños.

Para que la Agencia Española de Protección de Datos, en cuanto autoridad pública independiente encargada de velar por la privacidad y la protección de datos de los ciudadanos, en particular si se utilizan nuevas tecnologías, pueda tener conocimiento de los posibles tratamientos ilícitos de datos que afecten a los menores y adolescentes y ejercer las competencias que le atribuyen el RGPD y la LOPDGDD, se hace necesario articular los mecanismos de colaboración necesarios, por lo que se proponen las siguientes modificaciones:

«Artículo 8. *Colaboración público-privada.*

2. Asimismo, las Administraciones Públicas competentes adoptarán las medidas necesarias con el fin de asegurar el adecuado desarrollo de las acciones de colaboración con el sector de las de las nuevas tecnologías contempladas en el capítulo VIII del título III.

En especial, se fomentará la colaboración de las empresas de tecnologías de la información y comunicación, **la Agencia Española de Protección de Datos,** las Fuerzas y Cuerpos de Seguridad y la Administración de Justicia con el fin de detectar y retirar, a la mayor brevedad posible, los contenidos ilegales en las redes que supongan una forma de violencia sobre los niños, niñas y adolescentes».

Artículo 34. *Coordinador o Coordinadora de bienestar y protección*.

«2. Las Administraciones educativas competentes determinarán los requisitos y funciones que debe desempeñar el Coordinador o Coordinadora de bienestar y protección. Así mismo, determinarán si estas funciones han de ser desempeñadas por personal ya existente en el centro escolar o por nuevo personal.

Las funciones encomendadas al Coordinador o Coordinadora de bienestar y protección deberán ser al menos las siguientes:

[…]

i) Informar a la Agencia Española de Protección de Datos sobre aquellas situaciones que puedan implicar un tratamiento ilícito de datos de carácter personal de los menores y jóvenes.

Por la misma razón y al objeto de permitir que los niños, niñas y adolescentes que fueran víctimas de violencia o presenciaran alguna situación de violencia sobre otra persona menor de edad, puedan comunicarlo, personalmente, o a través de sus representantes legales, a la Agencia Española de Protección de Datos, cuando se pueda haber producido un tratamiento ilícito de datos personales, con el fin de que ésta pueda ejercer sus competencias, se propone la modificación del artículo 17.1:

«Artículo 17. *Comunicación de situaciones de violencia por parte de niños, niñas y adolescentes.*

1. Los niños, niñas y adolescentes que fueran víctimas de violencia o presenciaran alguna situación de violencia sobre otra persona menor de edad, podrán comunicarlo, personalmente, o a través de sus representantes legales, a los servicios sociales, , a las Fuerzas y Cuerpos de Seguridad, al Ministerio Fiscal o a la autoridad judicial **y, en su caso, a la Agencia Española de Protección de Datos**».

V

Para garantizar una adecuada protección del derecho fundamental a la protección de datos y la rápida retirada de los contenidos que atente gravemente contra el mismo, la AEPD ha creado un Canal específico de denuncia, para evitar la continuidad del tratamiento ilegítimo de los datos personales en casos particularmente graves como víctimas de violencia de género, abuso o agresión sexual o acoso, o cualquier otro colectivo especialmente vulnerable como el de los menores de edad, personas discriminadas por su orientación sexual o raza, personas con discapacidad o enfermedad grave o en riesgo de exclusión social. El Canal prioritario de la AEPD para comunicar la difusión ilícita de contenido sensible y solicitar su retirada pretende ofrecer una respuesta rápida en situaciones excepcionalmente delicadas, como aquellas que incluyen la difusión de contenido sexual o violento. El objetivo es establecer una vía de comunicación para que la Agencia, como autoridad independiente, pueda adoptar, si es preciso, medidas urgentes que limiten la difusión y el acceso a los datos personales.

Con el fin de garantizar la eficacia de dicho canal y su uso por menores de edad, se hace preciso habilitar la posibilidad de denuncia, por sí mismos, por los menores de edad con grado de madurez suficiente, sin necesidad de estar acompañadas de una persona adulta.

Asimismo, teniendo en cuenta que, en muchas ocasiones, el tratamiento ilícito de datos personales se realiza por otros menores de edad, es preciso concretar la responsabilidad de los mayores de 14 años, a los que la LOPDGDD reconoce capacidad para prestar el consentimiento para el tratamiento de sus datos personales y para el ejercicio de los derechos correspondientes, así como establecer la responsabilidad de los padres, tutores, acogedores y guardadores legales o de hecho, por este orden, en razón al incumplimiento de la obligación impuesta a éstos que conlleva un deber de prevenir la infracción administrativa que se impute a los menores de edad.

Atendiendo a lo anterior, y partiendo del reconocimiento de las competencias que, en materia de tratamientos de datos personales, corresponden a la Agencia Española de Protección de Datos, se propone la adición de un nuevo Capítulo en el Título III, con un único artículo (52 bis):

«Capítulo XI: “De la Agencia Española de Protección de Datos”.

Artículo 52 bis:

1. La Agencia Española de Protección de Datos ejercerá las funciones y potestades que le corresponden de acuerdo con lo previsto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal, con el fin de garantizar una protección específica de los datos personales de los menores en los casos de violencia ejercida sobre la infancia y la adolescencia, especialmente cuando se realice a través de las tecnologías de la información y la comunicación.

2. La Agencia garantizará la disponibilidad de un canal accesible y seguro de denuncia de la existencia de contenidos ilícitos en Internet que comportaran un menoscabo grave del derecho a la protección de datos personales.

3. Se permitirá a las personas menores de edad con grado de madurez suficiente, que así lo soliciten, formular denuncia por sí mismas y sin necesidad de estar acompañadas de una persona adulta.

4. Los mayores de 14 años podrán ser sancionados por hechos constitutivos de infracción administrativa de acuerdo con la normativa sobre protección de datos personales.

5. Cuando la autoría de los hechos cometidos corresponda a un menor de dieciocho años, responderán solidariamente con él de la multa impuesta sus padres, tutores, acogedores y guardadores legales o de hecho, por este orden, en razón al incumplimiento de la obligación impuesta a éstos que conlleva un deber de prevenir la infracción administrativa que se impute a los menores».

VI

Especial atención requiere el Título V, relativo a la organización administrativa, que comienza con un Capítulo I que prevé la creación del Registro Central de información sobre la violencia contra la infancia y la adolescencia. El citado precepto no establece la finalidad del Registro ni las garantías adecuadas para la protección del derecho fundamental a la protección de datos personales, si bien del mismo parace derivarse una finalidad estadística y de mejor conocimiento de la situación para la adopción de las medidas oportunas, por lo que, teniendo en cuenta que dicho registro podría implicar el tratamiento de datos correspondientes a infracciones y sanciones administrativas o a condenas e infracciones penales, procedería la anonimización, de modo que los datos sean convertidos en anónimos de forma que el interesado no sea identificable, lo que excluiría la aplicación del RGPD.

En el caso de que los datos no fueran anonimizados, el precepto legal debería establecer todas las garantías adecuadas que limitaran los riesgos para los datos personales de los afectados, incluidas las medidas técnicas y organizativas apropiadas para garantizar el cumplimiento de los principios del RGPD, en los términos que se señalan en el apartado siguiente.

Por ello, se propone la siguiente redacción:

«Artículo 53. *Registro Central de información sobre la violencia contra la infancia y la adolescencia*.

1. **Con la finalidad de compartir información que permita el conocimiento uniforme de la situación de la violencia contra la infancia y la adolescencia,** El Gobierno establecerá , mediante orden ministerial se determinará la creación del Registro Central de información sobre la violencia contra la infancia y la adolescencia, así como la información concreta y el procedimiento a través del cual el Consejo General del Poder Judicial, el Consejo Médico Forense, las Fuerzas y Cuerpos de Seguridad, el RUSSVI (Registro Unificado de Servicios Sociales sobre Violencia contra la infancia) y las distintas Administraciones Públicas deben suministrar los datos requeridos al registro.

La orden ministerial señalará la información que debe notificarse, **anonimizada**, al Registro que, como mínimo, comprenderá los siguientes aspectos:

a) Con respecto a las víctimas: edad, sexo, tipo de violencia, gravedad, nacionalidad y, en su caso, discapacidad.

b) Con respecto a las personas agresoras: edad, sexo y relación con la víctima.

c) Información policial (denuncias, victimizaciones, etc) y judicial.

d) Medidas puestas en marcha, frente a la violencia sobre la infancia y adolescencia».

VII

El Capítulo II del Título V se refiere a la certificación negativa del Registro Central de Delincuentes Sexuales y de Trata de Seres Humanos, "desarrollando y ampliando la protección de las personas menores de edad a través del perfeccionamiento del sistema de exigencia del requisito de no haber cometido delitos contra la libertad o indemnidad sexuales o de trata de seres humanos con fines de explotación sexual para desarrollar actividades que supongan contacto habitual con personas menores de edad", tal y como señala su Exposición de Motivos".

Esta Agencia ha tenido ocasión de pronunciarse en relación con el acceso a los datos que figuran en el Registro Central de Delincuentes Sexuales en sus informes de 25 de julio de 2014, referente al Anteproyecto de Ley de Protección a la Infancia y de 13 de octubre de 2015, relativo al Proyecto de Real Decreto por el que se regula el Registro Central de Delincuentes Sexuales.

En el Informe de 25 de julio de 2014, en relación con el requisito actualmente recogido en el artículo 13.5 de la Ley Orgánica 1/1996, se señalaba lo siguiente:

"Para ello debe partirse como premisa del hecho de que, a diferencia de lo que señala la Exposición de Motivos, y sin perjuicio de lo ya señalado en cuanto a la inexactitud de su fundamentación legal, el citado artículo 13.5 no implica necesariamente la creación de ningún tipo de registro o base de datos referida específicamente a los autores de los delitos contra la libertad e indemnidad sexual de los menores, sino que sólo establece como requisito imprescindible para el ejercicio de actividades que implique el contacto habitual con niños que el interesado no haya sido condenado por la comisión de estos delitos.

En consecuencia, lo que prevé el Anteproyecto es que con carácter previo a la prestación de los servicios a los que se refiere el Anteproyecto el empleador o la Administración que autorice el desarrollo de la actividad puedan conocer que el interesado carece de antecedentes relacionados con la comisión de estos delitos.

Dicho esto, debe tenerse en cuenta que el interesado, pese a la valoración que haya de hacerse de la conducta que condujo a la condena penal por los delitos mencionados, no deja de ser titular del derecho fundamental a la protección de sus datos de carácter personal, por lo que una medida restrictiva de este derecho deberá en todo caso respetar el principio de proporcionalidad, en los términos consagrados por el Tribunal Constitucional, y además como consecuencia del principio de injerencia mínima producir la mínima intromisión en ese derecho.

Dicho esto, no cabe duda de que la previa condena por la comisión de los delitos mencionados en el artículo 13.5 es generadora de una situación de riesgo para la libertad e integridad sexual de los menores de edad con los que pudiera trabajar el condenado, siendo así que los derechos del menor se encuentran especialmente garantizados a partir de la aplicación del interés superior de aquéllos, previsto expresamente en el artículo 2 de la Ley 1/1996.

No debe olvidarse lo ya señalado en el apartado III de este informe en cuanto a la importancia y relevancia que ha de otorgarse a este principio, siendo especialmente importante traer a colación en este momento que, si bien esta Agencia ha declarado que su aplicación podría no bastar por sí misma como fundamento para el tratamiento de datos de carácter personal, ello se ha señalado cuando el tratamiento se refiere a los datos del propio menor, dado que la colisión se produce entonces entre la protección de su interés superior y el derecho a la protección de datos. Sin embargo, en el caso al que ahora se está haciendo referencia, el acceso a los datos al que se refiere el artículo 13.5 de la Ley Orgánica 1/1996, en la redacción propuesta no afectaría a los datos del menor, sino únicamente a los de los terceros que pretendieran realizar actividades que impliquen un contacto habitual con niños.

Por este motivo, la protección del interés superior del menor podría considerarse causa legal suficiente para amparar el acceso a la información por parte de quien pretenda contratar al interesado o por la

Administración que hubiera de autorizar la realización de tales actividades.

Pero, ya se ha dicho, para ello deberá darse cumplimiento a las garantías del derecho fundamental a la protección de datos de carácter personal, lo que por una parte exigiría valorar si resulta necesaria la creación de un registro específico para atender a la finalidad perseguida y, por otra, obligaría a analizar las condiciones en que debería producirse dicho acceso.

En cuanto a la creación del registro, debe tenerse en cuenta que el artículo 13.5 se refiere a la existencia de condenas por sentencia firme. En este sentido, no debe olvidarse que el artículo 2. 3 a) del Real Decreto 95/2009, de 6 de febrero, por el que se regula el Sistema de registros administrativos de apoyo a la Administración de Justicia integra en el mencionado sistema al Registro Central de Penados, en el que se procederá a “la inscripción de las resoluciones firmes por la comisión de un delito o falta que impongan penas o medidas de seguridad, dictadas por los Juzgados o Tribunales del orden jurisdiccional penal”. Es decir, la información referida a las condenas firmes ya se incorpora a un registro existente, lo que parece hacer innecesaria la creación de otro sistema de información distinto, quedando el tratamiento de los datos sometido además a las normas de este registro ya existente en cuanto a sus accesos y conservación de la información.

Sentado lo anterior, debería ahora valorarse cómo podría verificarse el cumplimiento por el interesado de la condición establecida en el artículo 13.5 propuesto; es decir, el procedimiento de acreditación de la inexistencia de los antecedentes penales. A tal efecto, ciertamente los artículos 5 y 6 del Real Decreto mencionado, referidos al acceso a los registros del sistema en general y al registro de penados en particular, no prevén los accesos a la información a los fines que se establecen en el artículo 13.5.

No obstante, el artículo 17.1 del Real Decreto establece claramente que “A petición del titular interesado, podrán certificarse directamente los datos relativos a su persona contenidos en las inscripciones de los Registros Centrales de Penados, de Medidas Cautelares Requisitorias y Sentencias No Firmes, de Protección de las Víctimas de Violencia Doméstica, de Sentencias de Responsabilidad Penal de los Menores y de Rebeldes Civiles y suscribir certificaciones negativas respecto a personas que no figuren inscritas en los mismos”, existiendo diversos supuestos en las normas actualmente vigente que

exigen la aportación de este tipo de certificaciones para la realización de determinados trámites o la obtención de autorizaciones, pudiendo incluso encontrarse ejemplos de la exigencia de este requisito en el ámbito laboral en relación con sectores específicos.

Pues bien, siendo posible que el legislador pueda exigir la aportación de una certificación negativa por el interesado para que proceda la autorización del mismo para la realización de actividades que impliquen un contacto habitual con niños o para la contratación del interesado para la realización de esas actividades, parece lógico que la medida que permite una mejor conciliación de la especial protección del interés superior del menor, consagrado por el artículo 2 de la Ley Orgánica 1/1996 con el derecho a la protección de datos de carácter personal sería la exigencia de esa certificación negativa del registro, referida específicamente a la comisión de los delitos mencionados por el artículo 13.5.

Para ello sería suficiente que el Anteproyecto clarificase que a los efectos establecidos en el precepto que ahora se está analizando, quienes pretendan llevara cabo las actividades a las que se refiere el mismo deberán aportar un certificado del Registro Central de Penados que acredite la inexistencia de condenas por la comisión de los delitos mencionados. Para ello **sería suficiente añadir un segundo párrafo al artículo 13.5 propuesto, en que se indicase que:**

> **“A tal efecto, quien pretenda el acceso a tales profesiones deberá acreditar esta circunstancia mediante la aportación de certificación negativa del Registro Central de Penados.”**

Y en el informe de 13 de octubre de 2015 se añadía:

“De lo que apuntaba el anterior informe de esta Agencia se desprende que el sistema que la misma plantaba se basaba en la aportación por el interesado del certificado negativo del Registro, teniendo en cuenta que la creación de un nuevo Registro lo residenciaría en éste y no en el de Penados.

Este modelo podría encajar con el establecido en el Proyecto sometido a informe, por cuanto cabría considerar que el mismo parte de un modelo en que, en principio, el interesado estaría obligado a la

aportación del certificado, si bien en los supuestos en los que el destinatario fuese una Administración Pública, aquél se encontraría exonerado de su obligación en los términos establecidos en la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, cuyo artículo 6.1 b) reconoce a los interesados el derecho "a no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información".

Sin embargo, el artículo citado se completa con la exigencia adicional de que "en el caso de datos de carácter personal, se cuente con el consentimiento de los interesados en los términos establecidos por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, o una norma con rango de Ley así lo determine, salvo que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados", añadiendo que "el citado consentimiento podrá emitirse y recabarse por medios electrónicos".

El artículo 13.5 de la Ley Orgánica 1/1996, al referirse a la exigencia a la que ahora estamos haciendo referencia dispone que "quien pretenda el acceso a tales profesiones, oficios o actividades deberá acreditar esta circunstancia mediante la aportación de una certificación negativa del Registro Central de delincuentes sexuales". Es decir, impone al interesado la obligación de acreditar la inexistencia de estos antecedentes, sin que se prevea un acceso directo por el empleador al mencionado Registro.

Ello afecta al apartado 1 del artículo 9 del Proyecto ahora informado, dado que al no existir una habilitación legal para el acceso directo al Registro, el acceso deberá producirse previo consentimiento del interesado.

El Proyecto prevé expresamente esta circunstancia. Sin embargo hace posteriormente referencia a la posible existencia de una habilitación legal. No obstante, como se ha indicado, la norma que impone la obligación de acreditar la inexistencia de antecedentes penales por los delitos a los que se refiere el Proyecto precisamente excluye esta habilitación, por lo que **procedería suprimir el inciso "salvo que una norma con rango de Ley lo exceptúe", debiendo además indicarse que a falta de consentimiento el certificado se expedirá a instancia del propio interesado, en términos similares a los previstos en el apartado 2 del artículo 9**."

Como señala su Exposición de Motivos, el texto que ahora se informa "extiende la obligación de acreditar el requisito de no haber cometido delitos contra la libertad e indemnidad sexuales a todos los trabajadores y trabajadoras, lo sean por cuenta propia o por cuenta ajena, tanto del sector

público como del sector privado", manteniendo el criterio actualmente vigente de que sea el trabajador el que aporte la certificación negativa del Registro Central de Delincuentes Sexuales y Trata de Seres Humanos, salvo en el caso en que se deba acreditar ante la Administración, en cuyo caso y siempre que conste el consentimiento expreso del interesado, podrá obtenerse directamente por las mismas, como manifestación del derecho a no aportar documentos que obren en poder de la Administración recogido en el artículo 28.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Sin embargo, el texto remitido introduce dos disposiciones que alteran dicho sistema de acreditación de la ausencia de condenas penales. El primero, el apartado 3 del artículo 54, en el que se señala que "La Administración General del Estado deberá establecer los mecanismos necesarios que permitan la comprobación automática de la inexistencia de antecedentes mediante el cruce de la información existente en las bases de datos de trabajadores por cuenta ajena y por cuenta propia y la recogida en Registro Central de Delincuentes Sexuales y de Trata de Seres Humanos". Y el segundo, el apartado 3 del artículo 55, que indica que "Asimismo, la Administración General del Estado establecerá los mecanismos necesarios que permitan, para las personas que desarrollan actividades de voluntariado, la comprobación de la inexistencia de antecedentes mediante el cruce de la información recopilada por las asociaciones en las que desarrollen su actividad voluntaria y la recogida en el Registro Central de Delincuentes Sexuales y de Trata de Seres Humanos".

De acuerdo con dichos preceptos, la Administración General del Estado deberá habilitar mecanismos de cruce de información, sin especificar cómo se va a articular dicho cruce, cuales son los datos que se van a intercambiar, quienes son las personas que va a poder acceder a dicha información y cuáles van a ser las garantías que acrediten un tratamiento lícito de dichos datos.

La falta de concrección de dichos apartados impiden un análisis detallado de los mismos desde la perspectiva de la protección de datos personales. No obstante, de los mismos se desprende que a través de dichos mecanismos se va a poder acreditar la ausencia de antecedentes penales por vías diferentes a la aportación de la certificación negativa por el propio afectado y que dicho acceso se va a permitir no sólo a la Administración, sino también a personas o entidades privadas, como resulta más claramente del apartado 3 del artículo 55 relativo a las personas que desarrollan actividades de voluntariado, y de la Disposición transitoria única. Certificaciones periódicas del Registro Central de Delincuentes Sexuales y de Trata de Seres Humanos:

> "En tanto no sean de plena aplicación los mecanismos a los que se refiere el artículo 54.3, los trabajadores por cuenta ajena y los voluntarios deberán aportar períodicamente a su empleador u

> organización dedicada a labores de voluntariado, al menos cada dos años, una certificación negativa del Registro Central de Delincuentes Sexuales y de Trata de Seres Humanos".

Por tanto, procede analizar la proporcionalidad de dicha medida, diferenciando si el acceso se produce por parte de empleadores u organizaciones dedicadas a labores de voluntariado o por parte de la Administración.

En el primer caso, si lo que se pretendiera fuera articular los mecanismos que permitieran a los empleadores u organizaciones dedicadas a labores de voluntariado acceder directamente al contenido del Registro Central de Delincuentes Sexuales y de Trata de Seres Humanos, al tratarse de datos relativos a condenas e infracciones penales, debería partirse de lo dispuesto en el artículo 10 del RGPD: "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".

Al amparo del citado precepto, el artículo 10 de la LOPDGDD prevé lo 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 consiguiente, el primer requisito para que proceda el tratamiento para fines distintos de los señalados en el citado precepto es que venga establecido en una norma con rango de ley. No obstante, dicha norma debe cumplir con los requisitos de proporcionalidad que justifiquen la limitación del derecho fundamental a la protección de datos, tal y como ha señalado reiteradamente el Tribunal Constitucional. Todo ello conduce a la necesidad de valorar si en el supuesto planteado se cumplirían los presupuestos necesarios para apreciar la existencia de proporcionalidad en el tratamiento. A tal efecto, es preciso recordar que la citada proporcionalidad exige, según la doctrina del Tribunal Constitucional, siguiendo a tal efecto la sentada por el Tribunal Europeo de Derechos Humanos, la superación de un triple juicio, en el sentido de determinar si la medida adoptada 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), es decir, si la injerencia producida en el titular del derecho objeto de restricción por la medida es la mínima en aras al logro del fin legítimo perseguido con aquélla.

Además, la norma legal habilitante que supere el citado juicio de proporcionalidad debería establecer todos y cada uno de los presupuestos y condiciones de la intervención, así como las garantías adecuadas de tipo técnico, organizativo y procedimental, tal y como recuerda la sentencia del Tribunal Constitucional 76/2019 de 22 de mayo:

> "[…]
> d) Como los demás derechos, el derecho fundamental a la protección de datos personales no tiene carácter absoluto. Puede ser restringido por medio de la ley, siempre que ello responda a un fin de interés general, y los requisitos y el alcance de la restricción estén suficientemente precisados en la ley y respeten el principio de proporcionalidad. A los efectos del presente proceso deben destacarse dos requisitos de esos límites:
>
> - En primer lugar, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas debe responder a un fin constitucionalmente legítimo o encaminarse a la protección o la salvaguarda de un bien constitucionalmente relevante, pues "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) , FJ 8 y las allí citadas) y, además, han de ser proporcionadas al fin perseguido con ellas (SSTC 11/1981 (RTC 1981, 11) , FJ 5, y 196/1987 (RTC 1987, 196) , FJ 6)" (STC 292/2000, FJ 15).

- En segundo lugar, por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, ora incida directamente sobre su desarrollo (art. 81.1 CE), ora limite o condicione su ejercicio (art. 53.1 CE), precisa una habilitación legal (por todas, STC 49/1999, de 5 de abril (RTC 1999, 49) , FJ 4). En la STC 49/1999, FJ 4, definimos la función constitucional de esa reserva de ley en los siguientes términos:

"Esa reserva de ley a que, con carácter general, somete la Constitución española la regulación de los derechos fundamentales y libertades públicas reconocidos en su Título I, desempeña una doble función, a saber: de una parte, asegura que los derechos que la Constitución atribuye a los ciudadanos no se vean afectados por ninguna injerencia estatal no autorizada por sus representantes; y, de otra, en un Ordenamiento jurídico como el nuestro en el que los Jueces y Magistrados se hallan sometidos "únicamente al imperio de la Ley" y no existe, en puridad, la vinculación al precedente (SSTC 8/1981 (RTC 1981, 8) , 34/1995 (RTC 1995, 34) , 47/1995 (RTC 1995, 47) y 96/1996 (RTC 1996, 96)) constituye, en definitiva, el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas. Por eso, en lo que a nuestro Ordenamiento se refiere, hemos caracterizado la seguridad jurídica como una suma de legalidad y certeza del Derecho (STC 27/1981 (RTC 1981, 27) , fundamento jurídico 10)."

Esta doble función de la reserva de ley se traduce en una doble exigencia: por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, esa norma legal "ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica", esto es, "ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención" (STC 49/1999, FJ 4). En otras palabras, "no sólo excluye apoderamientos a favor de las normas reglamentarias [...], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites" (STC 292/2000, FJ 15).

La segunda exigencia mencionada constituye la dimensión cualitativa de la reserva de ley, y se concreta en las exigencias de previsibilidad y certeza de las medidas restrictivas en el ámbito de los

derechos fundamentales. En la STC 292/2000, FJ 15, señalamos que, aun teniendo un fundamento constitucional, las limitaciones del derecho fundamental establecidas por una ley "pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad en los propios límites que imponen y su modo de aplicación", pues "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"; "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". En la misma Sentencia y fundamento jurídico precisamos también el tipo de vulneración que acarrea la falta de certeza y previsibilidad en los propios límites: "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, FJ 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, FJ 15; 142/1993, de 22 de abril (RTC 1993, 142) , FJ 4, y 341/1993, de 18 de noviembre (RTC 1993, 341) , FJ 7)".

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 (RTC 2000, 292) , 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 (TJCE 2014, 104) , 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 (RCL 1999, 1190, 1572) , las sentencias TEDH, Liberty y otros c. Reino Unido de 1 de julio de 2008 (TEDH 2008, 45) , nº 58243/00, §§ 62 y 63; Rotaru c. Rumanía (TEDH 2000, 130) , antes citada, §§ 57 a 59, y S y Marper c. Reino Unido (TEDH 2008, 104) , 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 (LCEur 2007, 2329) 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 (LCEur 2006, 820) 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 (LCEur 2002, 140) .

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.

La exigencia de especial protección de esta categoría de datos está prevista en el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (RCL 1985, 2704) , de 28 de enero de 1981 (instrumento de ratificación publicado en el Boletín Oficial del Estado núm. 274, de 15 de noviembre de 1985), cuyo artículo 6 establece lo siguiente: "Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. [...]." Esa exigencia ha sido igualmente afirmada por la Agencia Española de Protección de Datos. De acuerdo con el preámbulo de su Circular 1/2019 (RCL 2019, 398) , esas garantías adecuadas y específicas para proteger los intereses y derechos fundamentales de los afectados "adquieren una especial relevancia tanto por la importancia de los datos personales objeto de tratamiento como por tratarse de tratamientos a gran escala de categorías especiales que entrañarán un alto riesgo para los derechos y libertades de las personas físicas difícilmente mitigable si no se toman medidas adecuadas". Asimismo, como ya se indicó en el fundamento jurídico 4 de esta Sentencia, el Reglamento (UE) 2016/679 (LCEur 2016, 605) reitera la exigencia de que el legislador que regule el tratamiento de datos personales relativos a las opiniones políticas establezca dichas garantías adecuadas [art. 9.2 g) y considerando 56].

Las garantías adecuadas deben velar por que el tratamiento de datos se realice en condiciones que aseguren la transparencia, la

supervisión y la tutela judicial efectiva, y deben procurar que los datos no se recojan de forma desproporcionada y no se utilicen para fines distintos de los que justificaron su obtención. La naturaleza y el alcance de las garantías que resulten constitucionalmente exigibles en cada caso dependerán de tres factores esencialmente: el tipo de tratamiento de datos que se pretende llevar a cabo; la naturaleza de los datos; y la probabilidad y la gravedad de los riesgos de abuso y de utilización ilícita que, a su vez, están vinculadas al tipo de tratamiento y a la categoría de datos de que se trate. Así, no plantean los mismos problemas una recogida de datos con fines estadísticos que una recogida de datos con un fin concreto. Tampoco supone el mismo grado de injerencia la recopilación y el procesamiento de datos anónimos que la recopilación y el procesamiento de datos personales que se toman individualmente y no se anonimizan, como no es lo mismo el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, la salud, la vida sexual o la orientación sexual de una persona física, que el tratamiento de otro tipo de datos.

El nivel y la naturaleza de las garantías adecuadas no se pueden determinar de una vez para todas, pues, por un lado, deben revisarse y actualizarse cuando sea necesario y, por otro lado, el principio de proporcionalidad obliga a verificar si, con el desarrollo de la tecnología, aparecen posibilidades de tratamiento que resultan menos intrusivas o potencialmente menos peligrosas para los derechos fundamentales".

Partiendo de la anterior doctrina constitucional, en el caso de que lo que se pretendiera fuera la verificación de la ausencia de condenas penales directamente por el empleador o la organización dedicada a labores de voluntariado, dicho tratamiento de datos personales debe considerarse excesivo, al existir otras posibilidad menos lesiva para el derecho fundamental a la protección de datos como es la aportación de la certificación por el propio trabajador o voluntario, ratificándose esta Agencia en el criterio manifestado en su informe de 25 de julio de 2014:

"Pues bien, siendo posible que el legislador pueda exigir la aportación de una certificación negativa por el interesado para que proceda la autorización del mismo para la realización de actividades que impliquen un contacto habitual con niños o para la contratación del interesado para la realización de esas actividades, parece lógico que la medida que permite una mejor conciliación de la especial protección del interés superior del menor, consagrado por el artículo 2 de la Ley Orgánica 1/1996 con el derecho a la protección de datos de carácter personal sería la exigencia de esa certificación negativa del registro, […]".

Si bien, como también se señalaba por esta Agencia en el informe de 13 de octubre de 2015, en los supuestos en los que el destinatario fuese una Administración Pública, aquél se encontraría exonerado de su obligación en los

términos establecidos actualmente por la Ley 39/2015, siempre que preste su consentimiento expreso.

Por el contrario, si lo que se pretendiera fuera el acceso a los datos obrantes en el Registro Central de Delincuentes Sexuales y de Trata de Seres Humanos de las Administraciones Públicas en el ejercicio de sus potestades de control e inspección, al amparo de lo previsto en el artículo 6.1.e) del RGPD (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) la ley debería definir con precisión todos los presupuestos del tratamiento y las garantías adecuadas, en los términos anteriormente señalados, teniendo en cuenta que no cabe un acceso masivo e indiscriminado a los datos personales, tal y como resalta la sentencia del Tribunal Constitucional 17/2013, de 31 de enero:

"En cuanto al segundo párrafo de la disposición adicional impugnada, el mismo autoriza a los órganos de la Administración estatal, competentes en el ámbito de los procedimientos administrativos que se tramiten en el ámbito que regula la Ley Orgánica de derechos y libertades de los extranjeros y solamente en el ejercicio de las competencias que tienen atribuidas, para acceder a los ficheros en los que obren datos necesarios para su actuación de la Agencia Estatal de Administración Tributaria, la Tesorería General de la Seguridad Social y el Instituto Nacional de Estadística, este último en lo relativo al padrón municipal de habitantes, lo cual ha de realizarse de acuerdo con la legislación sobre protección de datos sin que sea preciso el consentimiento del interesado. Al respecto, conviene hacer notar que la mención del precepto a los procedimientos administrativos tramitados en el ámbito de la Ley Orgánica de derechos y libertades de los extranjeros no puede entenderse sino haciendo referencia a la tramitación de un determinado expediente en el que resulta necesaria la constancia de determinado dato que ya obra en poder de otro órgano de la Administración General del Estado, tratándose así de un acceso específico en cada caso ajustado a los datos que resulten precisos para la tramitación de un expediente determinado y no de un acceso masivo o indiscriminado. La finalidad de esa cesión no es otra que comunicar el contenido de ficheros con datos tributarios, de Seguridad Social o de residencia, datos que, en cualquier caso, son ya previamente conocidos por la Administración General del Estado, atendiendo a la necesidad de que la misma disponga de la información oportuna para la gestión de procedimientos en materia de extranjería que son también de su competencia. Por ello, en la medida en que han de tratarse de datos relacionados con un concreto procedimiento y que ya obran en poder de la Administración pública, no puede considerarse vulnerado el art. 18.4 CE. En todo caso, como ya hemos señalado, tal acceso solamente puede producirse cuando ese dato resulte necesario o pertinente en relación con la tramitación de un concreto expediente, lo que permite analizar o determinar en cada caso la conformidad del acceso con lo establecido en el régimen legal que le resulta de aplicación.

Así, rectamente interpretada en los términos antes expuestos, resulta que esa cesión de datos que el acceso previsto supone ha de realizarse de acuerdo con lo que al respecto disponga la Ley Orgánica de protección de datos lo que determina, no solamente la aplicación de lo que la misma dispone en materia de información al interesado respecto de la cesión de datos (art. 5.4 LOPD), sino también que la cesión, establecida en una norma legal [art.11.2.a) LOPD], se produce para el cumplimiento de finalidades legítimas del órgano cedente y del cesionario (art. 4.1 LOPD), finalidades que, desde el punto de vista material, no resultan ser incompatibles entre sí (art. 4.2 LOPD), sino que, por el contrario, los datos son comunicados para el cumplimiento de fines directamente relacionados con las funciones legítimas de cedente y cesionario que contribuyen a garantizar un bien de relevancia constitucional: dar cumplimiento a lo dispuesto en la ley, en este caso la de extranjería (arts. 10.1 y 13.1 CE)".

Por consiguiente, deben suprimirse el artículo 54.3, 55.3 y la disposición transitoria única del Anteproyecto, estableciendo la obligación de los trabajadores por cuenta ajena y los voluntarios de aportar períodicamente a su empleador u organización dedicada a labores de voluntariado, al menos cada dos años, una certificación negativa del Registro Central de Delincuentes Sexuales y de Trata de Seres Humanos.