N/REF: 0046/2021

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente al Anteproyecto de Ley General de Telecomunicaciones, solicitado 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 anteproyecto transpone al ordenamiento jurídico español la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas, regulando el régimen general de las telecomunicaciones, compendiando la normativa vigente, actualizando aquellos aspectos que han sufrido importantes modificaciones desde la aprobación de la anterior Ley General del año 2014 y sentando las bases para el despliegue de las redes de muy alta capacidad. De este modo, introduce reformas estructurales en el régimen jurídico de las telecomunicaciones, a fin de fomentar la inversión de los operadores en redes de muy alta capacidad, mejorar la protección de los derechos de los usuarios y actualizar, entre otras, la normativa sobre Servicio Universa, gestión del espectro y seguridad de las redes, contribuyendo a la vertebración del territorio y a la lucha contra la despoblación y el cambio climático.

I

La Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas, refunde en un único texto el paquete de Directivas comunitarias aprobadas en el año 2002 y modificadas en el año

2009, que forman parte del marco regulador para las redes y servicios de comunicaciones electrónicas (Directivas acceso, autorización, marco y servicio universal) con excepción de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), que se mantiene en vigor en tanto no se proceda a la aprobación del conocido como Reglamento Eprivacy.

Por consiguiente, tal y como señala el Considerando 15 de la Directiva (UE) 2018/1972 *"El tratamiento de datos personales mediante servicios de comunicaciones electrónicas, contra remuneración o de otro modo, debe ajustarse al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo"*, sin perjuicio de las especificaciones que, como norma especial aplicable a las comunicaciones electrónicas, se contienen en la Directiva 2002/58/CE.

A este respecto, el propio RGPD en su Considerando 173, dispone que *"El presente Reglamento debe aplicarse a todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales en relación con el tratamiento de datos personales que no están sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, incluidas las obligaciones del responsable del tratamiento y los derechos de las personas físicas. Para aclarar la relación entre el presente Reglamento y la Directiva 2002/58/CE, esta última debe ser modificada en consecuencia. Una vez que se adopte el presente Reglamento, debe revisarse la Directiva 2002/58/CE, en particular con objeto de garantizar la coherencia con el presente Reglamento."*

Y en el artículo 95 se refiere a la relación del RGPD con la Directiva 2002/58/CE, señalando lo siguiente:

El presente Reglamento no impondrá obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación de la Unión en ámbitos en los que estén sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE.

Por lo tanto, la Directiva 2002/58/CE mantiene, en relación con el RGPD, el carácter de norma especial que tenía con la Directiva 95/46/CE, tal y como se reconoce en su Considerando 10 *("En el sector de las comunicaciones electrónicas es de aplicación la Directiva 95/46/CE, en particular para todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales que no están cubiertas de forma específica por las disposiciones de la presente Directiva, incluidas las obligaciones del*

responsable del tratamiento de los datos y los derechos de las personas. La Directiva 95/46/CE se aplica a los servicios de comunicaciones electrónicas que no sean de carácter público.), y en su artículo 1, relativo al ámbito de aplicación y objetivo, en el que después de disponer en su apartado 1 que *"La presente Directiva establece la armonización de las disposiciones nacionales necesaria para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad y la confidencialidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad"* añade en su apartado 2 que *"Las disposiciones de la presente Directiva especifican y completan la Directiva 95/46/CE a los efectos mencionados en el apartado 1."*

Por lo tanto, la Directiva 2002/58/CE y, consecuentemente, los preceptos del presente anteproyecto que transponen dicha Directiva, vienen a configurar un régimen especial, al que se someterían únicamente los tratamientos que la misma regula, frente al régimen general de protección de datos que se recoge en el RGPD. Por este motivo, las disposiciones del mismo serán de aplicación a todos los tratamientos llevados a cabo dentro del ámbito de aplicación del derecho de la Unión y que no estén regulados específicamente por la Directiva, tal y como se desprende del ámbito de aplicación establecido en el artículo 2 del Reglamento y en los términos que especifica su artículo 95. Asimismo, dicho carácter de norma especial es igualmente predicable respecto de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), cuyas disposiciones deben ser tenidas en cuenta al constituir la "lex generalis" aplicable para garantizar el derecho fundamental a la protección de datos de carácter personal.

Partiendo de lo anterior, el presente informe se centrará, por un lado, en el análisis de aquellos preceptos que son transposición de la Directiva 2002/58/UE y, por otro, en aquellos que, siendo transposición de la Directiva (UE) 2018/1972, afectan al tratamiento de datos personales. Asimismo, se analizará el régimen sancionador establecido por dicha normativa en cuanto afecte a las competencias de esta Agencia.

Para la emisión del presente informe se han tenido en cuenta los criterios que ha mantenido esta Agencia en informes anteriores, como el informe 49/2011, referente al Anteproyecto de Ley por la que se modifica la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones y en el informe 21/2013 referente al Anteproyecto de Ley General de Telecomunicaciones.

II

Dada su trascendencia para esta Agencia, se considera conveniente comenzar con el análisis de las competencias que corresponden a la Agencia

Española de Protección de Datos (AEPD) en cuanto autoridad de control competente en materia de protección del derecho fundamental a la protección de datos personales, ya que, como reiteradamente ha venido señalando esta Agencia, la regulación contenida en el anteproyecto tiene una incidencia fundamental en la aplicación de la normativa de protección de datos de carácter personal y en la actuación de la AEPD, como ocurre, significativamente, en materia de seguridad de las redes, en particular el artículo 60, y en los distintos derechos de los usuarios regulados en los artículos 65 y 66.

A este respecto, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales dispone en su artículo 47 lo siguiente:

> *Corresponde a la Agencia Española de Protección de Datos supervisar la aplicación de esta ley orgánica y del Reglamento (UE) 2016/679 y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del mismo reglamento, en la presente ley orgánica y en sus disposiciones de desarrollo.*
>
> ***Asimismo, corresponde a la Agencia Española de Protección de Datos el desempeño de las funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea**.*

En relación con estas últimas competencias, recuerda el Preámbulo del Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos que:

> *Por otro lado, hay que tener en cuenta que la Agencia Española de Protección de Datos no solo ejerce las competencias derivadas del Reglamento, sino que también ejercerá las que establece la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Igualmente ejerce actualmente las potestades derivadas de la Directiva 2002/58 del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, que en la actualidad se recogen en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, **y en la legislación en materia de telecomunicaciones.***

En este sentido, la legislación sobre telecomunicaciones ha venido atribuyendo a la Agencia Española de Protección de Datos, en cuanto

autoridad nacional competente para la protección del derecho fundamental a la protección de datos, competencias para velar por el adecuado cumplimiento de los derechos derivados de dicho derecho fundamental, competencias que se mantienen en el texto objeto de informe y a las que posteriormente se hará referencia.

A este respecto, los apartados 2 y 3 del artículo 15 bis de la Directiva 2002/58/CE, introducidos por la Directiva 2009/136/CE disponen que:

> *"2. Sin perjuicio de los posibles recursos judiciales existentes, los Estados miembros velarán por que la autoridad nacional competente y, cuando proceda, otros organismos nacionales, tengan potestad para solicitar el cese de las infracciones mencionadas en el apartado 1.*
>
> *3. Los Estados miembros velarán por que las autoridades nacionales competentes y, cuando proceda, otros organismos nacionales, dispongan de las competencias y recursos necesarios en materia de investigación, incluida la facultad de obtener cualquier información pertinente que pudieran necesitar para supervisar y aplicar las disposiciones nacionales adoptadas de conformidad con la presente Directiva."*

Por consiguiente, ostentando esta Agencia la consideración de autoridad nacional con competencias específicas para velar por la adecuada aplicación de la normativa sobre protección de datos personales en el ámbito de las telecomunicaciones, debería incluirse a la misma en la enumeración de autoridades públicas competentes específicas en materia de telecomunicaciones contenida en el artículo 98.1 del anteproyecto, añadiendo una letra c) que se refiere a la Agencia Española de Protección de Datos en el ejercicio de las competencias que se le ha asignado en materias reguladas por esta Ley.

Por otro lado, y al objeto de perfilar las competencias de las distintas autoridades específicas, debe hacerse referencia a la competencia que el artículo 99 atribuye a los órganos superiores y directivos del Ministerio de Asuntos Económicos y Transformación Digital en su letra c):

> *c) Ejercer las competencias que en materia de acceso a las redes y recursos asociados, interoperabilidad e interconexión le atribuye la presente Ley y su desarrollo reglamentario, en particular, en los siguientes supuestos:*
> *[…]*
> *2. Cuando se haga necesario para garantizar el cumplimiento de la normativa sobre datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas*.

Dicha competencia debe entenderse sin perjuicio de las que corresponde a esta Agencia, por lo que debería añadirse al apartado 2 la frase **“sin perjuicio de las competencias que corresponden a la Agencia Española de Protección de Datos”.**

Por las mismas razones, el procedimiento extrajudicial de controversias al que se refiere el artículo 78 del anteproyecto, competencia del Ministerio de Asuntos Económicos y Transformación Digital, referido a los derechos específicos de los usuarios finales de servicios de comunicaciones electrónicas reconocidos en la ley y en su normativa debe entenderse sin perjuicio de las competencias de esta Agencia, en el supuesto en que se refiera a los derechos derivados de la garantía del derecho fundamental a la protección de datos personales. Por ello, debería añadirse un nuevo apartado con la siguiente redacción:

Lo establecido en el presente artículo se entiende, en los supuestos en que se refieran al derecho a la protección de datos personales, sin perjuicio del derecho de los usuarios finales a presentar una reclamación ante la Agencia Española de Protección de Datos.

Por otro lado, y desde una perspectiva general de las competencias de esta Agencia, debe recordarse que, en relación con los derechos digitales regulados en el Título X de la Ley Orgánica 3/2018, a los que se refiere expresamente la disposición adicional decimoquinta del anteproyecto, las mismas se limitan a los derechos recogidos en los artículos 89 a 94 de dicha ley orgánica, tal y como reconoce expresamente al artículo 2.1. de la misma.

II

Por lo que se refiere a las competencias específicas que el anteproyecto reconoce a la AEPD, debe comenzarse por el análisis del artículo 60 del anteproyecto de ley, que bajo la rúbrica de “Protección de los datos de carácter personal”, transpone el artículo 4 de la Directiva 2002/58/UE relativo a la “Seguridad del tratamiento” y en el que se identifican las medidas de seguridad, que como mínimo, deben adoptar los operadores. A este respecto, ya en nuestro informe 49/2011, reiterado en el 21/2013, se manifestaba que dichas medidas han de ser consideradas las “mínimas“ a implantar, “sin perjuicio” de la aplicación de la normativa general de protección de datos personales, de tal modo que los operadores, además de aplicar las medidas de seguridad expresamente contenidas en el artículo 60, deberán cumplir con las exigencias de seguridad previstas en dicha normativa general, y en este sentido debe entenderse la remisión del apartado 4:

4. Lo dispuesto en el presente artículo será sin perjuicio de la aplicación 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 y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y su normativa de desarrollo.

A este respecto hay que destacar que, como indica la Exposición de motivos de la Ley 3/2018 "la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan". De este modo, el cambio de aproximación de la normativa de protección de datos implica necesariamente una modificación en el enfoque que habrá de darse a las medidas de seguridad, en que se evoluciona de un modelo de lista de cumplimiento a otro de análisis de riesgo y de impacto en la protección de datos, basado en una gestión continua del riesgo partiendo del análisis de riesgos al que se refiere el artículo 24.1 del RGPD al disponer que *"Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario"*.

Esta previsión se completa con lo señalado en el considerando 75 del Reglamento, según el cual *"Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos*

personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados".

A su vez, en relación con la seguridad del tratamiento, el artículo 32.1 establece que *"Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo".*

Por otro lado, una de las especificidades de la Directiva 2002/58/UE, tras su modificación por la Directiva 136/2009, fue la de regular los supuestos de violación de los datos personales, estableciendo una obligación de notificación a la autoridad nacional competente así como, en determinadas circunstancias, al abonado o particular afectado, careciendo la Directiva 95/46/CE de previsiones al respecto.

Sin embargo, en el momento actual, el RGPD ha procedido a regular con carácter general, dentro de la normativa dedicada a la seguridad de los datos personales, tanto la notificación de una violación de la seguridad de los datos personales a la autoridad de control (artículo 33) como la comunicación de una violación de la seguridad de los datos personales al interesado (artículo 34), que dado su carácter de norma general, será aplicable en todo aquello que específicamente no esté previsto en la norma especial, como ocurre, por ejemplo, respecto del contenido mínimo de la notificación a la autoridad de control que regula el apartado 3 del artículo 33 del RGPD, por lo que se propone que el párrafo primero del apartado 3 del artículo 60 se redacte de la siguiente forma:

> 3. En caso de violación de los datos personales, el operador de servicios de comunicaciones electrónicas disponibles al público notificará sin dilaciones indebidas dicha violación a la Agencia Española de Protección de Datos, **en la forma señalada en el apartado 3 del artículo 33 del RGPD.**

Asimismo, debe tenerse en cuenta que la Ley Orgánica 3/2018, además de reforzar la independencia de la Agencia, le ha atribuido la potestad de dictar circulares que serán obligatorias una vez publicadas en el Boletín Oficial del Estado.

Esta nueva potestad debería reconocerse en el último párrafo del apartado 3 del artículo 60, que transpone el apartado 4.4. párrafo primero, de la Directiva 2002/58/CE, proponiéndose la siguiente redacción:

> La Agencia Española de Protección de Datos podrá adoptar directrices y, en caso necesario, dictar **circulares** sobre las circunstancias en que se requiere que el operador notifique la violación de los datos personales, sobre el formato que debe adoptar dicha notificación y sobre la manera de llevarla a cabo, con pleno respeto a las disposiciones que en su caso sean adoptadas en esta materia por la Comisión Europea.

III

Por otro lado, las competencias que el artículo 60 del anteproyecto atribuye a la AEPD en relación con las violaciones de seguridad no se corresponden con las competencias sancionadoras que a la misma se atribuyen en el artículo 115.3 del anteproyecto.

A este respecto, ya en el informe 21/2013 se destacaba la necesidad de sancionar adecuadamente el incumplimiento de las obligaciones recogidas en la Directiva 2002/58/CE:

> *Como punto de partida debe recordarse nuevamente que la imposición de sanciones como consecuencia del incumplimiento de las previsiones que en el derecho nacional vengan a transponer la Directiva 2002/58/CE viene expresamente impuesto por su artículo 15 bis, al establecer que "Los Estados miembros determinarán el régimen de sanciones — incluidas las sanciones penales, cuando proceda — aplicable en caso de incumplimiento de las disposiciones nacionales adoptadas en virtud de la presente Directiva y adoptarán todas las medidas necesarias para garantizar su aplicación. Las sanciones que se prevean serán efectivas, proporcionadas y disuasorias y podrán ser aplicadas para cubrir el período de cualquier infracción, aún cuando se haya corregido posteriormente esta infracción. Los Estados miembros notificarán dichas disposiciones a la Comisión, a más tardar, el 25 de mayo de 2011 y le comunicarán sin demora cualquier modificación ulterior de las mismas". De este modo, la inexistencia de disposiciones sancionadoras del régimen contenido en las normas de transposición de dicha Directiva implicaría una insuficiente plasmación de aquélla.*

Asimismo, dicho informe destacaba la inexistencia de un régimen sancionador concreto en relación con la vulneración del deber de notificación de violaciones de protección de datos personales, que únicamente podría incardinarse en las previsiones del artículo 78.10 del anteproyecto entonces informado, que posteriormente sería el artículo 78.11 de la Ley General de Telecomunicaciones de 2013: *"El incumplimiento de las obligaciones de*

servicio público, de las obligaciones de carácter público y la vulneración de los derechos de los consumidores y usuarios finales, según lo establecido en el Título III de la Ley y su normativa de desarrollo".

Y a este respecto en el citado informe se decía que

"La primera cuestión que cabe plantearse de la lectura del precepto es la de si la ausencia de notificación constituirá efectivamente una vulneración de las obligaciones de servicio público establecidas en el Título III. A tal efecto, esta Agencia considera que la conducta debería ser constitutiva de una tipificación específica".

Por ello, y para clarificar adecuadamente el marco competencial, se insiste en la conveniencia de tipificar específicamente las conductas contrarias a las obligaciones impuestas por el artículo 60 del anteproyecto, debiendo corresponder la competencia sancionadora a esta Agencia. A este respecto, teniendo en cuenta que la Ley Orgánica 3/2018 tipifica como infracción grave, en su artículo 73, letra f) *"La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679"*, en la letra r) *"El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679"* y en la letra s) *"El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 34 del Reglamento (UE) 2016/679 si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación"*, el incumplimiento del deber de adopción de las medidas técnicas y organizativas adecuadas, así como del deber de notificación previsto en el artículo 60 del anteproyecto deberían tipificarse, igualmente, como infracción grave y, teniendo en cuenta, que dichas obligaciones no difieren sustancialmente de las establecidas con carácter general para todos los responsables en el RGPD, remitir a la normativa general para su sanción, proponiéndose **la inclusión de un párrafo 5 en el artículo 60 del siguiente tenor:**

5. El incumplimiento de las obligaciones establecidas en el presente artículo se sancionará de conformidad con lo establecido en el Reglamento (UE) 2016/679, pudiendo ser constitutivo de las infracciones tipificadas en el artículo 73 letras f), r) y s) de la Ley Orgánica 3/2018.

Y, en el supuesto de que no se considere conveniente unificar el régimen sancionador en el presente supuesto, se mantiene la necesidad de tipificar

adecuadamente dichas conductas en el anteproyecto, atribuyendo la competencia sancionadora a la AEPD, **añadiendo una nueva letra en el artículo 108 con la siguiente redacción:**

> **La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, o el incumplimiento de los deberes de notificación de una violación de la seguridad de los datos, en los términos exigidos por el artículo 60.**

Asimismo, debe modificarse el artículo 115.3 para incluir dicho supuesto de infracción grave entre las que son competencia de la AEPD.

IV

Para concluir con el análisis de las competencias de la AEPD, debe hacerse referencia a las infracciones de la normativa de telecomunicaciones que, por afectar al derecho fundamental a la protección de datos personales, deben ser competencia de esta Agencia, y que comprendería:

- El incumplimiento de las obligaciones del artículo 60, en los términos señalados en el apartado anterior, y que debe ser objeto de tipificación específica como infracción grave en el caso de no remitirse a la normativa general.

- La vulneración de los derechos de los consumidores y usuarios finales, según lo establecido en el título III de la Ley y su normativa de desarrollo, incluidos los derechos de conservación de número, de itinerancia en la Unión Europea e internacional, en materia de comunicaciones intracomunitarias reguladas y acceso abierto a internet, tipificada como infracción grave en el apartado 30 del artículo 108.

- El incumplimiento de las obligaciones de carácter público, según lo establecido en el Título III de la Ley y su normativa de desarrollo, tipificada como infracción leve en el apartado 12 del artículo 109.

  En estos dos últimos supuestos, cuando se vulneren los derechos de los usuarios finales sobre protección de datos y privacidad reconocidos en los artículos 65 y 66.

Por ello, debería modificarse el artículo 115.3 para adaptarse a las competencias de la AEPD, proponiéndose la siguiente redacción:

A la Agencia Española de Protección de Datos, en el caso de que se trate de las infracciones graves del artículo 108 tipificadas en el apartado

XX y de las infracciones graves del artículo 108 tipificadas en el apartado 28 y de las infracciones leves del artículo 108 tipificadas en el apartado 12 cuando se vulneren los derechos de los usuarios finales sobre protección de datos y privacidad reconocidos en los artículos 65 y 66.

V

En lo que se refiere a la regulación de los derechos de los usuarios finales y consumidores que se contiene en el Capítulo IV del Título III, y por lo que se refiere al derecho fundamental a la protección de datos personales, debe comenzarse haciéndose referencia a la exclusión de las microempresas que se contiene en el apartado 2 del artículo 64:

> 2. Los operadores que suministren redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público estarán obligados a respetar los derechos reconocidos en este capítulo, a excepción de las microempresas que presten servicios de comunicaciones interpersonales independientes de la numeración, salvo que también presten otros servicios de comunicaciones electrónicas. Estas microempresas deben informar a los usuarios finales y consumidores antes de celebrar un contrato que se benefician de esta excepción y que, por tanto, no están obligadas a respetar los derechos reconocidos en este capítulo.

Dicha exclusión encuentra su fundamento en la Directiva 2018/1972, que después de señalar en su Considerando 255 que *"De conformidad con el principio de proporcionalidad, una serie de disposiciones sobre los derechos de los usuarios finales en la presente Directiva no deben aplicarse a las microempresas que prestan únicamente servicios de comunicaciones interpersonales independientes de la numeración. Según la jurisprudencia del Tribunal de Justicia, la definición de «pequeña o mediana empresa», que incluye las microempresas, debe ser interpretada de forma estricta. Para incluir solo a las empresas que sean microempresas efectivamente independientes, es necesario analizar la estructura de las microempresas que formen un grupo económico, cuyo peso supera el de una microempresa, y asegurarse de que la definición de «microempresa» no se eluda por medios puramente formales"*, dispone en su artículo 98, primero del Título III dedicado a los derechos de los usuarios finales que *"El presente título, con excepción de los artículos 99 y 100, no se aplicará a las microempresas que presten servicios de comunicaciones interpersonales independientes de la numeración salvo que también presten otros servicios de comunicaciones electrónicas".*

Por consiguiente, de acuerdo con el propio precepto, dentro de los artículos que no se excluyen de su aplicación a la microempresas se encuentra el artículo 100, relativo a las *Salvaguardias de derechos fundamentales*:

> *1. Las medidas nacionales relativas al acceso o al uso por parte de los usuarios finales de los servicios y las aplicaciones a través de redes de comunicaciones electrónicas respetarán la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta») y los principios generales del Derecho de la Unión.*
> *2. Cualquier medida relativa al acceso o al uso por parte de los usuarios finales de los servicios y las aplicaciones a través de redes de comunicaciones electrónicas, que sea susceptible de limitar el ejercicio de los derechos y libertades reconocidos en la Carta solo podrá imponerse si está prevista por ley y respeta tales derechos o libertades, es proporcionada, necesaria, y responde efectivamente a objetivos de interés general reconocidos por el Derecho de la Unión o a la necesidad de protección de los derechos y libertades de los demás en línea con el artículo 52, apartado 1, de la Carta y con los principios generales del Derecho de la Unión, que incluyen el derecho a la tutela judicial efectiva y a un juicio justo. Por lo tanto, dichas medidas solo podrán ser adoptadas respetando debidamente el principio de presunción de inocencia y el derecho a la intimidad. Se garantizará un procedimiento previo, justo e imparcial, que incluirá el derecho de los interesados a ser oídos, sin perjuicio de que concurran las condiciones y los arreglos procesales adecuados en los casos de urgencia debidamente justificados, de conformidad con la Carta.*

Por otro lado, ya se ha indicado que la citada Directiva 2018/1972, del Parlamento Europeo y del Consejo, de 11 de diciembre, por la que se establece el Código Europeo de Comunicaciones Electrónicas, refunde en un único texto el paquete de Directivas comunitarias aprobadas en el año 2002 y modificadas en el año 2009, que forman parte del marco regulador para las redes y servicios de comunicaciones electrónicas (Directivas acceso, autorización, marco y servicio universal) con excepción de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

Y la Directiva 2002/58/CE, que no se ve afectada por la Directiva 2018/1972, no contempla la exclusión de su ámbito de aplicación de las microempresas, como tampoco se contempla en el RGPD.

A este respecto, debe atenderse a la definición ampliada de servicio de comunicaciones electrónicas, que justificaría dicha exclusión, tal y como señala la MAIN (la negrita es nuestra):

Asimismo, como importante novedad, para asegurar que el alcance del marco regulatorio se mantenga al ritmo de los desarrollos tecnológicos y del mercado y que los prestadores de servicios similares quedan sometidos a una similar carga regulatoria (level playing field), se establece que la definición de servicio de comunicación electrónica bajo el Código cubre:

servicios de acceso a internet;
servicios de comunicaciones interpersonales (SCI) y
servicios que consisten total o principalmente en el transporte de señales.

La inclusión de los servicios de comunicaciones interpersonales es un cambio clave. Estos son servicios que permiten intercambios interactivos e interpersonales de información a través de redes de comunicaciones electrónicas entre un número finito de personas donde el remitente determina los destinatarios. Esto podría incluir llamadas de voz, correos electrónicos y servicios de mensajería. Este cambio permitirá que servicios prestados a través de Internet, comúnmente llamados "over the top" o servicios OTT, entren dentro del alcance del régimen regulatorio, previéndose, sin embargo, la excepción de aquellos servicios en los que el elemento de comunicación constituya una característica secundaria y auxiliar.

En virtud del Código, las obligaciones de los SCI basados en numeración, se igualan a las de los operadores tradicionales en múltiples materias (protección de la privacidad, ILC, protección del consumidor, restricciones a la transmisión de contenido dañino o ilegal, tasas). Los SCI independientes de la numeración quedan sujetos a menores obligaciones, especialmente cuando se trata de microempresas.

Por otro lado, cualquier limitación del derecho fundamental a la protección de datos personales requeriría no solo de una norma con rango de ley que así lo prevea, conforme a lo previsto en el artículo 53 de nuestra Constitución, sino que además, y según reiterada doctrina constitucional a la que más adelante se hará referencia, que dicha limitación se adopte 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, cautelas que, como puede observarse, se corresponden con las previstas en el artículo 100 de la Directiva 2018/1972.

Por todo ello, la exclusión general de las microempresas respecto de los derechos de los usuarios finales y consumidores derechos en ningún caso puede afectar al derecho fundamental a la protección de datos personales. Por la misma razón, tampoco es admisible dicha exclusión general respecto de las

empresas, autoridades públicas o usuarios finales a los que se refiere el segundo párrafo del apartado 2 del artículo 64:

> Tampoco están obligados a respetar los derechos reconocidos en este capítulo las empresas, autoridades públicas o usuarios finales que suministren el acceso a una red pública de comunicaciones electrónicas a través de RLAN, cuando dicho suministro no forme parte de una actividad económica o sea accesorio respecto de otra actividad económica o un servicio público que no dependa del transporte de señales por esas redes.

Por lo tanto, dicha exclusión no puede entenderse en el sentido de que no deba respetarse el derecho fundamental a la protección de datos personales, sino que no debe serlo en los términos específicos regulados en el anteproyecto, lo que, atendiendo al carácter de ley especial de esta normativa y según lo señalado anteriormente, implicará que queden sujetas al régimen general de RGPD y la LOPDGDD en la medida en que afecte al tratamiento de datos de carácter personal.

Por consiguiente, debería incluirse un apartado tercero en el apartado 2 del artículo 64 con la siguiente redacción:

> **Las excepciones contempladas en el presente apartado lo serán sin perjuicio de la aplicación 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 y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y su normativa de desarrollo.**

VI

En cuanto a la regulación específica de dichos derechos, el anteproyecto mantiene, con carácter general, la misma redacción de la vigente Ley General de Telecomunicaciones, salvo algunas modificaciones puntuales, debiendo destacarse, tal y como se señalaba en el informe 21/2013, que afectan al derecho fundamental a la protección de datos personales no solo los contemplados expresamente bajo la rúbrica “Derecho a la protección de datos personales y la privacidad en relación con las comunicaciones no solicitadas, con los datos de tráfico y de localización y con las guías de abonados” (artículo 66 del anteproyecto), sino también algunos de los incluidos entre los “Derechos

específicos de los usuarios finales y consumidores de redes y servicios de comunicaciones electrónicas disponibles al público", como son el derecho a detener el desvío automático de llamadas efectuado a su terminal por parte de un tercero; el derecho a impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de su línea en las llamadas que genere o la presentación de la identificación de su línea al usuario que le realice una llamada; el derecho a impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen en las llamadas entrantes y a rechazar las llamadas entrantes en que dicha línea no aparezca identificada (artículo 65 del anteproyecto, letras n, ñ y o).

Por otro lado, es destacable la remisión que, en cuanto al concepto de consentimiento, se hace al RGPD en el apartado 5 del artículo 66, en cuanto norma general aplicable, a la que ya se remitía la letra f) del artículo 2 de la Directiva 2002/58/CE.

El artículo 4.11 del RGPD define el «consentimiento del interesado» como *"toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".*

Dicho precepto no hace sino recoger los requisitos de un consentimiento válido que se habían venido perfilando por el Grupo del 29, especialmente en su Dictamen 15/2011 sobre la definición del consentimiento, garantizando que el interesado tenga el control sobre sus datos. Como señalaba el Grupo del 29 en sus Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 adoptadas el 28 de noviembre de 2017 y se ha recogido en las recientes Directrices del Comité Europeo de Protección de Datos 05/2020 sobre el consentimiento con arreglo al Reglamento 2016/679, de 4 de mayo de 2020, si no se cumple plenamente con el RGPD "el control del interesado será meramente ilusorio y el consentimiento no será una base jurídica válida para el tratamiento, lo que convertirá dicha actividad de tratamiento en una actividad ilícita", teniendo en cuenta, además, que "los requisitos estipulados en el RGPD para obtener un consentimiento válido se aplican a situaciones que entran dentro del ámbito de aplicación de la Directiva sobre la privacidad y las comunicaciones electrónicas".

VII

Por otro lado, debe hacerse referencia a la obligación de los operadores de poner a disposición de las autoridades receptoras de las comunicaciones de emergencia de la información relativa a la ubicación de las personas que efectúan dicha comunicación que se establece en el artículo 74.2 del anteproyecto:

> 2. Los operadores de servicios de comunicaciones interpersonales disponibles al público basados en numeración, cuando dichos servicios permitan realizar llamadas a un número de un plan de numeración nacional o internacional, tienen la obligación de encaminar gratuitamente las comunicaciones de emergencia a los servicios de emergencia cuando se utilice el número de emergencia 112 u otros números de emergencia que se determinen.
> Asimismo, los operadores citados pondrán a disposición de las autoridades receptoras de dichas comunicaciones de emergencia la información que mediante real decreto se determine relativa a la ubicación de las personas que efectúan la comunicación de emergencia, inmediatamente después del establecimiento de dicha comunicación. El establecimiento y la transmisión de la información relativa a la localización del llamante es gratuita tanto para el llamante como para las autoridades receptoras de dichas comunicaciones de emergencia cuando se utilice el número de emergencia 112 u otros números de emergencia que se determinen.
> Mediante real decreto se establecerán criterios para la precisión y la fiabilidad de la información facilitada sobre la ubicación de las personas que efectúan comunicaciones de emergencia a los servicios de emergencia.

En este punto, hay que tener en cuenta lo dispuesto en el artículo 109.6 de la Directiva 2018/1972, del Parlamento Europeo y del Consejo, de 11 de diciembre, por la que se establece el Código Europeo de Comunicaciones Electrónicas:

> 6.Los Estados miembros velarán por que la información relativa a la ubicación de las personas que efectúan llamadas se ponga a disposición del PSAP más indicado inmediatamente tras el establecimiento de la comunicación de emergencia. Dicha información incluye los datos sobre ubicación de la red y, si están disponibles, los datos relativos a la localización del llamante procedentes del dispositivo móvil. Los Estados miembros garantizarán que el establecimiento y la transmisión de la información relativa a la localización del llamante sea gratuita para este último y para el PSAP con respecto a todas las comunicaciones de emergencia al número único europeo de emergencia «112». Los Estados miembros podrán ampliar el ámbito de dicha obligación de modo que abarque las comunicaciones de emergencia a números nacionales de emergencia. Las autoridades de reglamentación competentes, en caso necesario previa consulta al ORECE, establecerán criterios para la precisión y la fiabilidad de la información facilitada sobre la localización del llamante.

Respecto de la importancia de disponer de los datos de localización procedentes del terminal del afectado cuando se efectúan llamadas a los servicios de emergencia se pone de manifiesto en el Considerando 290 de dicha Directiva:

> "La información sobre la localización del llamante, aplicable a todas las comunicaciones de emergencia, mejora el nivel de protección y seguridad de los usuarios finales y facilita a los servicios de emergencia el ejercicio de sus funciones, siempre que la transferencia a los servicios de emergencia correspondientes de la comunicación de emergencia y de los datos asociados esté garantizada por el sistema nacional de PSAP. La recepción y el uso de esta información sobre la localización del llamante, que incluye tanto la información relativa a la ubicación basada en redes como, cuando se disponga de ella, la información relativa a la ubicación basada en el terminal del llamante, debe ajustarse al Derecho de la Unión aplicable sobre el tratamiento de datos personales y medidas de seguridad. Las empresas que aportan la localización basándose en la red deben poner la información sobre la localización del llamante a disposición de los servicios de emergencia tan pronto como la llamada llegue a ese servicio, independientemente de la tecnología utilizada.
>
> No obstante, las tecnologías de localización basadas en el terminal se han demostrado bastante más exactas y rentables debido a la disponibilidad de datos facilitados por el sistema europeo de navegación por complemento geoestacionario, el sistema de satélite Galileo y otros sistemas mundiales de navegación por satélite y datos wifi. Por lo tanto, la información sobre la localización del llamante obtenida del terminal debe complementar la información de localización basada en la red, incluso en caso de que solo se disponga de ella después de establecida la comunicación de emergencia. Los Estados miembros deben velar por que, siempre que sea posible, la localización del llamante obtenida del terminal se ponga a disposición del PSAP más apropiado. Puede que esto no sea posible en algunos casos, por ejemplo cuando la localización no esté disponible en el terminal o a través del servicio de comunicaciones interpersonales empleado, o cuando no es factible técnicamente obtener esta información. Además, los Estados miembros deben garantizar que los PSAP sean capaces de recuperar y gestionar la información disponible sobre la localización del llamante, siempre que resulte factible. El establecimiento y la transmisión de dicha información deben ser gratuitos tanto para el usuario final como para la autoridad encargada de tramitar la comunicación de emergencia, independientemente de cuáles sean los medios de establecimiento (por ejemplo, mediante el terminal o la red) o de transmisión (por ejemplo, a través de un canal de voz, SMS o IP)".

Esta Agencia ha tenido la oportunidad de pronunciarse respecto de dicha cuestión en nuestro Informe 39/2019, respecto de la consulta formulada por el Director General de Protección Civil relativa a cuál sería la base jurídica que determine la licitud del tratamiento de los datos de localización del llamante por teléfono móvil a los servicios de emergencia mediante el empleo de AML (Advance Mobile Location), en la que se señalaba lo siguiente:

> *Tal y como se describe en la misma, AML es un mecanismo, ya desplegado en algunos países, por el que los centros de atención a llamadas de emergencia (servicios 112 y similares, conocidos como PSAP por su siglas en inglés) pueden recibir de forma automática información sobre la ubicación del llamante (cuando éste llama desde un teléfono móvil) con una precisión muy superior a la que puede obtenerse actualmente a través de la información que proporcionan los operadores de telefonía móvil, basada en la ubicación de la estación base desde la que se origina la llamada.*
>
> *AML es independiente del operador, ya que funciona sobre el teléfono móvil (directamente desde el sistema operativo, por lo que no requiere que el usuario descargue una app o realice una configuración previa). Cuando detecta que se está produciendo una llamada a un número de emergencias, AML activa la ubicación del móvil en alta precisión (típicamente obtenida a partir de redes WIFI o Bluetooth cercanas, o de un servicio GNSS, como GPS o Galileo) y genera un mensaje con las coordenadas de la ubicación. El mensaje (que puede ser un SMS, un mensaje de datos, o ambos) es enviado a un número y/o una URL predefinidos para cada país. El servicio se puede configurar para que el mensaje sea reenviado cada cierto tiempo mientras la llamada de voz siga activa.*
>
> *Asimismo, en la consulta se manifiesta que los PSAP en los países donde ya se ha producido el despliegue de AML son unánimes en constatar la mejora que supone para la actuación de los servicios de emergencia, ya que les permite disponer de información mucho más precisa sobre el punto al que deben dirigirse y que en España, los servicios 112, gestionados por las Comunidades Autónomas, son conscientes de estas mejoras y han reclamado repetidas veces que se active el despliegue de AML en nuestro país. Por su parte, la Asociación Europea de Números de Emergencia (EENA, por sus siglas en inglés) fomenta y apoya el despliegue de este sistema y difunde información sobre la tecnología que puede consultarse en su página web https://eena.org/aml/.*

Por otro lado, se indica que el pasado 17 de diciembre de 2018 se publicó en el DOUE la Directiva 2018/1972, del Parlamento Europeo y del Consejo, de 11 de diciembre, por la que se establece el Código Europeo de Comunicaciones Electrónicas (EECC, por sus siglas en inglés), que establece en su artículo 109.6 que:

Los Estados Miembros velaran por que la información relativa a la ubicación de las personas que efectúan llamadas se ponga a disposición del PSAP más indicado inmediatamente tras el establecimiento de la comunicación de emergencia. Dicha información incluye los datos sobre ubicación de la red y, si están disponibles, los datos relativos a la localización del llamante procedentes del dispositivo móvil. Los Estados miembros garantizarán que el establecimiento y la transmisión de la información relativa a la localización del llamante sea gratuita para este último y para el PSAP con respecto a todas las comunicaciones de emergencia al número único europeo de emergencia «112» […]

Por lo que, además del interés y la conveniencia de desplegar el AML por las mejoras que supone en la respuesta a emergencias, existe ahora un imperativo legal para realizar este despliegue en un plazo menor de dos años, a cuyo efecto la Comisión Permanente del Consejo Nacional de Protección Civil ha constituido un Grupo de Trabajo con el objetivo de llevar a cabo las acciones necesarias para desplegar el sistema AML en España.

[…]

III

Partiendo de lo anterior y, tal y como se indica en la consulta y en la página web de EENA, la ventaja esencial que aporta un teléfono inteligente con AML es que reconoce cuándo se realiza una llamada de emergencia y, si aún no está activado, activa el GNSS del teléfono para recopilar la información de ubicación de la persona que llama. Luego, el teléfono envía un SMS automático a los servicios de emergencia con la ubicación de la persona que llama, antes de apagar el GNSS nuevamente. El servicio también puede usar Wi-Fi, según cuál sea mejor en un momento dado.

Por lo tanto, dicho sistemas es mucho más preciso que el empleado en la actualidad, en el que para determinar la ubicación desde la que se realiza la llamada es necesario realizar una búsqueda sobre la red de telefonía que da servicio al llamante, estableciendo únicamente una ubicación aproximada sobre la base de las antenas que están cursando la llamada. Sin embargo, con el mecanismo AML, según

EENA, el sistema es 4.000 veces más preciso que la localización GSM tradicional, con un total del 85% de las llamadas localizadas dentro de un radio de menos de 50 metros, mientras que con la localización mediante la red móvil, el radio puede tener varios kilómetros.

En este sentido, el Dictamen 13/2011 del Grupo del Artículo 29 sobre los servicios de geolocalización en los dispositivos móviles inteligentes ya indicaba que el método de posicionamiento mediante datos de estaciones bases "da una idea rápida y general de la ubicación, pero no es muy preciso en comparación con los datos GPS y Wifi. La precisión es de aproximadamente 50 metros en las zonas urbanas densamente pobladas y de hasta varios kilómetros en las zonas rurales", mientras que la tecnología GPS "ofrece un posicionamiento exacto, de entre 4 y 15 metros".

De ahí que varios países hayan implementado ya esta tecnología (según la página web de EENA, a fecha de junio de 2019 lo tendrían implementado Austria, Bélgica, Estonia, Finlandia, Islandia, Irlanda, Lituania, Moldavia, Países Bajos, Nueva Zelanda, Noruega, Eslovenia, Emiratos Árabes Unidos, Reino Unido y Estados Unidos) y las autoridades europeas promuevan el empleo de la misma, tal y como se recoge en el artículo 109.6 de la Directiva 2018/1972, del Parlamento Europeo y del Consejo, de 11 de diciembre, por la que se establece el Código Europeo de Comunicaciones Electrónicas (ya transcrito) y se fundamenta en su Considerando 290:

"La información sobre la localización del llamante, aplicable a todas las comunicaciones de emergencia, mejora el nivel de protección y seguridad de los usuarios finales y facilita a los servicios de emergencia el ejercicio de sus funciones, siempre que la transferencia a los servicios de emergencia correspondientes de la comunicación de emergencia y de los datos asociados esté garantizada por el sistema nacional de PSAP. La recepción y el uso de esta información sobre la localización del llamante, que incluye tanto la información relativa a la ubicación basada en redes como, cuando se disponga de ella, la información relativa a la ubicación basada en el terminal del llamante, debe ajustarse al Derecho de la Unión aplicable sobre el tratamiento de datos personales y medidas de seguridad. Las empresas que aportan la localización basándose en la red deben poner la información sobre la localización del llamante a disposición de los servicios de emergencia tan pronto como la llamada llegue a ese servicio, independientemente de la tecnología utilizada.

No obstante, las tecnologías de localización basadas en el terminal se han demostrado bastante más exactas y rentables debido a la disponibilidad de datos facilitados por el sistema europeo de

navegación por complemento geoestacionario, el sistema de satélite Galileo y otros sistemas mundiales de navegación por satélite y datos wifi. Por lo tanto, la información sobre la localización del llamante obtenida del terminal debe complementar la información de localización basada en la red, incluso en caso de que solo se disponga de ella después de establecida la comunicación de emergencia. Los Estados miembros deben velar por que, siempre que sea posible, la localización del llamante obtenida del terminal se ponga a disposición del PSAP más apropiado. Puede que esto no sea posible en algunos casos, por ejemplo cuando la localización no esté disponible en el terminal o a través del servicio de comunicaciones interpersonales empleado, o cuando no es factible técnicamente obtener esta información. Además, los Estados miembros deben garantizar que los PSAP sean capaces de recuperar y gestionar la información disponible sobre la localización del llamante, siempre que resulte factible. El establecimiento y la transmisión de dicha información deben ser gratuitos tanto para el usuario final como para la autoridad encargada de tramitar la comunicación de emergencia, independientemente de cuáles sean los medios de establecimiento (por ejemplo, mediante el terminal o la red) o de transmisión (por ejemplo, a través de un canal de voz, SMS o IP)".

Por tanto, el tratamiento del dato de localización se encontraría amparado en la letra d) del artículo 6.1. del RGPD: el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, independientemente de quién realice dicho tratamiento, ya que en este caso el factor determinante de la licitud del tratamiento es la protección de un interés esencial para la vida, tal y como destaca el Considerando 46:

"El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano".

En este sentido se he venido pronunciando esta Agencia en relación con los servicios prestados a través del 112, atendiendo a la necesaria protección de intereses vitales, sin que la nueva regulación contenida en

el RGPD suponga, en este punto, novedad alguna respecto al régimen anterior. Así, en el Informe 438/2015 se realizaba un análisis detallado de la cuestión que por su importancia se transcribe a continuación:

[…]

Igualmente, esta Agencia viene fundamentando, reiteradamente, en la necesaria protección de intereses vitales del interesado o de otra persona física, las comunicaciones a las entidades municipales por la Comisión Nacional de los Mercados y la Competencia de los datos de los abonados al servicio telefónico para la prestación del servicio sobre números de abonado en el marco de las llamadas de emergencia, siendo el más reciente el Informe 186/2018:
[…]

Por consiguiente, tal y como se ha expuesto en el apartado anterior, el tratamiento del dato de localización en las llamadas a los servicios de emergencia mediante el mecanismo AML sería lícito al amparo de lo previsto en la letra d) del artículo 6.1. del RGPD y en los términos que puedan establecerse en la normativa que transponga al ordenamiento jurídico español la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo de 11 de diciembre de 2018 por la que se establece el Código Europeo de las Comunicaciones Electrónicas, normativa que deberá ajustarse al resto de principios recogidos en el RGPD y que deberá ser objeto del preceptivo dictamen por la Agencia Española de Protección de Datos.

Todo ello sin perjuicio de que, atendiendo a los concretos términos en que se proceda a dicha transposición y, en el caso de que dicha normativa tenga rango de ley, el tratamiento pueda encontrar también su fundamento en el artículo 6.1 del RGPD, letra c (el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento) y 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).

A este respecto, el anteproyecto remitido no contiene disposición alguna respecto al uso de sistemas que permitan utilizar la información del terminal del afectado, incluso en los supuestos en los que no haya prestado su consentimiento, para facilitar su localización cuando se efectúan llamadas a los servicios de emergencia, limitándose el apartado 2 del artículo 74 a remitirse a un futuro desarrollo reglamentario que establecerá “criterios para la precisión y la fiabilidad de la información facilitada sobre la ubicación de las personas que efectúan comunicaciones de emergencia a los servicios de emergencia”.

Dicha remisión es insuficiente para amparar dichos tratamientos de datos personales en el cumplimiento de una obligación legal, ya que el artículo 8 de la LOPDGDD es claro al señalar que

> "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."

La exigencia de una norma con rango de ley deriva directamente de lo dispuesto en el artículo 53 de la Constitución y en la doctrina constitucional relativa a la limitación de los derechos fundamentales. En este sentido, el Tribunal Constitucional, en su STC 76/2019, de 22 de mayo, tras citar, entre otras, a su anterior STC 292/2000, de 30 de noviembre, señala:

> - 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, 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, 34/1995, 47/1995 y 96/1996) 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, 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).

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

> "En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; SSTC 66/1995, de 8 de mayo [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)."

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

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

> En cuanto a la justificación de dicha injerencia, cabe precisar que el requisito, previsto en el artículo 52, apartado 1, de la Carta, de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que la permita debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).

Igualmente, el apartado 65 de la Sentencia (STJUE) de la misma fecha 6 de octubre de 2020 (C-623/17), Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, con cita, como la anterior, de la sentencia Schrems 2, dice:

> 65 Cabe añadir que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).

En definitiva, el apartado 175 de la STJUE de 16 de julio de 2020, C-311/2020, Schrems 2, dice: Cabe añadir, sobre este último aspecto, que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate [dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 139 y jurisprudencia citada].

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

Y en dicha STJUE de 16 de julio de 2020, Schrems 2, se añade (y se reitera posteriormente en las citadas sentencias de 6 de octubre de 2020):

> 176 Finalmente, para cumplir el requisito de proporcionalidad según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario, la normativa controvertida que conlleve la injerencia debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos

de carácter personal contra los riesgos de abuso. En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 140 y 141 y jurisprudencia citada).

Partiendo de lo anterior, si se pretende habilitar el empleo de tecnologías como el sistema AML al objeto de facilitar la localización de los llamantes a los servicios de emergencia, debería recogerse en el apartado 2 del artículo 74 del anteproyecto la posibilidad de que, para facilitar la precisión de la ubicación, puedan utilizarse los datos procedentes del terminal del afectado, incluso en el supuesto de que para ello fuera necesario la activación automática de los servicios que permitan la ubicación del móvil en alta precisión, recogiendo asimismo el texto legal las garantías oportunas, como pueda ser la relativa a los tipos de datos que pueden tratarse, la limitación de la finalidad de su uso a los efectos de facilitar la localización del llamante en relación con la concreta llamada de emergencia, no admitiéndose su uso para una finalidad distinta, o el plazo de conservación de dichos datos, teniendo en cuenta los criterios que puedan facilitarse por la Dirección General de Protección Civil.

VIII

El artículo 72, al regular las “Guías de abonados y servicios de información sobre números de abonado”, se refiere en los últimos párrafos del apartado 2 al suministro de datos por parte de la CNMC en los siguientes términos:

La Comisión Nacional de los Mercados y la Competencia deberá suministrar gratuitamente los datos que le faciliten los citados operadores a las siguientes entidades

a) entidades que elaboren guías telefónicas de abonados.
b) operadores que presten el servicio de consulta telefónica sobre números de abonado.
c) entidades que presten los servicios de llamadas de emergencia de conformidad con el artículo 74 de la presente Ley.
d) agentes facultados para realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el capítulo V del título VIII del libro II de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de

mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica.

El suministro de los datos por parte de la Comisión Nacional de los Mercados y la Competencia a las entidades anteriores, se realizará de conformidad con las condiciones que se establezcan mediante real decreto y de acuerdo con el procedimiento para el suministro y recepción de la información que, en su caso, pueda fijar la Comisión Nacional de los Mercados y la Competencia mediante circular.

Fuera de los casos anteriores, el suministro de los datos por parte de la Comisión Nacional de los Mercados y la Competencia en favor de otras Administraciones u organismos públicos podrá autorizarse cuando exista cobertura normativa para dicho suministro.

A este respecto, conviene reiterar lo señalado a lo largo del presente informe relativo a la necesidad de que la "cobertura normativa" a que se refiere el anteproyecto debe tratarse de una norma con rango de ley que establezca las garantías adecuadas.

En este punto, debe destacarse que han sido numerosas las consultas recibidas por esta Agencia respecto a la posibilidad de que la CNMC suministre los números de teléfono de los abonados correspondientes a las muestras seleccionadas con la finalidad de realizar estudios estadísticos o encuestas por parte de organismos públicos, como consecuencia de las restricciones derivadas de la Pandemia del Covid-19, destacando en todos los informes emitidos la necesidad de que se proceda a su regulación legal, en el caso de que se pretenda generalizar esta modalidad, lo que se podría realizar en el presente anteproyecto, estableciendo las garantías específicas que se estimen adecuadas.

En este sentido se pronuncia, entre otros, el informe 29/2021, relativo a la consulta formulada por la CNMC respecto de la cesión al Ministerio de Educación y Formación Profesional, de los números de teléfono de los hogares seleccionados por el Instituto Nacional de Estadística para realizar las entrevistas que forman parte del Programa para la Evaluación Internacional de Competencias de la Población Adulta de la OCDE, en la que se señala lo siguiente:

I

Esta Agencia ya ha tenido ocasión de pronunciarse, en diferentes ocasiones, respecto de la procedencia de la comunicación de los

números de teléfono por parte de la CNMC a los servicios estadísticos de distintos organismos para la realización de encuestas incluidas en el Plan Estadístico Nacional, destacando que el criterio relevante al objeto de determinar la forma en la que procederá dicha comunicación no deriva de la obligatoriedad de la realización de la encuesta por el organismo público correspondiente, sino en la obligatoriedad de su cumplimentación por parte de los afectados.

En el presente caso, al referirse la consulta a la elaboración de una estadística oficial, de cumplimentación obligatoria, incluida en el Plan Estadístico Nacional y ejecutada por los servicios estadísticos del Estado, resulta de aplicación el criterio mantenido por esta Agencia en sus informes 75/2020 y 78/2020.

Así decíamos en el Informe 78/2020:

> *La consulta, a la que se acompaña el informe emitido por el delegado de protección de datos del ministerio, plantea la necesidad de que, para la realización de la Encuesta de Hábitos Deportivos 2020, se remitan por la Comisión Nacional de los Mercados y de la Competencia (CNMC) los números de teléfono de las personas seleccionadas en la muestra de la Encuesta realizada por el Instituto Nacional de Estadística (INE).*
>
> *La consulta justifica su solicitud en el hecho de que se trata de una estadística de cumplimentación obligatoria, invocando al respecto lo manifestado por esta Agencia en su Informe 70/2015, y que como consecuencia de la situación social y sanitaria causada por la pandemia del coronavirus COVID-19 y las restricciones derivadas de las medidas adoptadas por las comunidades autónomas en materia de salud pública, no es posible realizar las mismas de manera presencial.*
>
> *Asimismo, se especifica que el número de teléfono forma parte de la información solicitada en el cuestionario de la encuesta como instrumento de control de calidad de las gestiones realizadas, que su uso se limitaría exclusivamente a la realización de los trabajos de campo de la Encuesta, de modo que no sería objeto de tratamiento adicional, procediéndose a su destrucción una vez dado el visto bueno de calidad al informe realizado, garantizándose, igualmente, la confidencialidad del tratamiento al estar sujeto al secreto estadístico por la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública.*
>
> *La consulta se refiere a la elaboración de una estadística oficial, de cumplimentación obligatoria, incluida en el Plan Estadístico Nacional y ejecutada por los servicios estadísticos del*

Estado, para la realización de la cual es necesario, dadas las restricciones derivadas de la pandemia del COVID-19, obtener previamente los números de teléfono de los encuestados por parte de la CNMC, lo que implica, tal y como se indicó en el Informe de esta Agencia 49/2020 la comunicación de unos datos personales para una finalidad distinta de la que se habían obtenido. Al tratarse de una comunicación de datos entre organismos administrativos, debe estarse, en primer término, a lo previsto en su normativa específica, constituida, en el presente caso, por la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, cuyo artículo 23 incluye, dentro de los Servicios Estadísticos del Estado, además del INE y el Consejo Superior de Estadística, a "las unidades de los diferentes departamentos ministeriales y de cualesquiera otras entidades públicas dependientes de la misma a las que se haya encomendado aquella función", atribuyendo en su artículo 33 a los servicios estadísticos de los departamentos ministeriales, entre otras competencias, en su letra f), "La elaboración y ejecución de los proyectos estadísticos que se les encomiende en el Plan Estadístico Nacional".

Por otro lado, la citada ley, en su artículo 7.1. señala que "Se establecerán por Ley las estadísticas para cuya elaboración se exijan datos con carácter obligatorio" recogiéndose en la disposición adicional cuarta de la Ley 4/1990, de 29 de junio, de Presupuestos Generales del Estado para 1990 las estadísticas de cumplimentación obligatoria entre las que la disposición adicional segunda de la Ley 13/1996, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social incluyó "Las estadísticas que formen parte del Plan Estadístico Nacional y específicamente según el artículo 45.2 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, aquellas cuya realización resulte obligatoria para el Estado español por exigencia de la normativa de la Unión Europea. Asimismo, las estadísticas que pudieran realizarse al amparo del artículo 8.3 de la citada Ley".

Asimismo, y en lo que se refiere a la adecuación de la misma a lo previsto en el Reglamento general de protección de datos, el artículo 25 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales señala lo siguiente:

> *Artículo 25. Tratamiento de datos en el ámbito de la función estadística pública.*

1. El tratamiento de datos personales llevado a cabo por los organismos que tengan atribuidas las competencias relacionadas con el ejercicio de la función estadística pública se someterá a lo dispuesto en su legislación específica, así como en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

2. La comunicación de los datos a los órganos competentes en materia estadística solo se entenderá amparada en el artículo 6.1 e) del Reglamento (UE) 2016/679 en los casos en que la estadística para la que se requiera la información venga exigida por una norma de Derecho de la Unión Europea o se encuentre incluida en los instrumentos de programación estadística legalmente previstos.

De conformidad con lo dispuesto en el artículo 11.2 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, serán de aportación estrictamente voluntaria y, en consecuencia, solo podrán recogerse previo consentimiento expreso de los afectados los datos a los que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679.

3. Los organismos competentes para el ejercicio de la función estadística pública podrán denegar las solicitudes de ejercicio por los afectados de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 cuando los datos se encuentren amparados por las garantías del secreto estadístico previstas en la legislación estatal o autonómica.

Por consiguiente, atendiendo a lo previsto en la normativa específica, resulta que, en el presente caso, nos encontramos ante el supuesto de una estadística de cumplimentación obligatoria al estar incluida en el Plan Estadístico Nacional aprobado por Real Decreto 410/2016, de 31 de octubre, figurando entre la información que se debe facilitar, tal y como indica la consulta, el número de teléfono como instrumento de control de calidad de las gestiones realizadas, de modo que "Esta variable se convierte, por lo tanto, no solamente en un instrumento de contacto inicial con el informante, sino que también es parte del contenido del cuestionario".

Y al tratarse de una estadística de cumplimentación obligatoria, existe una obligación legal de los ciudadanos previamente seleccionados en la muestra de la encuesta de facilitar la información solicitada, tipificándose en el artículo 50 de la Ley 12/1989 como infracción leve "La remisión o el retraso en el envío de datos cuando no hubiere causado perjuicio grave para

el servicio, y hubiere obligación de suministrarlos", como infracción grave "La no remisión o el retraso en el envío de los datos requeridos cuando se produjese grave perjuicio para el servicio, y hubiere obligación de suministrarlos" y como infracción muy grave "La resistencia notoria, habitual o con alegación de excusas falsas en el envío de los datos requeridos, cuando hubiere obligación de suministrarlos".

Precisamente es la obligatoriedad en la cumplimentación de la encuesta la que permite diferenciar este supuesto de aquellos otros en los que la misma es voluntaria, como son las realizadas por el Centro de Investigaciones Sociológicas, ya que, al implicar el tratamiento de categorías especiales de datos, el artículo 5 de la Ley 39/1995, de 19 de diciembre, de Organización del Centro de Investigaciones Sociológicas recoge el principio de voluntariedad de las respuestas, lo que exige que, en el caso de pretenderse la comunicación de los números de teléfono por parte de la CNMC al CIS, deban adoptarse garantías adicionales, tal y como se analiza en el Informe 49/2020.

Por lo tanto, en el presente caso, la comunicación de los datos de los abonados al servicio telefónico por parte de la CNMC para la elaboración de una estadística oficial, de cumplimentación obligatoria, incluida en el Plan Estadístico Nacional y ejecutada por los servicios estadísticos del Estado encontraría su fundamento 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").

En todo caso, deberá cumplirse por el responsable del tratamiento con los principios establecidos en el artículo 5 del RGPD, señalándose en la consulta que el uso de estos teléfonos se limitaría exclusivamente a la realización de los trabajos de campo de la Encuesta, de modo que no sería objeto de tratamiento adicional, adecuándose a los principios de limitación de la finalidad y de minimización de datos y que el principio de limitación del plazo de conservación también quedaría garantizado al destruirse los números de teléfono facilitados, una vez dado el visto bueno de calidad al informe realizado.

Asimismo, habría que añadir el resto de garantías propias del ejercicio de la función estadística, como el sometimiento al secreto estadístico o la disociación de los datos desde el

momento en que se realiza la encuesta, separando las respuestas dadas por los encuestados de los números de teléfono, así como el resto de medidas técnicas y organizativas apropiadas para garantizar el respetos a los derechos y libertades de los afectados y la adecuación del tratamiento a la normativa sobre protección de datos personales que corresponde adoptar al Ministerio de Cultura como responsable del tratamiento, de acuerdo con el principio de responsabilidad proactiva.

Por todo ello, esta Agencia entiende que la comunicación de los números de teléfono por la CNMC a los servicios estadísticos del Ministerio de Cultura, en los términos previstos en el presente informe, se encuentra amparada por el RGPD siempre y cuando, tal y como ya se señalaba en el Informe 70/2015, el dato sea únicamente utilizado para la realización de la estadística en cuyo ámbito es solicitado.

Todo ello sin perjuicio de que, basándose la consulta en las restricciones derivadas de la pandemia del COVID-19 y tal y como se adelantaba en el Informe 49/2020, estando recomendado en el apartado 28 del Programa anual 2020 del Plan Estadístico Nacional 2017-2020, el fomento de la recogida multicanal en las encuestas a hogares a través de medios electrónicos y telefónicos teniendo en cuenta la evolución de la sociedad en el uso de Internet y la efectividad de la recogida telefónica de datos, esta Agencia considera necesario que, en el caso de que se prevea la generalización de las encuestas a través de medios electrónicos y telefónicos, se impulse la correspondiente modificación legislativa que garantice la seguridad jurídica y la adecuación de los correspondientes tratamientos de datos personales al RGPD y a la doctrina del Tribunal Constitucional, mediante el establecimiento de las garantías específicas que se estimen adecuadas.

Por lo tanto, debiéndose aplicar el mismo criterio al presente caso al concurrir idénticas circunstancias, debe concluirse que la comunicación de los números de teléfono por la CNMC al Instituto Nacional de Evaluación Educativa, en los términos previstos en el presente informe, se encuentra amparada por el RGPD siempre y cuando, tal y como ya se señalaba en el Informe 70/2015, el dato sea únicamente utilizado para la realización de la estadística en cuyo ámbito es solicitado.

Asimismo, esta Agencia insiste en la necesidad, ya indicada en los informes anteriores, de que se impulse la correspondiente modificación legislativa que garantice la seguridad jurídica y la

adecuación de los correspondientes tratamientos de datos personales al RGPD y a la doctrina del Tribunal Constitucional, mediante el establecimiento de las garantías específicas que se estimen adecuadas.