Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente al Proyecto de Orden Ministerial conjunta por la que se define el formato de entrega de los datos conservados por los operadores de servicios de comunicaciones electrónicas o de redes públicas de servicios de comunicaciones electrónicas a los agentes facultados, solicitado de esta Agencia Española de Protección de Datos de conformidad con lo dispuesto en los artículos 37 h) de la Ley Orgánica, de 13 de diciembre, de Protección de datos de Carácter Personal, y 5 b) del Estatuto de la Agencia, aprobado por Real Decreto 428/1993, de 26 de marzo, 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.

I

El Proyecto sometido a informe tiene por objeto, de conformidad con lo dispuesto en su artículo 1, el establecimiento de las especificaciones técnicas y de formato de entrega a los agentes facultados de los datos objeto de conservación a los que se refiere el artículo 3 y la disposición adicional única de la Ley 25/2007, de 18 de octubre, de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, cuya disposición final cuarta establece en su apartado 1 que “La cesión a los agentes facultados de los datos cuya conservación sea obligatoria, se efectuará en formato electrónico, en la forma que se determine por Orden conjunta de los Ministros de Interior, de Defensa y de Economía y Hacienda, que se aprobará en el plazo de tres meses desde la entrada en vigor de esta Ley”.

La citada Ley, en desarrollo de la Directiva 2006/24/CE desarrolla la obligación de los operadores de comunicaciones electrónicas de “conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales”.

De este modo, el Proyecto sometido a informe establece en su artículo 2 el formato de entrega de los datos a los agentes facultados, previendo, como criterio general, el sometimiento de las comunicaciones para tal intercambio al formato establecido en la especificación técnica del Instituto Europeo de Normalización de las Telecomunicaciones ETSI TS 102 657, con las especificaciones y modificaciones efectuadas, respecto de su versión inglesa, en el Anexo I del Proyecto, referido igualmente a la comunicación de datos de localización del terminal, conforme dispone el artículo 3.

No obstante, se prevé en el párrafo segundo del artículo 2 un supuesto especial en caso de que el número de solicitudes individuales de cesión de datos efectuado por todos los agentes facultados en el año natural anterior sea inferior a 2000, dado que en ese caso se prevé la posibilidad de que la comunicación se verifique a través de una solución tecnológica acordada previamente con los agentes facultados, conforme se analizará con posterioridad.

El artículo 4 se refiere a los canales de comunicación entre los sujetos obligados y los agentes facultados, diferenciando los de información administrativa y de transmisión de los datos objeto de conservación, estableciendo el Anexo II del Proyecto las características y requisitos que deben cumplir ambos canales de comunicaciones, así como los pormenores del abono del coste de las comunicaciones por parte de los agentes facultados.

Asimismo, el artículo 5 establece las limitaciones a la comunicación de información relacionada con la conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones electrónicas entre sujetos facultados, indicando que “los sujetos obligados garantizarán en todo momento la confidencialidad de la información transmitida o almacenada, no pudiendo ser utilizada para ningún otro fin”.

Finalmente, se prevé que los operadores deberán implantar las medidas necesarias para el cumplimiento de lo dispuesto en la Orden en el plazo establecido en la disposición final cuarta de la Ley 25/2007, conforme a cuyo apartado 2 “Los sujetos obligados a los que se refiere el artículo 2 de esta Ley, tendrán un plazo de seis meses desde la entrada en vigor de la misma para configurar, a su costa, sus equipos y estar técnicamente en disposición de cumplir con las obligaciones de conservación y cesión de datos”.

II

De las cuestiones planteadas por el texto sometido a informe, obviamente, la que resulta especialmente relevante a los efectos del análisis que debe efectuarse en este lugar es la relativa al formato de entrega de los datos, así como los canales de comunicaciones en que dicha entrega podrá tener lugar, contempladas en los artículos 2 y 4 de la Orden.

A tal efecto, resulta particularmente relevante, en relación con la incidencia de esta materia en la regulación del derecho fundamental a la protección de datos de carácter personal, lo dispuesto en el artículo 8 de la Ley 25/2007, en que se establece lo siguiente:

> *"1. Los sujetos obligados deberán identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados, con sujeción a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.*
>
> *2. Las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos serán las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo.*
>
> *3. El nivel de protección de los datos almacenados se determinará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.*
>
> *4. La Agencia Española de Protección de Datos es la autoridad pública responsable de velar por el cumplimiento de las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, y de la normativa de desarrollo aplicables a los datos contemplados en la presente Ley."*

Dichas previsiones se complementan con lo establecido en el artículo 81.4 del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, en que se prevé que "a los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenidas en el artículo 103 de este Reglamento".

El artículo 103, a su vez, regula el registro de acceso a los datos de carácter personal objeto de tratamiento, disponiendo en sus cinco primeros apartados lo siguiente:

> *"1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.*

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados."

III

Como se ha indicado, el Proyecto establece, como punto de partida, la aplicación del estándar ETSI TS 102 657, con determinadas modificaciones, contenidas en el Anexo I del texto, debiendo considerarse dicho estándar como adecuado a los efectos previstos en la normativa de protección de datos de carácter personal.

No obstante, el párrafo segundo del artículo 2 del Proyecto establece que "salvo acuerdo en contra entre las partes, cuando el sujeto obligado haya recibido un número de solicitudes individuales de cesión de datos entre todos los agentes facultados inferior a 2000 solicitudes durante el año natural anterior, en lugar de utilizar el formato de entrega basado en la norma ESTI TS 102 657 podrá optar por utilizar otra solución tecnológica acordada previamente con los agentes facultados, en formato electrónico y cuyo nombre se adecuará a lo definido en el punto 7.1 del Anexo I de esta Orden Ministerial", añadiendo que en caso de resultar mayor el número de solicitudes en el año natural anterior se dispondrá de un plazo, que será de seis meses en virtud de la remisión efectuada por el Proyecto a la Ley 25/2007, para implantar el procedimiento basado en el estándar regulado por el Proyecto.

Del mismo modo, en cuanto a los canales de comunicación, el Anexo II especifica que "los sujetos obligados que hayan recibido un número inferior a 2000 solicitudes individuales de cesión de datos, según lo recogido en el artículo 2, podrán optar por otros canales seguros de comunicación, previo acuerdo con cada uno de los agentes facultados".

Esta previsión plantea una serie de dudas desde el punto de vista del establecimiento y mantenimiento de las garantías previstas en el estándar establecido como tipo en el Proyecto y, en definitiva, del cumplimiento de los requerimientos establecidos en la normativa vigente en materia de protección de datos de carácter personal.

En este sentido, no debe ignorarse que el protocolo establecido como tipo viene a garantizar una medida de seguridad adicional que, aun no siendo preceptivamente exigible en el tratamiento de los datos controvertidos, añade un plus de seguridad a la comunicación de los datos, cual es el cifrado de los datos durante la comunicación.

De este modo, los procedimientos que pudieran acordarse conforme al párrafo segundo del artículo 2 del Proyecto podrían implicar una merma en la seguridad respecto al adoptado como estándar generalmente aplicable.

Por otra parte, del tenor literal del Proyecto no resulta claro a qué anualidad se está haciendo referencia al mencionarse el “año natural anterior”, en el sentido de que el mismo podría ser considerado como el anterior a la entrada en vigor de la norma o si el cómputo operaría de tal manera que en el momento de recibirse la petición número 2001 en un período inferior al año ya sería de obligado cumplimiento el protocolo establecido en el Anexo I del Proyecto, debiendo implantarse el mismo en el plazo de seis meses desde el momento en que se produzca esa recepción de la petición número 2001 en un plazo inferior al año, lo que además exigiría que existiera algún tipo de constancia de si concurre o no esta circunstancia para determinar cuál sería el protocolo exigible.

En este sentido, ciertamente el Proyecto se refiere al “año natural”. Sin embargo, dado que el sistema acordado con arreglo a este párrafo supondrá, en principio, una menor garantía de la seguridad en la transmisión de los datos, sería preferible que el cómputo no hubiera de esperar al término del año natural, habida cuenta de que sería posible que en el primer ejercicio en que se superase el límite de 2000 peticiones individualizadas esta cifra se alcanzase en un plazo muy breve de tiempo y hubiera no obstante que esperar al término del año para que efectivamente se implantasen medidas que garantizasen una seguridad reforzada en la comunicación de los datos.

Además, el párrafo segundo del artículo 2 plantea problemas interpretativos si se atiende a lo previsto en el segundo párrafo de la disposición transitoria única, según el cual “aquellos sujetos obligados que inicien su actividad desde la entrada en vigor de esta Orden Ministerial deberán cumplir las obligaciones establecidas en esta Orden Ministerial desde el inicio de su actividad”.

En este sentido, esta exigencia de cumplimiento podría implicar el establecimiento de un “acuerdo” con los sujetos obligados en tanto no se produzca un volumen de solicitudes superior a 2000 en cómputo anual, por lo que sí sería obligado llegar a ese acuerdo, pero no someterse al estándar establecido en el Anexo I.

Finalmente, debería clarificarse que entiende la disposición por “acuerdo en contra de las partes”, en el sentido de clarificar quién deberá determinar las condiciones mínimas de seguridad exigibles al protocolo para que se cumplan las exigencias establecidas en la normativa de protección de datos de carácter personal. Al propio tiempo, deberían especificarse cuáles serían las consecuencias de la inexistencia del mencionado “acuerdo”.

Quiere todo ello decir que, a juicio de esta Agencia, sería necesario modificar el contenido del párrafo segundo del artículo 2 del Proyecto y, por extensión y en lo que resulte pertinente, del párrafo segundo de la disposición transitoria única del mismo, clarificando lo siguiente:

- Que en todo caso la solución tecnológica acordada conforme al precepto que se está analizando deberá garantizar el cumplimiento de las medidas de seguridad exigibles conforme a lo establecido en la normativa de protección de datos de carácter personal.

- Cómo debería computarse el plazo anual mencionado en el citado párrafo y si existirá algún deber de comunicación referido al hecho de que se ha superado el límite de 2000 comunicaciones en cómputo anual.

- Qué ha de entenderse como “acuerdo en contrario de las partes”.

- Las consecuencias de la existencia de este procedimiento alternativo en el régimen transitorio establecido en el Proyecto, en el sentido de determinar si el protocolo adoptado en el Anexo I no será exigible a los nuevos operadores en tanto no haya transcurrido su primer año natural de funcionamiento o no se superen en cómputo anual las 2000 solicitudes.

IV

Por otra parte, ya se indicó que el artículo 5 del Proyecto se refiere a las limitaciones a la comunicación de información relacionada con la conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones electrónicas entre sujetos facultados, indicando que “los sujetos obligados garantizarán en todo momento la confidencialidad de la información transmitida o almacenada, no pudiendo ser utilizada para ningún otro fin”.

Tal y como se establece en la Ley 25/2007, el objeto de la misma es la regulación de la obligación de conservación de la información a la que se

refiere el artículo 3 de la Ley y su comunicación a los agentes facultados, conforme a los requisitos establecidos en su artículo 7.

De este modo, sin perjuicio de la información que pudiera intercambiarse entre los sujetos obligados para la cooperación mutua en el adecuado desarrollo del sistema de comunicación de la información a los agentes facultados, debería quedar claro en todo caso que ese intercambio de información en modo alguno podría referirse a los datos de carácter personal respecto de los que existe la obligación de conservación y, en su caso, comunicación a los agentes facultados.

Ciertamente, el precepto, en el texto transcrito se refiere al deber de garantía de la confidencialidad de la información, que no puede ser empleada para fines distintos. No obstante, cabe considerar que esta referencia debería clarificarse en el sentido de que los operadores no procederán al intercambio de datos de carácter personal conservados conforme a las exigencias de la Ley 25/2007.

Por este motivo, sería conveniente clarificar el tenor del artículo 5, párrafo primero, del Proyecto en el sentido de indicar que el intercambio de información a que el mismo se refiere no alcanzará a los datos concretos objeto de conservación y deber de comunicación a los agentes facultados.