LA PROTECCIÓN DE DATOS Y LA ADMINISTRACIÓN ELECTRÓNICA

Montaña Merchán Arribas

Ministerio de Hacienda y Administración Pública

Usted es libre de:

Compartir - copiar, distribuir, ejecutar y comunicar públicamente la obra

hacer obras derivadas

Bajo las condiciones siguientes:

Atribución — Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciante (pero no de una manera que sugiera que tiene su apoyo o que apoyan el uso que hace de su obra).

No Comercial — No puede utilizar esta obra para fines comerciales.

CONTENIDO

Protección de datos y Administración Electrónica

CONCEPTO DE PROTECCIÓN DE DATOS

En el artículo 18.4 de nuestra Constitución se obliga especialmente a los poderes públicos a limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de los derechos.

La protección de los datos personales es un derecho fundamental, que deriva directamente de la Constitución y como tal derecho fundamental ha de ser respetado por todos, comenzando por la concienciación del propio sujeto titular de los datos.


Constitución Española
Don Juan Carlos I.
Rey de España.
A todos los que la presente vieren y entendieren.
Sabed: que las Cortes han aprobado y el Pueblo español ratificado la siguiente Constitución.

La Constitución Europea reconoce en dos ocasiones el derecho fundamental a la protección de datos:

En el artículo I-51 de Protección de datos de carácter personal (Parte I título VI De la vida democrática de la Unión), en el que reconoce que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan y que se establecerán normas respecto del tratamiento de datos de carácter personal.

En el artículo II-68 (Parte II título II Libertades), en el que se impone la base del consentimiento y se limita el uso así como el derecho a rectificación.

En nuestro ordenamiento jurídico este derecho fundamental está regulado por la Ley Orgánica 15/1999 (LOPD) que traspone la Directiva 95/46/CE (Directiva sobre protección de datos) y que dispone que será la Agencia Española de Protección de Datos la encargada de tutelar y garantizar ese derecho.

La protección de datos atribuye a los ciudadanos el poder disponer de sus datos e intenta garantizar, al titular de los mismos, que ya se trate del sector público o privado, los terceros van a utilizar sus datos personales con respeto, en base a su consentimiento e informándole en todo momento del uso que hacen de ellos.

Para entenderlo, no hay que olvidar que los datos de carácter personal son propiedad del interesado o los afectados, no de la administración, y consecuentemente todo tratamiento de los mismos debe hacerse con el respeto de los principios y derechos que sobre ellos contempla la Ley Orgánica de Protección de Datos de Carácter personal (LOPD).

En casi todas las actividades de nuestra vida cotidiana se recogen nuestros datos personales: para abrir una cuenta en un banco, para contratar energía, para comprar un billete de avión, para el comercio electrónico, para la asistencia médica, para el club de golf, etc.

Las administraciones públicas también necesitan, para realizar con eficacia su gestión administrativa, conocer o tratar datos personales y esto es así tanto si

la administración es o no electrónica. Ahora bien, esta actividad de la administración debe ser respetuosa con este derecho fundamental y en ningún caso vulnerarlo.

Es cierto que la informática y las telecomunicaciones han facilitado, desde hace tiempo, el tratamiento, el intercambio y la copia de los datos, en el ámbito privado y en el público. Además la Administración electrónica ha abierto nuevos canales de relación con los ciudadanos, de manera que esa relación, que antes era presencial, ahora puede ser telefónica o a través de Internet. Por ello, es indispensable una revisión de cómo la implantación y uso de la administración electrónica, se conjugan con este derecho fundamental.

PROTECCIÓN DE DATOS EN LA ADMINISTRACIÓN ELECTRÓNICA

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en adelante LAECSP, ha consagrado el derecho de éstos a comunicarse con las Administraciones por medios electrónicos, pero a la vez ha impuesto a la administración la obligación de poner los medios adecuados para garantizar la protección de datos.

Desde los principios generales esta Ley ya marca que “debe procurarse en la implementación de las relaciones electrónicas con el ciudadano, el derecho a la protección de datos de carácter personal en los términos establecido en la LOPD”.

La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico (LCE) también hace referencia a la necesidad de proteger los datos en las comunicaciones comerciales por vía electrónica.

Y de igual manera, la Ley 59/2003, de 20 de diciembre, de firma electrónica (LFE) hace referencia a la necesidad de proteger los datos, en el tratamiento de los mismos que los prestadores de servicios de certificación precisen hacer para el desarrollo de su actividad.

Es inherente a la Administración electrónica la utilización de la informática y las redes de telecomunicaciones para que el ciudadano pueda acceder de manera electrónica a la información, a los servicios públicos y/o presente cómodamente su solicitud desde cualquier lugar, de forma telemática y a distancia. En este momento la Administración General del Estado tiene el 98% de los procedimientos adaptados a la LAECSP y el ciudadano puede realizar casi el 99% de los trámites a través de Internet. Puede presentar la declaración de la renta, pedir su vida laboral, consultar los puntos de su permiso de conducir, solicitar una beca, matricularse en la Universidad, consultar los datos de empadronamiento, pagar sus impuestos, constituir una empresa, etc.

La Administración electrónica supone no sólo la utilización de las tecnologías en el interfaz con el ciudadano sino también en todas las fases del procedimiento administrativo. El tratamiento informatizado de los datos y el almacenamiento en las bases de datos influye en las tareas internas de la gestión administrativa, automatizándolas, facilitando las tareas habituales y repetitivas. Pero también condiciona a establecer medidas y responsabilidades

en torno a la seguridad de los datos, tanto de acceso a los sistemas, como a su transmisión o cesión.

Tal y como refleja la LOPD, los riesgos de vulneración de la privacidad personal están asociados a cualquier tratamiento de los datos personales, no exclusivamente a los automatizados. Por tanto, hay realizar ineludiblemente un análisis de riesgos y tomar las medidas adecuada para evitarlos, minimizarlos o derivarlos.

La encuesta de 2012 sobre Equipamiento y Uso de Tecnologías de Información y Comunicación (TIC) en los Hogares, realizada por el Instituto Nacional de Estadísticas, muestra que el 44,7% de la población ha interactuado en ese año alguna vez con las administraciones Públicas a través de Internet. El 59,4% de usuarios de Internet para obtener información de las web de la Administración, el 41,0% afirma haber descargado formularios oficiales y el 32,2% ha enviado formularios cumplimentados. Todavía son pocos los usuarios que confían en la Administración electrónica y esa adopción tiene que mucha que ver con la confianza que éstos depositen en los servicios electrónicos. Y esta confianza se basará en tres pilares:

A. Conocer el funcionamiento
B. Tener la seguridad de la validez jurídica de las transacciones
C. Respetar los derechos fundamentales de privacidad y protección de datos personales.

Aún más, sólo si protegemos los datos personales podemos establecer la relación de confianza necesaria para el desarrollo de las nuevas tecnologías de

la información y la comunicación en la sociedad y en las Administraciones Públicas.

Por eso es de suma importancia la concienciación y capacitación de los empleados públicos en la protección de los datos. Tema que ya señala la LAECSP, en la disposición adiciona segunda, al referirse a necesidad de formación de los empleados públicos en la protección de datos y el uso correcto de los medios electrónicos en la actividad administrativa.

El principio de transparencia y publicidad del procedimiento aparece en la LAECSP en el artículo 4 k), por el cual el uso de medios electrónicos debe facilitar la máxima difusión, publicidad y transparencia de las actuaciones administrativas. La protección de datos también afecta a la transparencia administrativa, entendida como "el derecho de acceso a la información administrativa o el derecho de tener información relativa a la actividad de la gestión pública".

La Ley de transparencia ha adquirido destacada trascendencia en Gobierno, esta Ley dedica el artículo 12 a la protección de datos personales.

En el contexto de la democracia, el Derecho a la Transparencia Administrativa es una obligación de toda Administración Pública. Pues como definió Noberto Bobbio hace años: "la democracia es el Gobierno del Poder Público en Público"

PRINCIPIOS DE LA PROTECCIÓN DE DATOS

El derecho fundamental de la protección de datos se desarrolla en la LOPD mediante unos “principios de la protección de datos” que, como veremos, tienen su revalidación en la LAECSP y que deben ser tenidos en cuenta por cualquier organización a la hora de implantar la Administración electrónica.

El tratamiento de datos de carácter personal ha de realizarse de acuerdo con los principios de calidad, información, consentimiento, finalidad, y seguridad.

Por ceñirnos al espacio estipulado, mencionaremos aquellos principios que est esenciales para el funcionamiento de la Administración electrónica y que deben aplicarse en las fases de recabar los datos, el tratamiento y la transmisión.

En resumen, se trata responder a las preguntas que el ciudadano puede plantear acerca de la privacidad de sus datos personales:

- ¿Qué datos necesita la administración recoger y con qué finalidad?
- ¿Qué sujetos tendrán acceso a mis datos?
- ¿Cómo se transmiten mis datos?
- ¿Qué seguridad se aplica?

Principio de calidad de los datos:

¿Qué datos necesita la administración recoger y con qué finalidad?

Los datos que la administración recabe deben tener un fin determinado, explícito y legítimo. Deben ser adecuados, pertinentes y no excesivos en relación con el ámbito y los fines para los que se han recogido y también es

necesario que la información sea exacta. Además no podrán permanecer más tiempo del necesario para cumplir con al finalidad para la que se obtuvieron.

La LAECSP, ya desde su exposición de motivos (apartado III) hace una referencia concreta el principio de calidad de los datos señalando que las normas de la LOPD deben bastar para ello.

Pero además, específicamente recoge el **Principio de proporcionalidad** en cuya virtud sólo se requerirán a los ciudadanos, en sus relaciones telemáticas con la administración, aquellos datos que sean estrictamente necesarios en atención a la finalidad para la que se soliciten. Por si sólo este principio ya es aplicable para obligar a revisar los formularios electrónicos, así como para replantear los documentos adicionales que en algunos casos se piden por costumbre.

La aplicación de este principio a la administración electrónica se plasma en tres puntos:

El **primero** sería el análisis del nivel de seguridad exigido para la identificación del ciudadano. No tiene la misma exigencia de identificación la consulta de los datos tributarios o la consulta del la titulación universitaria. En cada caso, se aplicará el nivel determinado por el análisis de riegos que supondría un acceso indebido, clave concertada o exclusivamente con certificado digital. A mayor riesgo mayor debe ser el nivel de seguridad.

Fig. 1: diferentes grados de seguridad en la identificación

El **segundo** punto es recabar estrictamente aquellos datos y documentos necesarios para la resolución del procedimiento administrativo. Por si no fuera suficiente el principio de proporcionalidad, el *artículo 34. De Criterios para la gestión electrónica*, también aboga por la simplificación de la documentación que se pide al ciudadano.

La LAECSP, establece el derecho del ciudadano a no aportar los datos y documentos que obren en poder de las Administraciones Públicas (art. 6.2 b). Si bien, este derecho de los ciudadanos no es nuevo puesto que ya estaba incluido en la LRJ-PAC (art. 35), no en todos los casos el interesado ha podido ejercitar ese derecho.

El **tercer** punto es que para ejercer este derecho es necesaria la interoperabilidad entre administraciones.

En este sentido, el Real Decreto 522/2006, de 28 de abril, suprimió la aportación de fotocopias de documentos de identidad en los procedimientos

administrativos de la Administración General del Estado y el Real Decreto 523/2006, de 28 de abril, suprimió la exigencia de aportar el certificado de empadronamiento, como documento probatorio del domicilio y residencia. Pues bien, esta aportación es innecesaria en los procedimientos electrónicos ya que la identificación digital ya proporciona los datos correctos de identidad y porque la administración puede verificarlos a través de la plataforma de intercambio de datos.

Tampoco el intercambio de datos debe suponer una limitación en el derecho fundamental a la protección de datos personales. El intercambio, igualmente, tiene que respetar este principio de proporcionalidad y de finalidad de forma que la información que se transmita esté limitada estrictamente a aquellos datos necesarios para la resolución del procedimiento administrativo. Estos intercambios no están exentos de control pues deben estar autorizados por el cedente que custodia los datos y garantizar la trazabilidad. Efectivamente, en la autorización deberá constar el procedimiento administrativo y el cesionario, no admitiéndose autorizaciones genéricas para cualesquiera procedimientos o funciones, que pueda desarrollar el organismo requirente.

.

Los beneficios que para los ciudadanos se derivan de la simplificación de la documentación a aportar han sido cuantificados aplicando el “Método simplificado de medición de cargas administrativas y de su reducción”. El ahorro unitario puede estar entre los 4 o 5 euros.

En este sentido en el “Plan de reducción de cargas administrativas y simplificación de documentos” se ha hecho una labor importante, en

colaboración con todos los Departamentos y con muy buenos resultados. De la aplicación del mismo se cifra en unos 28.500 M euros el ahorro que ha supuesto para ciudadanos y empresas el uso de la administración electrónica.

Por otra parte, en 2012 se hicieron 22.606.683 transacciones (consultas y verificaciones de datos) a través de la plataforma de intermediación de datos. La mayoría fueron consultas de datos de identidad y de domicilio, sin embargo también se consultaron datos catastrales, titulaciones académicas, datos de desempleo o cuotas de Seguridad Social o tributarias. El ciudadano no ha tenido que presentar en sus trámites, ni las fotocopias ni los certificados en papel que acreditan estos datos.

Si bien tecnológicamente es posible sustituir los certificados en papel por la transmisión de datos entre administraciones, la proyección de esta ventaja a los procedimientos administrativos está siendo realmente lenta. Es necesario agilizar este proceso de reducción de cargas.

Pero quizá, uno de los resultados más ventajoso es el aumento de la calidad de los datos y la consiguiente eliminación y/o detección de fraude. A los beneficios intrínsecos de intercambio de datos entre administraciones, de la lista, hay que sumar el ingreso por la disminución del fraude:

- La identificación digital acredita la identidad sin lugar a dudas;
- En la recogida de datos, se puede realizar un control más exhaustivo reduciendo errores;
- La firma electrónica asegura la integridad de la información.

- La cesión directa de los datos desde el organismo cedente, mejora la actualización y no da lugar a manipulaciones.

Principio del consentimiento

¿Qué sujetos tendrán acceso al dato? ¿Cómo se transmite el dato?

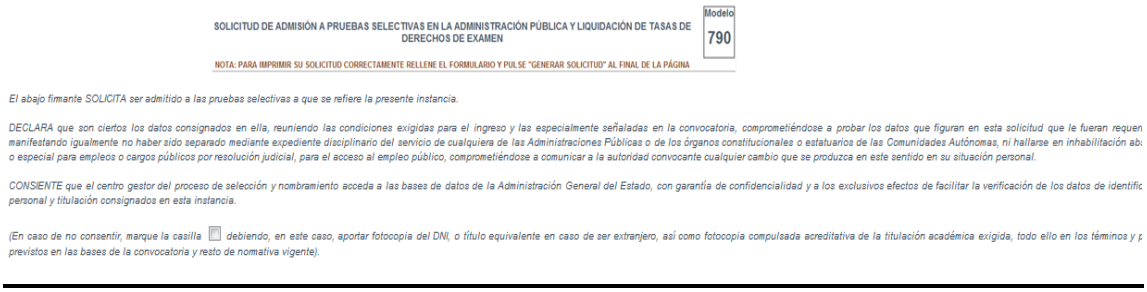
No podemos hablar de intercambio o cesión de datos y protección de los mismos, sin tratar el tema del consentimiento del ciudadano. Este principio de la LOPD infiere que el titular de los datos decide sobre cuándo, dónde y cómo se dan a conocer sus datos a terceros y por ello hay que recabar su consentimiento cuando éste es exigible.

En relación con las cesiones, el artículo 11.1 de la LOPD indica que “Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado”. No obstante, este consentimiento no será preciso, según el artículo 11.2 a) cuando una norma con rango de Ley otorgue cobertura a la cesión planteada.

En lo que respecta a la obtención del consentimiento en los casos en los que resulte necesario, la LOPD deja claro que éste debe ser **libre, específico, informado e inequívoco**. Por lo que deja abierta la posibilidad de recabar este consentimiento de forma **tácita o expresa**. La misma LOPD, hace una

excepción para los casos contemplados en el artículo 7 [(1)], que será expreso y por escrito.

La LAECSP habla en la exposición de motivos (apartado IV), de consentimiento del ciudadano. Sin embargo, hay que puntualizar distintos casos:



SOLICITUD DE ADMISIÓN A PRUEBAS SELECTIVAS EN LA ADMINISTRACIÓN PÚBLICA Y LIQUIDACIÓN DE TASAS DE DERECHOS DE EXAMEN

Modelo 790

NOTA: PARA IMPRIMIR SU SOLICITUD CORRECTAMENTE RELLENE EL FORMULARIO Y PULSE "GENERAR SOLICITUD" AL FINAL DE LA PÁGINA

El abajo firmante SOLICITA ser admitido a las pruebas selectivas a que se refiere la presente instancia.

DECLARA que son ciertos los datos consignados en ella, reuniendo las condiciones exigidas para el ingreso y las especialmente señaladas en la convocatoria, comprometiéndose a probar los datos que figuran en esta solicitud que le fueran requeri manifestando igualmente no haber sido separado mediante expediente disciplinario del servicio de cualquiera de las Administraciones Públicas o de los órganos constitucionales o estatuarios de las Comunidades Autónomas, ni hallarse en inhabilitación abs o especial para empleos o cargos públicos por resolución judicial, para el acceso al empleo público, comprometiéndose a comunicar a la autoridad convocante cualquier cambio que se produzca en este sentido en su situación personal.

CONSIENTE que el centro gestor del proceso de selección y nombramiento acceda a las bases de datos de la Administración General del Estado, con garantía de confidencialidad y a los exclusivos efectos de facilitar la verificación de los datos de identific personal y titulación consignados en esta instancia.

(En caso de no consentir, marque la casilla ☐ debiendo, en este caso, aportar fotocopia del DNI, o título equivalente en caso de ser extranjero, así como fotocopia compulsada acreditativa de la titulación académica exigida, todo ello en los términos y p previstos en las bases de la convocatoria y resto de normativa vigente).

Fig. 2: Consentimiento en el formulario 790 de inscripción a pruebas selectivas

A.-Procedimiento administrativo.

La iniciación de un procedimiento administrativo a solicitud de interesado por medios electrónicos requiere de la puesta a disposición de los correspondientes formularios de solicitud en la sede. En los formularios de solicitud el interesado aporta datos personales de diversa índole, como el nombre, el domicilio, la titulación académica, grado discapacidad, etc.

El artículo 35.3. de la LAECSP, dice expresamente que "con objeto de facilitar y promover su uso, los sistemas de solicitud podrán **incluir comprobaciones automáticas de esta información aportada** respecto de datos almacenados en sistemas propios o pertenecientes a otras administraciones e, incluso,

[1] Respecto la obtención del consentimiento debe ser expreso cuando se trate de datos de ideología, afiliación sindical, religión y creencias, (art 7 LOPD). O para datos relacionados con la salud, sexualidad u origen racial.

ofrecer el formulario cumplimentado, en todo o en parte, con objeto de que el ciudadano verifique la información y, en su caso, la modifique y complete".

Es decir, la LAECSP permite que se pueda realizar la verificación de los datos que aporta el ciudadano de manera automática. Evidentemente esta comprobación no exime de cumplir con el deber de informar al ciudadano.

B.-Comunicarse con el ciudadano.

La LAECSP exige consentimiento expreso cuando se trata de comunicarse con el ciudadano de forma electrónica o para que un funcionario realice trámites en nombre del ciudadano.

Este es el caso de la notificación electrónica, pues para ser notificado electrónicamente se requiere que el interesado haya señalado dicho medio como preferente o haya consentido su utilización.

Del mismo modo, para llevar a cabo la representación del interesado por funcionario público conforme a lo previsto en el artículo 22 de la Ley 11/2007, de 22 de junio, en los servicios y procedimientos para los que así se establezca, se requiere que el ciudadano preste consentimiento expreso, debiendo quedar constancia de ello.

C.- Intercambio de datos entre administraciones.

El artículo 6.2 b de intercambio de datos entre administraciones, cuando específicamente trata el tema del facilitar los datos a otra administración, remite a los términos establecidos por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal para recabar el consentimiento de los interesados, o a tener una norma con rango de Ley que permita recabarlos sin el consentimiento[2].

Se deduce, pues, que para el intercambio de datos el consentimiento debe ser inequívoco y puede ser tácito o expreso, siempre y que los datos de carácter personal no corresponden con los indicados en el artículo 7.

El consentimiento tácito está siendo uno de los puntos más controvertidos en relación con la prestación de servicios electrónicos al ciudadano. El problema del consentimiento tácito es la prueba, sin embargo en el mundo electrónico esa prueba es fácil de conseguir:

- Informando expresamente que el ejercicio del derecho implica el consentimiento.
- Incluyendo en el formulario una casilla de consentimiento
- Imposibilitando realizar el proceso sin el consentimiento (caso de la expedición de DNI electrónico para comprobar datos de residencia).

[2] La normativa de la Agencia Tributaria, permite consultar el domicilio de un ciudadano sin consentimiento previo, dado que esta información en la tramitación de un procedimiento de apremio, tiene una clara trascendencia tributaria, en la medida que el domicilio fiscal de las personas físicas coincide con su residencia habitual

- Obligando a seleccionar un elemento (caso de la validación de certificados digitales)

En los servicios electrónicos, asociados a la administración electrónica, el consentimiento puede recabarse y emitirse por medios electrónicos, bien marcando la casilla o aceptando las condiciones en una pantalla emergente, o cualquier otra forma que permita acreditar ese consentimiento. Para el canal telefónico puede utilizarse un sistema de grabación simple o con comunicación certificada que proporciona total seguridad jurídica. El modo de recabar este consentimiento debe ser simple y rápido sin que conlleve un aumento de carga para el ciudadano y o de retraso en los procesos.

En cualquier caso, el consentimiento se recaba para una finalidad y una actividad del cesionario de la cual el afectado debe estar informado siendo responsabilidad del que trata los datos custodiar la prueba del consentimiento. Y pr tanto responsable de incluir funcionalidades en lo procedimientos automatizados que permitan conservar y acreditar en el futuro la existencia de consentimiento.

C.- Los datos en Internet .

En muchos servicios que se encuentra en Internet se piden datos personales. Aportamos datos en las redes sociales, en los portales comerciales, o en los servicios de suscripción. Si bien los datos se facilitan voluntariamente, el interesado tiene el derecho a la cancelación de los datos una vez finalizada la

relación y siempre habría que informar al ciudadano mediante las políticas de seguridad.

Además siempre hay que asegurar la fiabilidad y seguridad que nos ofrece estos sitios y aportan tan sólo los datos necesarios para la finalidad con la que están siendo recabados.

Debe informarse al ciudadano, también en los servicios de suscripción, del uso de sus datos y la posibilidad de cancelar la suscripción y borrar sus datos. Así como de las estadísticas que se elaboren.

Es recomendable que el ciudadano marque una casilla de "haber leído las condiciones".

Las Administraciones deben tener en cuenta cumplir con estas condiciones en aquellas actividades que no constituye un procedimiento administrativo, como son los servicios de suscripción de alertas o de buzones de sugerencia.

Otro punto a tener en cuenta son las cookies. Las cookies son ficheros que se almacenan en el ordenador del usuario que navega a través de Internet y que, almacenan información de la navegación.

El artículo 5.3 de la Directiva 2009/136/CE, que modifica la Directiva 2002/58/CE ha reforzado la protección de los usuarios de las redes y servicios de comunicaciones electrónicas, al exigir el consentimiento informado antes de que la información se almacene en su terminal. Aunque el requisito se

aplica a todos los tipos de información almacenada o acceso al usuario de dispositivo terminal, la mayo parte de la discusión se ha centrado en el uso de cookies.

El Artículo 5.3 permite que algunas cookies queden exentas del requisito de obtener el consentimiento informado, si cumplen uno de los siguientes criterios:

- que la cookie se utilice "al solo fin de efectuar la transmisión de una comunicación a través de una red de comunicaciones electrónicas";
- "en la medida de lo estrictamente necesario a fin de que el proveedor de un servicio de la sociedad de la información preste un servicio expresamente solicitado por el abonado o el usuario".

Por su parte, la Agencia Española de Protección de Datos (AEPD) y los representantes de la industria han elaborado, en 2013, la primera guía en Europa sobre el uso de las cookies. En esta Guía sobre el uso de las cookies se recogen las orientaciones, para conciliar el uso de las cookies con la protección de la privacidad de los ciudadanos.

Las soluciones recogidas en la Guía ofrecen las líneas básicas para cumplir con las obligaciones previstas en el artículo 22.2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI) tras su modificación por el Real Decreto-ley 13/2012, de 30 de marzo.

En este sentido, hay que recordar que el Grupo de Trabajo del Artículo 29 en su Dictamen 4/2012 ha señalado que existen una serie de *cookies* exceptuadas, cuando se utilizan sólo con el fin de efectuar la transmisión de una comunicación, o en la medida que resulte estrictamente necesario para la prestación de un servicio expresamente solicitado por el destinatario, como son las de entrada del usuario, las *cookies* de autenticación o identificación o de seguridad, entre otras.

Principio de cesión o comunicación de los datos

Una cesión de datos es un tratamiento de datos que supone su revelación a una persona distinta del interesado. La LOPD detalla que únicamente pueden ser cedidos para fines directamente relacionados con las funciones del cedente y del cesionario y con el consentimiento del interesado salvo excepción prevista en la Ley.

En la práctica, las comunicaciones de datos en el ámbito de la administración pública pueden dar lugar al menos a tres escenarios diferentes:

a) Cuando se comunican datos **a** las Administraciones Públicas.
b) Cuando se comunican datos **desde** las Administraciones Públicas.
c) Cuando se comunican datos **entre** Administraciones Públicas.

<u>En el primer caso: se comunican datos a las Administraciones Públicas</u>

La LAECSP exige a los servicios electrónicos se acceda desde las sedes electrónicas. La sede debe estar identificada y establecer comunicaciones seguras. Esto significa que los datos que el interesado comunica a la Administración en los formularios van cifrados con una comunicación Secure Sockets Layer SSL.

En el segundo caso: se comunican datos desde las Administraciones Públicas

En este caso se encuentran las notificaciones electrónicas y también las publicaciones online en boletines o tablones cuya repercusión sobre los derechos de la persona puede ser alta.

En el caso de las notificaciones se garantiza que sólo el interesado puede tener acceso a su contenido por medio de la identificación con certificado digital, tanto si la notificación se realiza por comparecencia o por el servicio de dirección electrónica habilitada. El contenido de la notificación puede ir cifrado con una clave intercambiada únicamente en el proceso de aceptación de la notificación que a su vez irá cifrada con la clave pública del certificado del interesado. Lo cual garantiza que nadie tenga acceso al contenido.

En el caso de los boletines o tablones, en general, la difusión se hace sin el consentimiento de la persona afectada, pues la legitimación de estas publicaciones se basa en una habilitación legal. Pero ¿es legal que las Administraciones públicas publiquen datos personales en los Boletines Oficiales?

En los Boletines Oficiales se publican, infracciones, resoluciones administrativas, etc. Información que se ha publicado habitualmente en los boletines en papel, pero las capacidades de indexación automática de los buscadores web y el almacenaje de esta indización en sus sistemas, ha levantado la polémica.

Los diarios oficiales son fuentes de acceso público, de conformidad con lo dispuesto en el artículo 3, apartado j) de la Ley Orgánica 15/1999, lo cual

permite su consulta por cualquier persona que tenga acceso, y legitima ciertos usos de dicha información de acuerdo a la LOPD, incluida la cesión de dichos datos a terceros sin consentimiento del interesado. El problema es que los buscadores de Internet indexan la información de los boletines, manteniendo "eternamente" los datos en Internet, aunque estén fuera de plazo o se hayan modificado. Una vez publicado es casi imposible ejercer el derecho de "olvido"[3].

Es fundamental buscar un equilibrio entre la posible lesión a derechos de los ciudadanos y la publicación en internet y en todo caso, limitar la publicación a los datos personales imprescindibles del acto.

Puesto que el principio del derecho al olvido, en los que se refiere a la información difundida en Internet, es de difícil aplicación, hay que optar por tomar medidas técnicas en la publicación. No publicar en abierto de datos que puedan ser lesivos y derivarlos a una zona privada; generar un archivo, 'robots.txt', que permite dar ciertas directivas a los spiders de los buscadores (google, yahoo…) y no indexar ninguna de las páginas del boletín.

El tercer caso: se comunican datos entre Administraciones Públicas

Concierne a los intercambios de datos entre las Administraciones Públicas y es el más interesante desde el punto de vista de la LAECSP, en cuanto que en el ámbito de la administración electrónica la interoperabilidad es uno de los

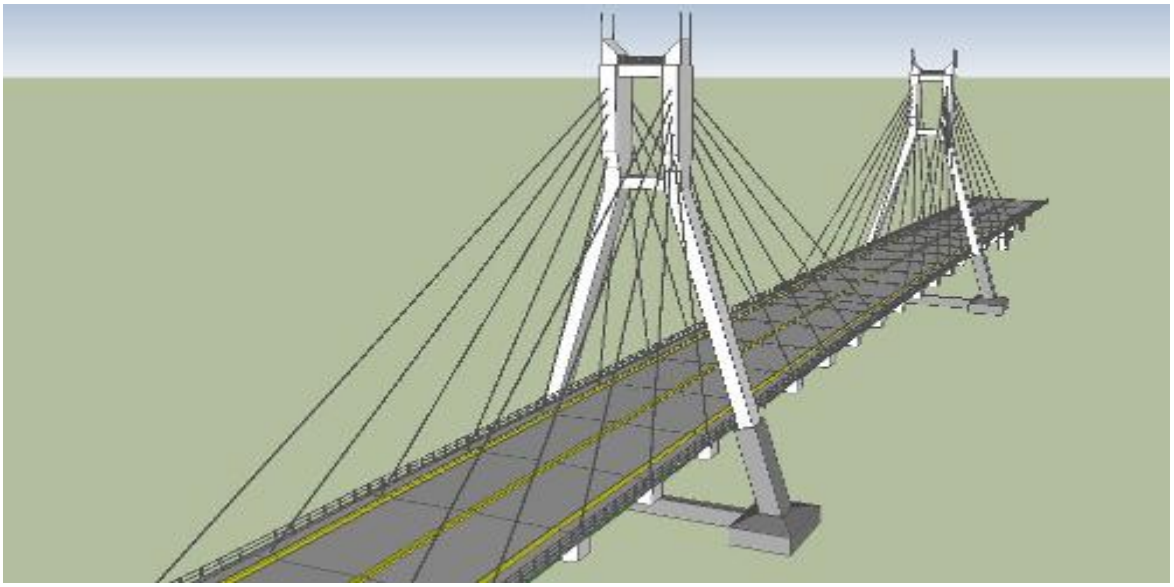
[3] Este debate ha llevado a la Agencia de Protección de Datos de la Comunidad de Madrid (APDM) a preparar la "Recomendación 2/2008, sobre publicación de datos personales en boletines y diarios oficiales en Internet, en sitios webs institucionales y en otros medios electrónicos y telemáticos".

mecanismos que facilitan los servicios más adaptados a los eventos vitales de los ciudadanos, pero que entraña un cierto volumen de cesiones de datos personales.

La interoperabilidad y el intercambio de datos cobran clara importancia en el ámbito de la Unión europea. Así, la Agenda Digital plantea avanzar hacia unos servicios públicos transfronterizos a través de Internet, que contribuyan al desarrollo del mercado único y a facilitar la movilidad de los ciudadanos europeos en cualquier país de la Unión Europea.

El desarrollo de estos servicios transfronterizos en el entorno de la UE, tendrán una repercusión importante en la transmisión de datos de carácter personal entre los países comunitarios. Por tanto, es fundamental aplicar, en el espacio Europeo, una normativa de protección de datos equivalente.

La integración económica y social resultante del establecimiento y funcionamiento del mercado interior, definido en el artículo 7 A del Tratado, implica necesariamente un notable flujo transfronterizos de datos personales



entre los agentes públicos de los Estados miembros. El fortalecimiento de la cooperación entre países comunitarios facilitará la circulación transfronteriza de datos personales, mientras que las diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria

Existen redes de telecomunicaciones que responde a la demanda creciente de intercambio seguro de información trans-europeos. La red s-TESTA es la red privada de la Unión Europea que conecta las redes administrativas de los Estados miembros, de las Instituciones y Agencias europeas. En España, la conexión de la Red SARA con sTESTA canaliza la integración de las administraciones en los servicios públicos transfronterizos. En marzo de 2009 se firmó el convenio con la Comisión Europea y, al menos, 21 servicios

utilizados por 16 entidades, en 18 materias sectoriales utilizan Red SARA para el intercambio de datos.

La falta de interoperabilidad en la identificación y firma electrónica constituye un obstáculo para el desarrollo de servicios transfronterizos. El objetivo del proyecto STORK, del que España forma parte, es el reconocimiento paneuropeo de las identidades electrónicas, en Servicios de Administración Electrónica de las administraciones europeas. Lo que implica consultar los datos de revocación de los certificados digitales.

Uno de los textos legislativos, aprobados en los últimos años, más importantes para la Unión Europea es la Directiva 2006/123/CE de Servicios en el Mercado Interior y la libertad de establecimiento, que se traspone en la Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio. Se trata de convertir en realidad la libre circulación de servicios, una de las libertades fundamentales contenidas en los tratados fundacionales de la Unión. O lo que es lo mismo, facilitar a las empresas, el ejercicio de la actividad en otros Estados miembros distinto al de su creación, ya sea temporal o con establecimiento.

En España donde los trámites para ejercer una actividad están repartidos en las tres administraciones, la interoperabilidad y el intercambio de datos es fundamental para cumplir con la Directiva y ofrecer un único punto de vista al prestador asociado con su evento vital “poner un negocio”[4].

[4] La ventanilla única de servicio UEGO.es es un claro ejemplo de cómo la interoperabilidad y la coordinación organizativa es fundamental para este tipo de servicios.

Por último también en las administraciones hay pagos electrónicos a través de Internet y corresponde tanto a la entidad que pone el servicio de pago, como a la que ejerce de “pasarela de pago”, responsabilizarse de las medidas de protección de los datos: un “canal seguro” para salvaguardar la confidencialidad en el envío de datos personales, fundamentalmente cuando entre ellos figura la identificación de la tarjeta de pago y eliminar la información una vez cumplido el trámite.

Todos los servicios **comunes**, que ofrece el Ministerio de Hacienda y Administraciones Públicas, observan las condiciones de la LOPD en distintas fases:

- Las comunicaciones tienen garantías de seguridad e integridad
- Las plataformas no guarda ningún dato personal de las transmisiones entre los cedentes y cesionarios.
- Para transferir datos del ciudadano se exige que el cedente recabe el consentimiento o tenga una norma de rango suficiente que avale la solicitud de datos.
- Con una finalidad que sea pertinente

Un aspecto relevante incide sobre el uso del intercambio electrónico y nos da paso al siguiente principio: el derecho del ciudadano a conocer qué cesiones han sido realizadas de sus datos. Por ello, tanto el cedente como el cesionario están obligados a conservar las transacciones.

Principio de información

El ciudadano tiene derecho a conocer la información almacenada sobre sí mismo. El ciudadano tiene derecho de acceso, de rectificación, cancelación y oposición de los datos propios. Lo que se llama los derechos ARCO.

Como primera medida de información, la LAECSP y el reglamento que la desarrolla (RD 1671/2009) obligan a poner en la sede un enlace a la Agencia de Protección de Datos, a informar sobre la protección de datos y disponer de políticas de privacidad accesibles.

Como segunda medida e independientemente del proceso de recogida de tratamiento que se haga con los datos, y si es con o sin consentimiento, es absolutamente necesario contar con un proceso de información en la recogida de datos personales que satisfaga las exigencias del artículo 5 de la LOPD. Esto afecta también, como ya se ha mencionado, a los datos que se obtienen de transferencias entre las administraciones.

La acreditación de la información al afectado puede llevarse a cabo en papel o en electrónico y mediante la existencia de indicios que de forma inequívoca permitan fundar que el interesado hubo de ser informado.

La tramitación telemática (administración electrónica) ofrece una gran oportunidad para cumplir con el deber de informar al ciudadano de estos derechos de modificación y cancelación. Por ejemplo, puede utilizar una práctica habitual en el comercio electrónico respecto a la aceptación de las condiciones, que consiste en impedir, el envío de la solicitud si no se ha aceptado la cláusula informativa. Si los datos se recogen por el canal telefónico

la acreditación podrá obtenerse a través de una alocución grabada. El organismo debe proceder a la conservación del documento, cinta, formulario electrónico o log mientras dure el tratamiento de los datos.

La incorporación de nuevos principios como el de transparencia, 'privacy by design' o 'derecho al olvido', se han introducido en el esquema de la protección de datos debido a la tecnología.

El concepto "privacy by design" se refiere a la filosofía que incorpora la privacidad desde las especificaciones de diseño de los sistemas, tanto desde el punto de vista técnico como organizativo. No es casualidad que se hable de la organización pues la mayoría de los riesgos para la privacidad provienen de la forma en que se utiliza la tecnología, no de la tecnología.

Basado en este concepto, cualquier diseño de servicios electrónico debe pensar en la privacidad, incluso algo tan simple como un buzón de participación ciudadana que tengan como objetivo recabar la opinión de la ciudadanía respecto de actuaciones públicas. Si el buzón de sugerencias no es anónimo deberían recoger únicamente los datos personales necesarios (nombre y correo electrónico) sin poder utilizar estos datos para un fin diferente (ni siquiera estadístico). Pedir datos territoriales o preferencias no es una buena práctica. Finalizado el proceso de participación, los datos deben ser eliminados.

El derecho de información en la recogida de datos personales constituye un derecho fundamental a la protección de datos personales y es un elemento estratégico para proporcionar confianza y seguridad al ciudadano.

LA OBLIGACIÓN EN CUANTO AL ENS

¿Qué seguridad se aplica?

La Ley 11/2007 es muy precisa en lo que respecta a la seguridad de la información. Así, reconoce como un derecho de los ciudadanos «la garantía de la seguridad y la confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas» —artículo 6.2.I)

El Esquema Nacional de Seguridad (ENS) refuerza la protección de la información en la utilización de medios electrónicos obligando a tener una política a de seguridad y un responsable de seguridad.

El ejercicio de los derechos ARCO contemplados en la LOPD es un derecho de los ciudadanos y por tanto, el ejercicio de tales derechos debe ser objeto del ENS.

Pero, la seguridad de la información no es sólo un tema de la tecnología y no es suficiente para asegurar la protección de los datos, es necesario tener medidas organizativas. El ENS establece la necesidad de crear un Comité de Seguridad, nombrar un Responsable de Seguridad, elaborar una política de seguridad y aplicar las medidas necesarias para el cumplimiento del esquema.

Es conveniente que el Responsable de LOPD y el de ENS sean distintos, pudiendo formar ambos parte del Comité de Seguridad y cuyo titular será el Responsable formal de ambas funciones. El Responsable de LOPD, debe tener conocimiento jurídico, mientras que el Responsable de Seguridad ENS que es un perfil eminentemente Tecnológico.

En cuanto a la conservación, basta con remitirse a la LOPD y decir que deben conservarse durante el tiempo necesario para las finalidades del tratamiento para el que han sido recogidos y deben ser eliminados cuando hayan dejado de ser necesarios o pertinentes para el fin con que se obtuvieron.

CONCLUSIONES

La Administración electrónica tiene que tener en cuenta especialmente el cumplimiento del principio de seguridad y el de la protección de datos.

No es posible asumir una administración electrónica de confianza y de calidad si no se encuentra garantizada la protección de datos.

En la medida en que los datos personales van a ser sometidos a un tratamiento automatizado, es necesario aplicar medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

Cada principio de la LOPD tiene su reflejo en la LAECP y ser contemplado en la implementación de los servicios de administración electrónica.

La protección de datos debe contemplarse en la administración electrónica desde el momento del diseño.

La protección de datos debe estar incluida en el Plan de implantación del ENS.

La protección de datos no es solo un tema de tecnología implica una organización y la capacitación a los empleados públicos.

La responsabilidad de la protección de datos es del organismo competente (titular del fichero) y no se puede ceder aunque el tratamiento lo realice otro departamento o administración o un prestador de servicios.

BILIOGRAFÍA

- Agencia de Protección de Datos https://www.agpd.es/
- Protección datos y normativa europea. http://europa.eu
- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
- Directiva 2002/58/CE Directiva sobre la privacidad y las comunicaciones electrónicas
- Decisión 2004/915/CE de la Comisión, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ...
- Acceso electrónico de los ciudadanos a los servicios públicos, Miguel Angle Davara Rodriguez
- La Administración electrónica y la protección de datos personales, Antonio Troncoso Reigada
- Protección de Datos y e-Administración, Emilio Aced Félez
- Nueva normativa europea de protección de datos, ambiciosa y necesaria, Jesús Herranz, gerente del área Nuevas Tecnologías de BDO Abogados
- Seguridad en el diseño (Privacy by design) D. Informática y Telecomunicaciones EUSKADI.net
- Recomendación Esquema Nacional de Seguridad. Preguntas frecuentes