El Proyecto EuroPriSe: los Sellos de Privacidad y la generación de confianza en la Administración Electrónica

Emilio Aced Félez y Francisco Javier Montes Pando

Agencia de Protección de Datos de la Comunidad de Madrid

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP) tiene como uno de sus objetivos fundamentales el dotar de seguridad jurídica a las relaciones de los ciudadanos con las Administraciones Públicas y fomentar la confianza de los mismos en estos nuevos canales de comunicación que reportan ventajas tangibles y evidentes, tanto a las AA.PP. como a las personas que los utilizan para interactuar con ellas.

En la generación de esta confianza, la convicción de que los organismos públicos van a respetar los principios y derechos que conforman el derecho fundamental a la protección de datos personales juega un papel esencial y así lo reconoce el preámbulo de la LAECSP cuando dice que *"(…) El reconocimiento general del derecho de acceder electrónicamente a las Administraciones Públicas tiene otras muchas consecuencias a las que hay dar solución y de las que aquí, de forma resumida, se enumeran algunas. Así, en primer lugar, la progresiva utilización de medios electrónicos suscita la cuestión de la privacidad de unos datos que se facilitan en relación con un expediente concreto pero que, archivados de forma electrónica como consecuencia de su propio modo de transmisión, hacen emerger el problema de su uso no en el mismo expediente en el que es evidente, desde luego, pero, sí la eventualidad de su uso por otros servicios o dependencias de la Administración o de cualquier Administración o en otro expediente. Las normas de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal deben bastar, y no se trata de hacer ninguna innovación al respecto, pero sí de establecer previsiones que garanticen la utilización de los datos obtenidos de las comunicaciones electrónicas para el fin preciso para el que han sido remitidos a la Administración. Por otra parte, los interesados en un procedimiento tienen derecho de acceso al mismo y ver los documentos. Lo mismo debe suceder, como mínimo, en un expediente iniciado electrónicamente o tramitado de esta forma. Dicho expediente debe poder permitir el acceso en línea a los interesados para verificar la situación del expediente, sin mengua de todas las garantías de la privacidad"*.

Y, más adelante, señala *"(…) En este contexto, una Ley para el acceso electrónico de los ciudadanos a las Administraciones Públicas se justifica en la creación de un marco jurídico que facilite la extensión y utilización de estas tecnologías. Y el principal reto que tiene la implantación de las Tecnologías de la Información y las Comunicaciones (TIC) en la sociedad en general y en la Administración en particular es la generación de confianza suficiente que elimine o minimice los riesgos asociados a su utilización. La desconfianza nace de la percepción, muchas veces injustificada, de una mayor fragilidad de la información en soporte electrónico, de posibles riesgos de pérdida de privacidad y de la escasa transparencia de estas tecnologías. Por otro lado, la legislación debe proclamar y erigirse sobre un principio fundamental como es la conservación de las garantías constitucionales y legales a los derechos de los ciudadanos y en general de las personas que se relacionan con la Administración Pública, cuya exigencia se deriva del artículo 18.4 CE, al encomendar a la ley la limitación del uso de la informática para preservar el ejercicio de los derechos constitucionales. Esta conservación exige afirmar la vigencia de los derechos fundamentales no sólo como límite, sino como vector que orienta esta reforma legislativa de acuerdo con el fin promocional consagrado en el artículo 9.2 de nuestro texto fundamental, así como recoger aquellas peculiaridades que exigen la aplicación segura de estas tecnologías. Estos derechos deben completarse con otros exigidos por el nuevo soporte electrónico de relaciones, entre los que debe estar el derecho al uso efectivo de estos medios para el desarrollo de las relaciones de las personas con la Administración. Las anteriores consideraciones cristalizan en un Estatuto del ciudadano frente a la administración electrónica que recoge un elenco no limitativo de las posiciones del ciudadano en sus relaciones con las Administraciones Públicas, así como las garantías específicas para su efectividad. Con este fin, la Ley crea la figura del Defensor del Usuario, que atenderá las quejas y realizará las sugerencias y propuestas pertinentes para mejorar las relaciones de ciudadanos en su trato con las Administraciones Públicas por medios electrónicos"*.

Finalmente, no podemos dejar de señalar en este breve repaso de aquellas disposiciones de la Ley 11/2007 que tienen por objeto la salvaguardia de este derecho fundamental y la generación de confianza a través de dicha protección, la que se contiene específicamente en su artículo 3 y que establece como finalidad específica de la Ley *"(…) 3. Crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos" y en su*

artículo 4 en el que se señala que "(…) La utilización de las tecnologías de la información tendrá las limitaciones establecidas por la Constitución y el resto del ordenamiento jurídico, respetando el pleno ejercicio por los ciudadanos de los derechos que tienen reconocidos, y ajustándose a los siguientes principios: a) El respeto al derecho a la protección de datos de carácter personal en los términos establecidos por la Ley Orgánica 15/1999, de Protección de los Datos de CarácterPersonal, en las demás leyes específicas que regulan el tratamiento de la información y en sus normas de desarrollo, así como a los derechos al honor y a la intimidad personal y familiar".

Asimismo, en la sección consagrada a lo que la Ley llama un Estatuto del Ciudadano ante la Administración Electrónica, dentro del artículo 6, se consagra el derecho de los ciudadanos a *"(…) b) A no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información siempre que, en el caso de datos de carácter personal, se cuente con el consentimiento de los interesados en los términos establecidos por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, o una norma con rango de Ley así lo determine, salvo que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados. El citado consentimiento podrá emitirse y recabarse por medios electrónicos"*.

Igualmente, en la regulación de las comunicaciones de datos entre distintas Administraciones Públicas contenida en el artículo 9, también aparece de modo prominente la necesidad de respetar lo establecido en la normativa de protección de datos cuando dispone que *"(…) Para un eficaz ejercicio del derecho reconocido en el apartado 6.2.b), cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo. 2. La disponibilidad de tales datos estará limitada estrictamente a aquellos que son requeridos a los ciudadanos por las restantes Administraciones para la tramitación y resolución de los procedimientos y actuaciones de su competencia de acuerdo con la normativa reguladora de los mismos. El acceso a los datos de carácter personal estará, además, condicionado al cumplimiento de las condiciones establecidas en el artículo 6.2.b) de la presente Ley"*.

Por todo ello, es evidente que cualquier instrumento o proceso de certificación por parte de una entidad independiente del cumplimiento de la normativa de protección de datos por parte de los productos y servicios ofrecidos por las Administraciones Públicas en el ámbito de las transacciones electrónicas tendrá un indudable efecto generador de confianza respecto de las prácticas de la Administración de que se trate.

Además, hoy en día es cada vez más frecuente que las Administraciones europeas intercambien datos de carácter personal por diferentes motivos así como que los ciudadanos de un determinado Estado miembro soliciten los servicios de Administración Electrónica de una entidad pública de otro Estado, por lo que una certificación de ámbito europeo aporta un valor añadido de interoperabilidad y coadyuva también a la generación de confianza no solo frente a los ciudadanos sino entere distintas Administraciones europeas que deben cooperar para ofrecer servicios a sus ciudadanos y que, de esta manera, tienen un mecanismo objetivo para saber que pueden confiar en las prácticas de protección de datos de otra Administración pública.

En este entorno es en el que se sitúa el **Proyecto EuroPriSe**, cofinanciado por la Comisión Europea a través del programa eTEN, que pretende llenar el vacío existente en este ámbito mediante la puesta en marcha de un mecanismo de certificación que, tras la pertinente evaluación, permita acreditar que un producto o servicio de Administración Electrónica satisface un alto estándar de protección de datos en consonancia con los principios de las normas europeas (Directiva 95/46(CE y Directiva 2002/58/CE, fundamentalmente) y nacionales (en España, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal) y, por ello, puede utilizarse de forma respetuosa con las mismas.

Por lo tanto, el establecimiento de este Sello de Privacidad significará la existencia de un certificado europeo que promueve la protección del consumidor, los derechos civiles y la aceptación de las normas de privacidad mediante mecanismos transparentes que, finalmente, desembocará en nuevas posibilidades de introducción de las Tecnologías de Protección de la Privacidad (PETs en sus siglas en inglés) y un incremento en la confianza en las Tecnologías de la Información.

La Agencia de Protección de Datos de la Comunidad de Madrid participa como socio en este proyecto junto a las autoridades de protección de datos francesa (CNIL) y de Schleswig-Holstein (ICCP, como coordinadora del mismo) y la London Metropolitan University del Reino Unido, VaF s.r.o. de Eslovaquia, Ernst & Young AB Suecia, TÜV

Informationstechnik GmbH de Alemania, la Academia Austríaca de Ciencias – Instituto de Tecnología y Borking Consultancy de los Países Bajos.

Pero antes de seguir adelante con la explicación del proyecto, es necesario realizar una breve presentación de la Agencia de Protección de Datos de la Comunidad de Madrid, creada al amparo de lo establecido en el artículo 41 de la LOPD y que es un Ente de Derecho público de los previstos en el artículo 6 de la Ley 9/1990, de 8 de noviembre, reguladora de la Hacienda de la Comunidad de Madrid, con personalidad jurídica propia y plena capacidad de obrar. Actúa en el ejercicio de sus funciones con plena independencia de la Administración de la Comunidad de Madrid.

Tiene como finalidad garantizar y proteger los derechos fundamentales de las personas físicas respecto al honor e intimidad familiar y personal, en lo relativo al tratamiento de sus datos personales. Sus competencias versan sobre los ficheros de titularidad pública creados o gestionados por la Comunidad Autónoma de Madrid, Entes que integran la Administración Local de su ámbito territorial, Universidades públicas y Corporaciones de derecho público representativas de intereses económicos y profesionales de la misma.

Volviendo a la descripción de EuroPriSe, el mecanismo de certificación que este proyecto propone se basa en la experiencia exitosa de un producto similar en el Länder alemán de Schleswig-Holstein y que ha sido puesto en marcha por la autoridad de control de aquel Länder. Se basa en un sistema de certificación en dos niveles.

En primer lugar, la autoridad de certificación define un procedimiento de acreditación de expertos que deseen participar en el proceso mediante la realización de las correspondientes evaluaciones de los productos y servicios. Todos aquellos profesionales o empresas interesados en prestar el servicio de evaluación pueden optar a dicha acreditación. Si superan el proceso de acreditación -cuyas normas y criterios serán públicos y transparentes- y la autoridad de certificación considera que tienen las necesarias cualificaciones profesionales y satisfacen una serie de requerimientos de solvencia financiera y deontológica, podrán comenzar a ejercer sus funciones como evaluadores.

Las organizaciones interesadas en obtener el sello pueden, de forma completamente voluntaria, contactar con cualquiera de los expertos acreditados para someterse a la evaluación, que deberá llevarse a cabo utilizando los estándares y procedimientos definidos durante el proyecto. Estos estándares partirán de la experiencia existente en

Alemania y se completarán y adaptarán para que puedan ser utilizados en una certificación de ámbito europeo.

Una vez finalizada la evaluación del producto o servicio por el experto, el informe del mismo es remitido a la autoridad de certificación para su revisión. La autoridad de certificación puede aprobar el mismo, pedir aclaraciones o información adicional o, si considera que la revisión no se ha realizado correctamente o que el producto o servicio no satisface los requerimientos establecidos, simplemente rechazar la concesión de sello.

El sello se otorga en una ceremonia pública y tiene una validez de dos años, tras los cuales es necesario recertificar el producto o servicio por si se hubieran producido cambios en el mismo que debieran ser revisados. Los productos aprobados pueden ostentar y mostrar públicamente el sello durante su periodo de validez y se constituirá un Consejo Europeo de Autoridades de Certificación encargado de supervisar que los procedimientos de certificación se aplican homogéneamente en todos los países y con un nivel de exigencia equivalente para evitar lo que se conoce como *"forum shoping"* o, lo que es lo mismo, la elección de un determinado país para obtener el certificado porque el proceso en el mismo sea menos exigente.

Tanto el esquema procedimental como los criterios generales de certificación serán públicos para garantizar la transparencia del proceso. Además, también se hará público un resumen del informe de certificación para dar información adicional sobre el mismo.

El proyecto se divide en seis conjuntos de actividades o (*working packages o WP*), siendo el primero de ellos el que contempla todas las actividades de gestión y control del proyecto.

Los cinco WP operativos son los relativos a Análisis de Mercado y Planificación de Negocio Transeuropeo (WP2), Adaptación y puesta en marcha del servicio transeuropeo de certificación EuroPriSe (WP3), Pruebas piloto y validación del servicio (WP4), Evaluación del servicio (WP5) y Comunicación (WP6). La Agencia de Protección de Datos de la Comunidad de Madrid lidera el WP5 relativo a la evaluación de las pruebas piloto y de planificación de la extensión del modelo al resto de Estados miembros de la Unión Europea.

Por lo tanto, durante el proyecto, se llevarán a cabo al menos seis ensayos completos del proceso en Alemania, Austria, Eslovaquia, España, Reino Unido y Suecia que

comprenderán desde la acreditación de un experto de acuerdo al procedimiento definido, la evaluación de un producto por el experto acreditado y la revisión de todo el proceso por la autoridad de certificación. A aquellos productos que superen el proceso de certificación en el ensayo piloto se les entregará el sello en un acto público y podrán hacer uso de él durante los dos años siguientes.

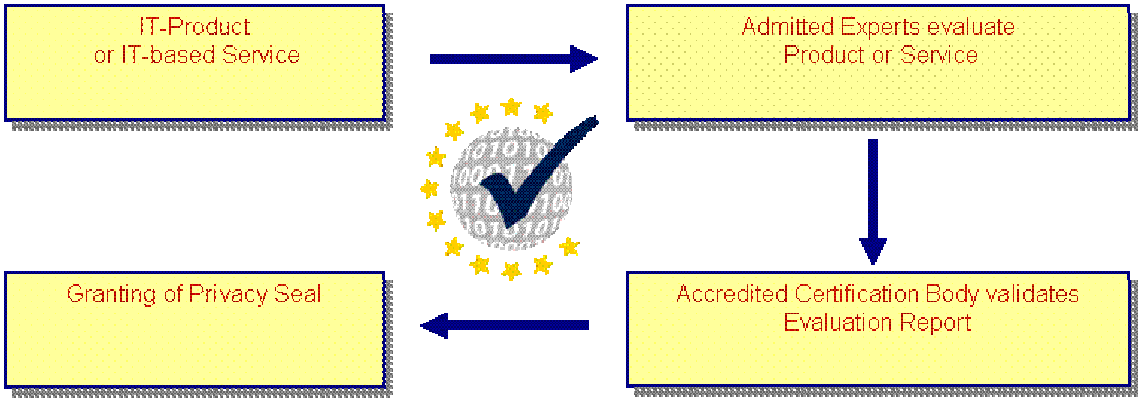
El proyecto comienza con un análisis de mercado, potencial y jurídico, seguido por la adaptación de los procedimientos del sello de Schleswig-Holstein así como con la definición de las pruebas piloto.

En la fase de pruebas y validación, los expertos se someterán al procedimiento de admisión en el que tendrán que probar su capacidad legal y técnica. La lista de expertos admitidos se publicará y podrán ser contactados por las organizaciones que deseen solicitar una certificación para el sello de privacidad.

Los productos y servicios que soliciten el sello deberán pasar el procedimiento de certificación diseñado en el WP3 y serán evaluados por los expertos admitidos. Una autoridad de certificación revisará el informe y, en su caso, otorgará el Sello Europeo de Privacidad. Por supuesto, tanto durante la realización del proceso de acreditación y certificación como a posteriori, los procedimientos y criterios utilizados serán validados y evaluados.

Además, uno de los resultados del proyecto será un plan de negocio para la implantación del servicio en la UE y aportará información detallada y probada sobre los aspectos financieros y legales más importantes de EuroPriSe. El proyecto, como ya se ha adelantado, preparará la institución de un Consejo Europeo del Sello de Privacidad para asegurar la calidad y continuidad del mismo.

Después de describir los pasos del proyecto, vamos a explicar con más detalle el procedimiento de certificación propuesto por EuroPriSe. El esquema de certificación, tal y como se ha comentado anteriormente, está basado en la experiencia del "Guetesiegel" alemán y consiste en una evaluación "en dos pasos" conducida por expertos legales en privacidad y expertos en TI, así como por un organismo de certificación. De una forma gráfica, el esquema sería el siguiente:



Para fabricantes y vendedores, el esquema se compone de cuatro pasos:

1. Selección de un experto: el fabricante o vendedor de un producto o servicio TI selecciona un experto o un centro de evaluación y le encarga llevar a cabo dicha evaluación, para lo cual deben contar con conocimientos legales y técnicos en privacidad y seguridad de datos. Una lista de expertos piloto que han demostrado su experiencia será publicada en el sitio web del proyecto EuroPriSe (www.european-privacy-seal.eu).

2. Evaluación: los expertos realizan los chequeos técnicos y legales en el producto y su documentación. En un primer paso, analizan el producto en lo relativo a su funcionalidad, área legal de aplicación y realización técnica. En un segundo paso, compilan los criterios relevantes de evaluación disponibles en el catálogo de criterios europeos y chequean el producto confrontándolo con estos criterios. Los resultados se entregan al fabricante en un informe de evaluación confidencial.

3. Validación: el fabricante envía el informe de evaluación al organismo de certificación. La tarea del organismo de certificación es asegurar la compatibilidad completa de todos los certificados. Por consiguiente, todos los informes de evaluación son validados respetando la metodología y los criterios de consistencia establecidos. Las cuestiones no identificadas por los expertos o las diferencias en las evaluaciones legales o técnicas entre el experto y el organismo de certificación son resueltas entre el fabricante, el experto y el organismo de certificación. Aunque no es necesario, se recomienda informar al organismo de certificación al comienzo del proceso de evaluación con el objetivo de permitir una adecuada interacción entre expertos y organismo de certificación desde el principio.

4. Certificación: el organismo de certificación aprueba el producto si cumple con la normativa de privacidad y seguridad y otorga el sello de privacidad europeo por un período de dos años. El organismo de certificación divulga a través del sitio web de EuroPriSe un informe público proporcionado por el solicitante.

La evaluación del producto y la validación de la evaluación son los pasos principales del procedimiento de certificación, por lo que vamos a proceder a su explicación detallada.

1. Evaluación: la primera tarea de los expertos es determinar las áreas legales que son relevantes para la evaluación. Estas áreas legales dependen del campo de aplicación del producto o servicio propuesto. Adicionalmente, el producto es analizado respetando su funcionalidad y su realización técnica. El objetivo es preparar un inventario detallado de los datos procesados. Si fuera necesario, el fabricante debe proporcionar documentación interna adicional para los expertos (especificaciones, anteproyectos, etc.)

   No todos los criterios disponibles en el catálogo de EuroPriSe son relevantes para cada tipo de datos procesados. El catálogo es una colección de todos los posibles criterios aplicables. Los expertos legales y técnicos escogen aquéllos que son relevantes respetando el área legal, el tipo de datos y la realización, y compilan un conjunto de criterios individuales adecuados para el producto con respecto al área de aplicación. El proyecto examinará si es útil compilar conjuntos de plantillas con los criterios (a veces llamados “perfiles de protección”) para productos típicos. Por supuesto, es deseable tener estos conjuntos al principio del proyecto, pero la decisión de si estos conjuntos son útiles y si merece la pena compilarlos debe realizarse después de la certificación piloto, y con respecto a tipos de productos y servicios que se prevea vayan a ser certificados.

   Los expertos evaluarán el producto o servicio de acuerdo al catálogo individual y entregarán sus conclusiones en un informe. Para facilitar la realización de este informe, hay una plantilla disponible. Es posible la emisión de dos informes separados, uno del experto legal y otro del experto técnico, o un único informe conjunto. Este informe puede contener secretos industriales o de negocio y está dirigido al fabricante. Lo ideal sería que el informe de evaluación diera respuesta a todas las cuestiones que una autoridad de protección de datos preguntaría con el fin de comprender cómo funciona un producto o servicio, qué

datos personales pueden ser procesados y qué regulaciones legales están afectadas.

2. Validación: el informe de evaluación es enviado al certificador para su revisión. Si el certificador comprueba que el producto cumple con los requisitos de cumplimiento de la legislación sobre privacidad y seguridad y la implantación de las mejores prácticas promovidas por EuroPriSe, se le otorga el Sello de Europeo de Privacidad. Aunque el certificador no llevará a cabo una segunda evaluación, durante el proceso se pueden plantear cuestiones específicas sobre el producto, su facilidad de uso y el campo de aplicación. Estas cuestiones tienen que ser respondidas por los expertos o por el fabricante.

   La principal tarea del certificador es asegurar la compatibilidad de todos los resultados de la evaluación con las regulaciones en protección de datos y los criterios definidos por EuroPriSe ya que las opiniones de los expertos en lo relativo a un tema específico pueden diferir. El certificador proporcionará criterios para resolver estas situaciones, ya que el organismo de certificación es el responsable de la decisión de certificación, no los expertos.

   Debido a los posibles y algunas veces frecuentes cambios en las regulaciones legales y al rápido desarrollo de las tecnologías de la información, una recertificación es necesaria pasados dos años. El procedimiento de recertificación puede ser rápido o más complejo dependiendo de los cambios que se hubieran producido en la regulación o en el mismo producto. Cambios menores del producto durante el período de dos años no implican, normalmente, una reevaluación completa. Si el fabricante decide innovar o cambiar el producto de un modo que afecte al cumplimiento con la legislación sobre privacidad y protección de datos (por ejemplo, creando nuevas interfaces, cambiando el campo de aplicación y el entorno), puede ser necesaria una evaluación adicional por los expertos o, incluso, una nueva evaluación y certificación dentro del período de dos años.

Del análisis de viabilidad realizado durante la fase de preparación del proyecto se deduce que las oportunidades que el Sello Europeo de Privacidad proporciona así como sus fortalezas hacen que, aunque existiendo riesgos potenciales, estos se vean ampliamente compensados por las posibilidades y expectativas del mismo.

Al mismo tiempo, algunas de las aportaciones de EuroPriSe hacen que se disminuyan algunos de los riesgos ya que, por ejemplo, la efectiva puesta en marcha de un

mecanismo de certificación de estas características contribuye a la aplicación efectiva y al cumplimiento de la legislación sobre privacidad y protección de datos, ya que establece un estándar que traduce a un lenguaje claro, concreto y más cercano a las reglas de negocio que el necesariamente genérico y abstracto de la legislación, los principios y garantías que deben implantarse en los productos y servicios que tratan datos personales.

Igualmente, junto con este estándar redactado en términos concretos y directamente aplicables a las organizaciones, EuroPriSe proporciona un procedimiento claro y transparente para verificar si un producto o servicio puede utilizarse con un alto nivel de respeto a la normativa europea de protección de datos personales además de establecer los requisitos que deben poseer los expertos para capacitarles para la realización de las evaluaciones con vistas a la obtención del Sello Europeo de Privacidad.

Así, a través de estos mecanismos, los responsables de productos y servicios de TI pueden acudir a este sistema voluntario de certificación para acreditar su compromiso con el respeto a los derechos de las personas y, en particular, con su derecho a la protección de datos y, al mismo tiempo, obtener una identificación clara de que sus productos y servicios son dignos de confianza por parte de los ciudadanos y de otros actores del sector público o privado con el que se relacionan como proveedores o clientes, ya que estos tienen un sistema fácil para comprobar que los mismos se esfuerzan en el cumplimiento de sus obligaciones en materia de protección de datos.

Del mismo modo, como consecuencia de la “traducción” de los principios de la norma de privacidad a elementos concretos y claramente comprobables, EuroPriSe se puede convertir en un elemento de capital importancia para mejorar la comprensión y las implicaciones de esta regulación tanto para los responsables de tratamientos públicos y privados como para el público en general, que podrá verificar mediante la consulta de los estándares y procedimientos y de los informes de certificación de los productos lo que significan en la práctica los principios jurídicos y los derechos legales que les confieren las leyes de protección de datos. Y esta mejor comprensión mejorará también, sin duda alguna, la concienciación y educación de los ciudadanos europeos sobre los derechos que tienen y las obligaciones que las leyes imponen a aquellos que tratan sus datos personales.

Finalmente, hay que concluir que un esquema independiente de certificación como el que propone EuroPriSe puede ser un elemento de gran importancia, un catalizador de la generación de confianza por parte de los ciudadanos en los servicios electrónicos

que recibe y, en particular, de que en la interacción con las Administraciones Públicas a través de los servicios de e-Administración, sus datos personales serán procesados con total respeto a los principios de finalidad y confidencialidad que la legislación exige, pero no solo porque el respeto a la ley sea obligatorio, y más especialmente si cabe para las AA.PP., sino porque los servicios habrán sido evaluados y certificados por terceros independientes para verificar si realmente las buenas prácticas necesarias para que ese respeto se produzca han sido realmente desplegadas e implantadas.