

I

Tal y como indica su artículo 1, el objeto del Anteproyecto sometido a informe es “regular determinados aspectos de los servicios electrónicos de confianza, como complemento del Reglamento (UE) nº 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE”.

Así, se indica en la Exposición de Motivos, que siendo el citado Reglamento parte integrante de nuestro ordenamiento jurídico en virtud del principio de primacía del derecho de la Unión, la función del texto sometido a informe es “complementarlo en aquellos aspectos concretos que el Reglamento no ha armonizado y cuyo desarrollo prevé en los ordenamientos jurídicos de los diferentes Estados miembros. Sus disposiciones han de ser interpretadas de acuerdo con el Reglamento (UE) nº 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014”

Debe en este punto señalarse que el considerando 11 del Reglamento 910/2014 recuerda que el mismo “debe aplicarse de forma que se cumplan plenamente los principios relativos a la protección de los datos personales establecidos en la Directiva 95/46/CE del Parlamento Europeo y del Consejo”; y añade que “por otra parte, los prestadores de servicios de confianza y el organismo de supervisión deben respetar asimismo los requisitos de confidencialidad y seguridad del tratamiento previstos en la Directiva 95/46/CE”.

Por este motivo, el artículo 5 del Reglamento, bajo la rúbrica “Tratamiento y protección de los datos” establece que “El tratamiento de los datos personales será conforme a lo dispuesto en la Directiva 95/46/CE”, indicando en su apartado 2 que “sin perjuicio de los efectos jurídicos que la

legislación nacional contemple para los seudónimos, no se prohibirá su utilización en las transacciones electrónicas”.

Asimismo, el artículo 24.2 j) señala que “los prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados (...) garantizarán un tratamiento lícito de los datos personales de conformidad con la Directiva 95/46/CE”.

En materia de seguridad, el artículo 19.1 del Reglamento impone a los prestadores cualificados y no cualificados de servicios de confianza la obligación de adoptar “las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan. Habida cuenta de los últimos avances tecnológicos, dichas medidas garantizarán un nivel de seguridad proporcionado al grado de riesgo. En particular, se adoptarán medidas para evitar y reducir al mínimo el impacto de los incidentes de seguridad e informar a los interesados de los efectos negativos de cualquiera de tales incidentes”.

Asimismo, regula la notificación de violaciones de seguridad en su apartado 2, según el cual “los prestadores cualificados y no cualificados de servicios de confianza, sin demoras indebidas pero en cualquier caso en un plazo de 24 horas tras tener conocimiento de ellas, notificarán al organismo de supervisión y, en caso pertinente, a otros organismo relevantes como el organismo nacional competente en materia de seguridad de la información, o la autoridad de protección de datos, cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes”.

En cuanto al régimen de supervisión, el considerando 31 indica que “los organismos de supervisión deben cooperar con las autoridades de protección de datos, por ejemplo informándoles de los resultados de las auditorías de los prestadores cualificados de servicios de confianza, en caso de resultar infringidas las normas sobre protección de datos de carácter personal. El suministro de información debe incluir, en particular, los incidentes en materia de seguridad y las violaciones de los datos de carácter personal”.

Así, el artículo 17.4, dentro de los deberes de colaboración de las autoridades de supervisión, se señala que dentro de sus funciones se incluirá



en particular “informar a otros organismos de supervisión y al público de la violación de seguridad o la pérdida de integridad, de conformidad con el artículo 19, apartado 2” (apartado c) y “cooperar con las autoridades de protección de datos, en particular, informándoles, sin demora indebida, de los resultados de las auditorías de los prestadores cualificados de servicios de confianza, en caso de posible infracción de las normas sobre protección de datos personales” (apartado f).

II

Por otra parte, conforme al apartado a) de la disposición derogatoria única del Anteproyecto queda derogada por el mismo la Ley 59/2003, de 19 de diciembre, de Firma electrónica.

Dicha Ley incorpora un artículo 17 referido a protección de datos personales en el que se establece lo siguiente:

“1. El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta ley se sujetará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en sus normas de desarrollo.

2. Para la expedición de certificados electrónicos al público, los prestadores de servicios de certificación únicamente podrán recabar datos personales directamente de los firmantes o previo consentimiento expreso de éstos.

Los datos requeridos serán exclusivamente los necesarios para la expedición y el mantenimiento del certificado electrónico y la prestación de otros servicios en relación con la firma electrónica, no pudiendo tratarse con fines distintos sin el consentimiento expreso del firmante.

3. Los prestadores de servicios de certificación que consignen un seudónimo en el certificado electrónico a solicitud del firmante deberán

constatar su verdadera identidad y conservar la documentación que la acredite.

Dichos prestadores de servicios de certificación estarán obligados a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica de Protección de Datos de Carácter Personal en que así se requiera.

4. En cualquier caso, los prestadores de servicios de certificación no incluirán en los certificados electrónicos que expidan, los datos a los que se hace referencia en el artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.”

Por último, no debe olvidarse que el marco regulador del derecho fundamental a la protección de datos de carácter personal se encuentra en el presente momento en una situación de modificación como consecuencia de la aprobación 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), que será plenamente aplicable, según su artículo 99.2, el día 25 de mayo de 2018.

III

Entrando ya en el análisis del Anteproyecto sometido al parecer de esta Agencia, los artículos 6 y 7 del texto se refieren, respectivamente, a la consignación de la identidad y atributos de los titulares de los certificados cualificados y al modo en que se comprobará la identidad y circunstancias de los solicitantes de los mismos.

En este punto, el artículo 6.1 a) del Anteproyecto dispone que “La identidad del titular en los certificados cualificados se consignará (...) en el supuesto de certificados de firma electrónica y de autenticación de sitio web expedidos a personas físicas, por su nombre y apellidos y su número de documento nacional de identidad, o a través de un seudónimo que conste

como tal de manera inequívoca. El número de documento nacional de identidad podrá sustituirse por otro código o número identificativo cuando el firmante carezca de él, siempre que le identifique unívocamente”.

A su vez, también en relación con las personas físicas, el artículo 7.1 establece que “La identificación de la persona física que solicite un certificado cualificado exigirá su personación ante los encargados de verificarla y se acreditará mediante el documento nacional de identidad, pasaporte u otros medios admitidos en derecho”, añadiendo que “Podrá prescindirse de la personación de la persona física que solicite un certificado cualificado si su firma en la solicitud de expedición de un certificado cualificado ha sido legitimada en presencia notarial”, debiendo constar en el certificado la forma en que la persona ha sido identificada, conforme al artículo 7.3.

El artículo 24.1 del Reglamento 910/014 establece que “Al expedir un certificado cualificado para un servicio de confianza, un prestador cualificado de servicios de confianza verificará, por los medios apropiados y de acuerdo con el Derecho nacional, la identidad y, si procede, cualquier atributo específico de la persona física o jurídica a la que se expide un certificado cualificado”.

De este modo, el citado precepto impone a los prestadores la obligación legal de proceder al tratamiento de los datos necesarios para la identificación.

Como se ha indicado, dichos datos serán el nombre, apellidos, documento nacional de identidad o documento equivalente o, en su caso un seudónimo, si consta de manera inequívoca.

El artículo 4.1 de la Ley Orgánica 15/1999 dispone que “Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido”. En este mismo sentido se pronunciaba el párrafo segundo del artículo 17.2 de la Ley 59/2003, ya reproducido con anterioridad.

Pues bien, los datos a los que se refiere el artículo 6.1 responden al citado principio, particularizando de forma taxativa la regla general que hasta ahora establecía la Ley 59/2003. A estos efectos, debe recordarse que el

artículo 1.2 del Real decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, señala que el citado documento “tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo”.

Por todo ello, el tratamiento de estos datos resulta amparado por el artículo 6.2 de la Ley Orgánica 15/1999 y es adecuado conforme a su artículo 4.1. Igualmente, dicho tratamiento estará legitimado por el artículo 6.1 c) del Reglamento General de Protección de Datos, que habilita el tratamiento basado en una obligación legal impuesta por el derecho interno o de la Unión Europea, cumpliéndose igualmente el principio de minimización previsto en su artículo 5.1 c), según el cual los datos deberán ser “adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados”.

Del mismo modo, en cuanto al procedimiento de comprobación de la identidad del solicitante, el artículo 7 del Anteproyecto resulta conforme con el artículo 24.1 del reglamento 910/2014, que a partir de su párrafo segundo regula los procedimientos posibles para llevar a cabo esa verificación.

IV

El artículo 8 del Anteproyecto lleva por rúbrica “protección de datos personales”, estableciendo en el apartado 1 (que realmente es único y compuesto de dos párrafo) lo siguiente:

“Los prestadores de servicios electrónicos de confianza que consignen un seudónimo en un certificado electrónico deberán constatar la verdadera identidad del firmante o titular del certificado y conservar la documentación que la acredite.

Dichos prestadores de servicios de confianza estarán obligados a revelar la citada identidad cuando lo soliciten los órganos judiciales y otras autoridades públicas para el ejercicio de las funciones que tienen atribuidas con sujeción a lo dispuesto en la legislación aplicable en materia de protección de datos personales.”

Dicho precepto parece adaptar el derecho español a lo previsto en el artículo 5 del reglamento 910/2014, reproducido en el apartado I de este informe, si bien limitándose a indicar en el primer párrafo que será precisa la constatación de la identidad del solicitante del certificado, conforme a lo establecido para los prestadores de certificados cualificados en los artículos 6 y 7 del Anteproyecto, a lo que acaba de hacerse referencia.

El segundo párrafo toma en consideración la previsión contenida en el artículo 5.2 del Reglamento 910/2014, especificando los supuestos en que los prestadores estarán obligados a revelar la identidad del interesado al que se refiere el seudónimo, que queda limitado a los supuestos en que la información se solicite por los órganos judiciales y otras autoridades públicas para el ejercicio de las funciones que tienen atribuidas.

Esta disposición supone una limitación de los supuestos en que será posible desvelar la identidad del interesado respecto de los que se preveían en el artículo 17.3, que ampliaba la revelación a “los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica de Protección de Datos de Carácter Personal en que así se requiera”, lo que a juicio de esta Agencia resulta más conforme con la normativa de protección de datos, al limitar los supuestos en que los datos serán revelados.

No obstante, sería necesario que se clarificase que la cesión de los datos a las autoridades públicas únicamente se producirá en los supuestos en los que la Ley atribuya expresamente a las mismas la facultad de recabar este tipo de información. No se trata de imponer la obligación de que la Ley prevea expresamente el acceso a los datos identificativos del titular del seudónimo, sino que exista una habilitación específica que otorgue a esas administraciones públicas o bien una potestad reforzada de investigación o bien imponga una obligación legal de colaboración con la misma.

Por ello, se considera necesario modificar el párrafo segundo del artículo 8 del Anteproyecto indicando que la revelación de los datos se podrá producir a “otras autoridades públicas para el ejercicio de las funciones que tienen atribuidas por las Leyes, con sujeción a lo dispuesto en la legislación aplicable en materia de protección de datos personales.”

Al propio tiempo, el artículo 8 del Anteproyecto no establece una cláusula general de sometimiento a la normativa de protección de datos por parte del prestador y de las administraciones competentes, similar a la establecida en el artículo 24.1 del Reglamento, que se remite a la Directiva 95/46/CE.

En este sentido, debe recordarse que el artículo 17.1 de la Ley 59/2003 establece que “El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta ley se sujetará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en sus normas de desarrollo”.

A nuestro juicio, es necesario que el artículo 8 del Anteproyecto se inicie con esta remisión general, que resulta especialmente relevante si se tiene en cuenta el cambio normativo que tendrá lugar como consecuencia de la plena aplicación del Reglamento general de Protección de Datos.

Por ello, **debería introducirse un nuevo apartado 1 al artículo 8 del Anteproyecto, pasando a formar el texto actual su apartado 2, con el siguiente tenor:**

“El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones que les hayan sido atribuidas se sujetará a lo dispuesto en la normativa de la Unión Europea y del derecho interno en materia de Protección de Datos de Carácter Personal.”

V

En materia de seguridad, resulta especialmente relevante lo dispuesto en el artículo 14 del Anteproyecto, cuyo apartado 1 dispone que “Los prestadores cualificados y no cualificados de servicios electrónicos de confianza notificarán al Ministerio de Energía, Turismo y Agenda Digital las violaciones de seguridad o pérdidas de la integridad señaladas en el artículo 19.2 del Reglamento (UE) nº 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, sin

perjuicio de su notificación a la Agencia Española de Protección de Datos, si procede, o a las personas afectadas, en su caso”.

Como ya se ha indicado con anterioridad, el artículo 19 del Reglamento 910/2014 impone este deber de notificación a los prestadores de servicios de confianza. A ello añade el artículo 19.1 con carácter previo que dichos prestadores tendrán la obligación de adoptar “las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan. Habida cuenta de los últimos avances tecnológicos, dichas medidas garantizarán un nivel de seguridad proporcionado al grado de riesgo. En particular, se adoptarán medidas para evitar y reducir al mínimo el impacto de los incidentes de seguridad e informar a los interesados de los efectos negativos de cualquiera de tales incidentes”.

Al propio tiempo, no debe olvidarse que el artículo 24.2 j) del Reglamento señala expresamente que los prestadores “garantizarán un tratamiento lícito de los datos personales de conformidad con la Directiva 95/46/CE”.

Como se ha indicado, el régimen de la Directiva 95/46/CE ha sido reemplazado por el Reglamento General de Protección de Datos, que en su artículo 33.1 dispone que “En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación”. Por este motivo, el artículo 19.2 del Reglamento 910/2014 se refiere expresamente a la notificación al organismo nacional relevante en materia de protección de datos.

Al propio tiempo, el artículo 34 regula el deber de notificación de la violación de seguridad al interesado “Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas”, así como cuando por estas mismas circunstancias lo considere necesario la propia autoridad de control.

De este modo, la obligación de notificación del artículo 14 del Anteproyecto se configura como complementaria de la que habrá de llevarse a cabo obligatoriamente a partir del 25 de mayo de 2018 a las autoridades de protección de datos. Por ello, la mención incluida en el último inciso del artículo 14.1 ha de considerarse ajustada al nuevo régimen del derecho de la Unión en materia de protección de datos de carácter personal.

No obstante, sería conveniente que el citado artículo 14, referido según su rúbrica a las “obligaciones de seguridad de la información”, fuese precedido de una referencia expresa a la aplicación de las normas de protección de datos, adaptando el derecho español a lo previsto en el artículo 19.1 del Reglamento 910/2014.

No se trata, obviamente, de reproducir este precepto, lo cual se haya vedado por el derecho de la Unión, sino de completarlo a la luz de lo dispuesto en el artículo 32.1 del Reglamento general de protección de datos, en virtud del cual “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”.

De este modo, se propone la inclusión de un nuevo apartado 1 del artículo 14, que prevea que “Además de las medidas a las que se refiere el artículo 19.1 del Reglamento 910/2014, los prestadores cualificados y no cualificados de servicios de confianza aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo en materia de protección de datos, 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”

VI

En relación con la notificación de violaciones de seguridad de los datos, los apartados e) y f) del artículo 19.3 del Anteproyecto tipifican como infracciones muy graves “No notificar, sin demoras indebidas pero en cualquier caso en un plazo de 24 horas tras tener conocimiento de ellas, al Ministerio de Energía, Turismo y Agenda Digital cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado, salvo que sólo afecte a los datos personales tratados por el prestador, o no ampliar la información notificada, según lo dispuesto en el artículo 14.3” así como “Cuando la violación de seguridad o la pérdida de integridad puedan atentar contra una persona física o jurídica a la que se ha prestado el servicio de confianza, no notificar también a la persona física o jurídica, sin demora indebida, la violación de seguridad o la pérdida de integridad”.



En relación con estos tipos sancionadores, parece preverse que no existirá vulneración de la norma en caso de que la violación únicamente afecte a los datos personales tratados por el prestador. Sin embargo, el artículo 14 del Anteproyecto en ningún momento prevé que no exista esta obligación de notificación al Ministerio en estos casos, ni prevé un mecanismo de remisión a esta Agencia Española de Protección de Datos de las violaciones de seguridad que afecten, únicamente o conjuntamente con otras quiebras de seguridad, a los datos de carácter personal.

Si se pretende excluir del régimen de responsabilidad la falta de notificación de este tipo de violaciones, **sería preciso que el artículo 14 estableciese un régimen más detallado que señale expresamente que cuando la violación sólo se refiera a datos de carácter personal deberá notificarse a la autoridad de protección de datos que resulte competente, así como un mecanismo de remisión de estas notificaciones por parte del Ministerio a la Agencia en caso de que la notificación se refiera a protección de datos y se hubiera dirigido a aquél.**

Al propio tiempo, es posible que una violación de seguridad entrañe riesgo para los datos personales unido a otros de distinta naturaleza. En este supuesto **debería, en primer lugar, arbitrarse el procedimiento que implicase el ejercicio por ambas autoridades de sus respectivas competencias en lo que afecte a la brecha notificada, incluyendo tanto el reparto de las mismas como la posibilidad de actuaciones conjuntas o delegadas de investigación de la violación de seguridad.**

Por otra lado, sería preciso dejar claro en el régimen sancionador del Proyecto que **la inexistencia de la notificación, en caso de que no sólo afecte a protección de datos podrá implicar la imposición de las sanciones previstas en el Anteproyecto sin perjuicio de las que pudieran corresponder en aplicación de la normativa de protección de datos**, dado que existiría una dualidad de bienes jurídicos protegidos: la seguridad e integridad de las certificaciones por una parte y el derecho fundamental a la protección de datos, por otra.

VII

Debe, por último, hacerse referencia al régimen de supervisión y control regulado por el Título IV del Anteproyecto.

En dicho Título, tras atribuirse la competencia en la materia al Ministerio de Energía, Turismo y Agenda Digital, se regula el alcance de las actuaciones inspectoras que podrán desarrollarse por éste y, en el artículo 18, el régimen de información y cooperación, incluyendo las obligaciones de información de los

prestadores, la entidad nacional de acreditación, los organismos de evaluación de la conformidad, los organismos de certificación y cualquier otra persona o entidad relacionada con el prestador de servicios y las competencias del Ministerio para el acceso a las instalaciones y la consulta de cualquier información relevante.

En este punto, debe recordarse que el considerando 31 del Reglamento 910/2014 señala que “los organismos de supervisión deben cooperar con las autoridades de protección de datos, por ejemplo informándoles de los resultados de las auditorías de los prestadores cualificados de servicios de confianza, en caso de resultar infringidas las normas sobre protección de datos de carácter personal. El suministro de información debe incluir, en particular, los incidentes en materia de seguridad y las violaciones de los datos de carácter personal”.

Ya se ha hecho referencia en el apartado anterior a la necesidad de que el Anteproyecto introduzca alguna previsión que regule el deber de colaboración y suministro de información por parte del órgano supervisor a la Agencia Española de Protección de Datos en lo que respecta a las posibles violaciones de seguridad que comprometan a datos de carácter personal. Estas previsiones deberían completarse con una cláusula general de colaboración que recogiese lo establecido, con carácter general, en el citado considerando 31.

Tal previsión sería lícita, por cuanto se referiría únicamente al establecimiento de mecanismos internos de cooperación entre autoridades del estado miembro dentro del margen previsto expresamente en el Reglamento 910/2014.

Por todo ello se propone la inclusión de un precepto que prevea expresamente el régimen de colaboración entre el Ministerio de Energía, Turismo y Agenda Digital y las autoridades de protección de datos y, en particular, esta Agencia Española de Protección de Datos, en los términos que se derivan directamente del considerando 31 del Reglamento 910/2014.