Protección de Datos y e-Administración

Emilio Aced Félez
Subdirector de Registro de Ficheros y Consultoría de la Agencia de Protección de Datos de la Comunidad de Madrid

1. Introducción

La interrelación de los ciudadanos con las AA.PP a través de medios electrónicos y telemáticos es hoy en día una realidad innegable. Esta moderna forma de interacción se va abriendo paso con fuerza en sectores específicos y es una cuestión de tiempo que los ciudadanos la empleen masivamente en todos los campos de su relación con los poderes públicos.

Por su parte, las Administraciones Públicas llevan muchos años desarrollando estrategias de Administración electrónica para prestar servicios públicos y facilitar la participación social que ha culminado con la promulgación de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP), que, mediante un salto cualitativo, reconoce a los ciudadanos el **derecho** a relacionarse con las Administraciones Públicas por medios electrónicos. Pero, además de cómo un reconocimiento de un derecho ciudadano, la e-Administración también debe de incardinarse y entenderse dentro las iniciativas que tratan de mejorar la calidad de los servicios públicos y la modernización del trámite administrativo.

Además, la LAECSP reconoce el papel fundamental de la protección de datos personales en el ámbito de la e-Administración e incluye como el primer principio general de la Ley, en su artículo 4, el respeto al derecho a la protección de datos de carácter personal, e incluso, anteriormente, en su Exposición de Motivos, afirma que *"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"* lo que pone de manifiesto la importancia capital que el legislador atribuye al respeto a la privacidad en el ámbito de la Administración electrónica.

Consciente de todo ello, la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM) ha aprobado la ***Recomendación 3/2008, de 30 de abril, sobre tratamiento de datos de carácter personal en servicios de administración electrónica***[1], cuya finalidad principal es hacer compatible el acceso electrónico de los ciudadanos a los servicios públicos con el respeto y defensa del derecho fundamental a la protección de datos.

La Recomendación no tiene carácter normativo, sino que es, más bien, un documento programático, que se enfrenta a los diferentes problemas existentes e intenta ofrecer respuestas a los mismos y servir de referencia a las AA.PP. bajo la supervisión de la Agencia.

2. Proporcionalidad, finalidad y calidad de datos

Un principio esencial de la protección de datos personales es la proporcionalidad de los datos recogidos con el fin que se persigue con su tratamiento. La LAECSP también otorga un papel preponderante a este principio y, en su artículo 4.g) dispone que solo se requerirán a los ciudadanos aquellos datos que sean estrictamente necesarios en atención a la finalidad para la que se soliciten (es decir, solo aquellos indispensables para la tramitación y resolución de los procedimientos correspondientes o para el ejercicio de derechos de los ciudadanos).

Un segundo aspecto que ha de tenerse en cuenta al tratar datos personales es que este tratamiento debe de limitarse a las finalidades para las que los mismos se recogieron y a aquellas compatibles con las primeras. Así, los datos aportados por el ciudadano al iniciar un procedimiento por medio de un servicio de administración electrónica o los que se obtengan por medio de elaboraciones de los mismos o por actos de trámite del correspondiente procedimiento, estarán vinculados a este, no pudiendo ser utilizados, con carácter general, por otros servicios o dependencias de la misma o distinta Administración, en otro expediente.

Para poder ser utilizados en un contexto diferente (otros procedimientos o servicios de e-Administración distintos) deberá existir una habilitación legal expresa o resultar necesario para dar cumplimiento a una libre y legítima relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión con ficheros de terceros. O, por supuesto, si se cuenta con el consentimiento del afectado.

La LAECSP reconoce también el derecho de no aportar los datos y documentos que obren en poder de las Administraciones Públicas y dispone que las AA.PP. utilizarán medios electrónicos para recabar dicha información. Este precepto, que ya figuraba en la Ley de Régimen Jurídico y Procedimiento Administrativo Común (LRJPAC) del año 1992 nunca tuvo una gran implantación debido a las dificultades y complicaciones para ponerlo en práctica en el mundo no virtual. Es, pues, ahora, cuando se dan las circunstancias jurídicas y tecnológicas necesarias para que pueda llegar a convertirse en una realidad tangible. Ello ha de hacerse con respeto a la protección de datos personales, ya que la Ley impone obtener el consentimiento previo de la personas para poder acceder a sus datos ya obrantes en manos de las AA.PP. Además, esta obtención de datos y documentos habrá de estar estrictamente limitada a los que se requieren para la tramitación del procedimiento.

Los servicios de administración electrónica que se limiten a facilitar información sobre servicios disponibles para su uso por los ciudadanos, con carácter general, no deberán recoger ningún tipo de dato de carácter personal. En el supuesto de que se usen *cookies* con la finalidad de facilitar la navegación al usuario, la utilización de los datos contenidos en las mismas que pudieran permitir la identificación del usuario estará limitado para esa específica finalidad.

Las sedes electrónicas y los registros telemáticos constituyen elementos vertebradores de la presentación de los servicios de e-Administración a los ciudadanos. El tratamiento de datos personales que lleven a cabo deberá limitarse –con excepción de servicios de carácter horizontal prestados por la propia sede como la autenticación de los usuarios, la validación de certificados electrónicos, las suscripciones a novedades o la notificación electrónica segura- a la puesta a disposición del órgano competente para la tramitación del procedimiento de los

datos y documentos presentados en ella. Por ello, el personal que atienda la sede electrónica o registro electrónico no accederá, en ningún caso, al contenido de los datos o documentos aportados por el ciudadano con destino a otros órganos, salvo a aquellos que identifiquen al solicitante, la solicitud realizada y el órgano competente para su resolución.

En relación con la actualización de la información, se consideran exactos los datos facilitados directamente por el usuario. En cualquier caso, existe la obligación de rectificar los datos erróneos o inexactos y cancelar los datos excesivos o inadecuados en un plazo de diez días desde que se conociera este hecho, salvo que la legislación reguladora establezca un procedimiento o plazo específico. Las correcciones o cancelaciones se notificarán a los órganos y organismos a los que se hubiera comunicado la información errónea.

La e-Administración proporciona, mediante el rediseño de procesos, una gran oportunidad para implantar y automatizar las medidas necesarias para proceder al bloqueo y cancelación de la información cuando haya dejado de ser necesaria para la finalidad para la que se obtuvo y, en su caso, se cumplan los plazos establecidos por la normativa reguladora de cada procedimiento.

3. Derecho de información y consentimiento del interesado

Este derecho cumple un papel fundamental en la transparencia de los tratamientos de datos personales pues, a través de él, los afectados pueden tener conocimiento de quién recoge y para qué sus datos personales.

Un aspecto específico de los procesos de e-Administración es el que se da en aquellos servicios que únicamente ofrecen información general al ciudadano, sin recabar directamente datos de carácter personal, pero que usan cualquier tipo de sistemas de seguimiento para facilitar la navegación (normalmente, *cookies*). Si ello es así, el servicio deberá informar, con carácter previo a la generación de la *cookie* de la utilización de las mismas, su finalidad y el resto de elementos descritos en el artículo 5.1 LOPD.

Cuando se recaben datos en sedes o registros electrónicos se informará, especialmente, de las comunicaciones a realizar a los órganos encargados de iniciar, gestionar y resolver las peticiones formuladas por los usuarios y, del mismo modo, si los datos van a ser incorporados a repositorios de datos o documentales, con el fin de facilitar el derecho a no aportar datos que ya obren en poder de la Administración.

En cualquier caso, si en el desarrollo de un procedimiento administrativo iniciado por un servicio de administración electrónica se realiza cualquier acto de notificación o comunicación al interesado, se informará al mismo de los datos objeto de tratamiento que no se hayan obtenido directamente del mismo.

En el caso de que el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquellos.

La prestación de servicios de administración electrónica que se correspondan con el ejercicio de potestades de los órganos administrativos no requerirá el consentimiento del interesado. Del mismo modo, aquellos servicios que permitan el

ejercicio de derechos subjetivos reconocidos al ciudadano se entenderá que podrán proceder al tratamiento de datos del afectado, al ser siempre estos servicios objeto de inicio a instancia del interesado e incluir su consentimiento tácito.

En cambio, la utilización de sistemas de seguimiento para facilitar la navegación o aquellos relativos a la remisión de información personalizada o de suscripciones a boletines o novedades, requerirán del consentimiento previo de los ciudadanos.

Cuando se requiera el consentimiento del interesado, se deberá de contar con un sistema de identificación inequívoca del mismo, asegurando la identidad, autenticidad e integridad de la información y se deberán prever los mecanismos necesarios para garantizar la revocación del mismo.

Para solicitar el consentimiento, se podrán utilizar sistemas de firma electrónica avanzada u otros medios contemplados en la LAECSP, como la introducción de claves o la aportación de información conocida solo por ambas partes. Se podrá recabar dando la posibilidad de marcar una casilla específica por el interesado, que previamente no esté marcada, en el formulario en el que se acceda al servicio de administración electrónica.

4. Derechos de acceso, rectificación, cancelación y oposición

En el ámbito de e-Administración, los servicios deberían de incluir la posibilidad del acceso electrónico y en tiempo real a los datos del afectado que obran en las bases de datos y en los expedientes que se tramitan electrónicamente, sin más requisito que la identificación y autenticación indubitada de los afectados mediante sistemas de firma electrónica avanzada o el resto de los previstos en la LAECSP.

El ejercicio de los derechos de rectificación, cancelación y oposición no tiene grandes especialidades en el entorno de la e-Administración salvo el de facilitar las solicitudes y la aportación de la documentación necesaria a través de medios electrónicos tras, como en el caso del derecho de acceso, acreditar inequívocamente la identidad del afectado.

En relación con el derecho a impugnar valoraciones sobre las personas realizadas exclusivamente por medios automáticos, la LOPD establece que los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecta de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

El afectado podrá impugnar los actos administrativos que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión y, además, deberán informar al afectado con carácter previo.

Igualmente, se deberá informar del resultado obtenido en la valoración llevada a cabo así como de los criterios y programas utilizados para su realización. No obstante, los afectados podrán verse sometidos a la decisión adoptada en el

proceso de valoración cuando este esté autorizado por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

5. Especialidades en casos concretos de servicios de e-Administración

En primer lugar hay que referirse a los llamados **Centros de Acceso Público a Internet (CAPI)** que las Administraciones Públicas ponen a disposición de los ciudadanos para facilitar su acceso a los servicios de Internet y, en particular, para facilitarles el acceso por medios electrónicos a la información y al procedimiento administrativo, con especial atención a la eliminación de las barreras que limiten dicho acceso.

Los usuarios de los CAPI deben respetar las normas y condiciones de utilización que las Administraciones establezcan para su uso ya que se trata de servicios públicos y gratuitos. No obstante, la aplicación de estar normas no puede suponer un menoscabo del derecho a la intimidad y confidencialidad de los usuarios tal como regula la normativa vigente en materia de protección de datos.

La política que se utilice en los CAPI para garantizar el cumplimiento de las normas de utilización, especialmente en cuanto a no acceder a sitios con contenido pornográfico, de incitación a la violencia, racismo o terrorismo, deberá al mismo tiempo garantizar la confidencialidad de cualquier acceso realizado, así como de los datos que los usuarios transmitan en sus conexiones a Internet.

Así, en ningún caso podrá procederse al análisis de los rastros de navegación, ni conocer la dirección IP o URL accedida, a efectos de detectar posibles infracciones de las normas de acceso y proceder a su sanción o retirada de los derechos de usuario. Tampoco deberá quedar registrado el contenido de los formularios accesibles en páginas de Internet, o correos o mensajes enviados por los usuarios. No se podrán utilizar sistemas de monitorización invasivos de la intimidad de los usuarios.

Cada vez que un usuario concluya una sesión de conexión a Internet deberán eliminarse todos los rastros de información generados durante la navegación así como las *cookies* o sistemas de seguimiento que hayan podido almacenarse en el equipo. Y, por supuesto, se implantarán todas las medidas de seguridad establecidas en el Reglamento de Desarrollo de la LOPD (RLOPD) aprobado por el Real Decreto 1720/2007.

Otro aspecto importante regulado por la Recomendación es la obligación de que en la página de inicio de todas los sitios web institucionales de las Administraciones Públicas y órganos administrativos sometidos a la misma aparezca un enlace relativo a su **Política de privacidad**, que contendrá la información completa sobre todos los aspectos relativos a la protección de datos personales de la Web, declarando, si ese fuera el caso, que no se recogen datos de carácter personal.

La Política de privacidad deberá contener un mensaje explícito, específico y fácilmente comprensible, de manera que se transmita al usuario de Internet una idea clara del contenido al que va a acceder, y, en su caso, se advierta de la posible recogida de datos de carácter personal.

Asimismo, deberá contener, al menos, información sobre el titular del sitio web institucional, la finalidad del mismo, las medidas técnicas de seguridad adoptadas,

del posible uso de *cookies,* otros tratamientos invisibles y del posible uso de la dirección IP del usuario así como cualquier otra que la legislación sobre protección de datos de carácter personal establezca como obligatoria.

Por otra parte, cada vez es más frecuente que los sitios web institucionales ofrezcan servicios de **suscripción a servicios a noticias y novedades así como a alertas SMS**. Con carácter general, en el caso de suscripciones a noticias, *newsletters* y novedades, se deberá solicitar del ciudadano única y exclusivamente su dirección de correo electrónico, el código de usuario y contraseña elegidos, el tipo de información que quiere recibir y, en algún caso, la edad (servicios para mayores o para menores).

Deberá especificarse claramente qué campos son obligatorios para poder acceder al servicio. En todo caso, los campos obligatorios deben limitarse a los estrictamente necesarios para la gestión del servicio y sin que pueda haber ninguna discriminación por no rellenar los campos voluntarios.

Por lo que respecta a la suscripción mediante Internet a los servicios de alertas de mensajes SMS, el único dato que deberá recabarse es el número de teléfono móvil al que se vaya a enviar la alerta correspondiente.

Otro de los servicios que prestan actualmente las Administraciones Públicas a través de Internet es la posibilidad de que los ciudadanos se suscriban a **bolsas de empleo**, recabando para ello datos de carácter personal.

En este caso, será conforme con el principio de calidad de datos la recogida de los correspondientes a nombre, apellidos, número de teléfono, sexo, estado civil, fecha y país de nacimiento, nacionalidad, permiso de trabajo y permiso de conducir. Si se desea recoger datos adicionales, deberá de hacerse tras una cuidadosa evaluación de su necesidad para la finalidad para la que se recogen tal y como establece el artículo 4 de la LOPD.

En este apartado un aspecto muy importante es la información que se debe proporcionar a los ciudadanos, haciendo especial hincapié en las cesiones previstas en relación con los datos de carácter personal recabados e indicando expresamente si los mismos serán comunicados a empresas para facilitar la contratación del afectado integrante de la bolsa de empleo.

Cada vez es más frecuente también la utilización de ***chats* institucionales** para el contacto directo y en tiempo real con los ciudadanos. En general, para participar en estos *chats* no será necesario solicitar y recabar del ciudadano datos identificativos como el nombre y apellidos, facilitándose que los mismos participen mediante la elección de un alias o pseudónimo que garantice su anonimato.

En el caso de que se solicitasen datos de carácter personal como el número de teléfono, móvil o fijo, o la dirección de correo electrónico, se deberá informar a los ciudadanos en los términos establecidos por la LOPD.

Las TIC también facilitan la puesta en marcha de **procesos de participación ciudadana** que tengan como objetivo recabar la opinión o sugerencias de la ciudadanía respecto de actuaciones realizadas, en curso o pendientes de realizar por parte de las AA.PP., a través de sitios Web institucionales publicando en ellos la documentación relativa a un determinado proyecto. Esta publicación deberá

hacerse de forma disociada, sin contener datos de carácter personal, especialmente en la documentación relativa a planes urbanísticos o proyectos de carreteras.

Si se recaban datos de carácter personal de los participantes en el proceso de participación (como, por ejemplo, la dirección de correo electrónico), estos no podrán utilizarse para ningún otro fin distinto. Una vez finalizado el proceso de participación, los datos serán cancelados.

Igualmente, cuando se establezcan **foros de opinión** se deberán solicitar los datos personales estrictamente necesarios para permitir al ciudadano expresar su opinión en los mismos.

En todo caso, será suficiente la solicitud y obtención de un nombre de usuario y de una dirección de correo electrónico del ciudadano afectado por el tratamiento. Será necesario articular un procedimiento para obtener el consentimiento de la persona que ostente la tutela o patria potestad cuando los que deseen entrar en el foro sean menores de catorce años.

En relación con las opiniones de los ciudadanos suscritos a los foros que se encuentren en sitios Web institucionales, de conformidad con la Constitución española, que reconoce y protege el derecho a expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra o el escrito o cualquier otro medio de reproducción, se podrán publicar opiniones sobre cualquier cargo público, siempre y cuando las opiniones se refieran a la gestión político-administrativa del mismo, pudiendo publicarse por tal condición de cargo público los datos personales de los mismos (nombre, apellidos y cargo).

No obstante, es contraria a la normativa sobre protección de datos la publicación de datos personales de estos cargos públicos referentes a su esfera particular como, por ejemplo, su dirección de correo electrónico particular o la dirección de su vivienda. En este último supuesto podría derivarse responsabilidad por vulneración de lo dispuesto en la normativa sobre protección de datos personales, tanto en relación con la persona que desvele dichos datos personales como respecto del titular del sitio Web institucional por proceder a la publicación de los mismos.

Asimismo, si algún usuario vertiese alguna opinión en la que se mencionen datos de carácter personal de los ciudadanos, la Administración Pública u órgano administrativo competente no deberá publicar dichos datos, ya que, en caso contrario, se vulneraría también el derecho a la protección de datos personales de los ciudadanos afectados.

6. Publicación de datos personales en Internet

Un tratamiento de especial relevancia y con una gran injerencia en la privacidad de las personas es la publicación de los datos de carácter personal en Internet, en general, y en los boletines y diarios oficiales en particular. La razón fundamental para que se produzca esta invasión de la privacidad, con el acceso prácticamente indiscriminado a todos los datos publicados sobre una persona, es la existencia de los motores de búsqueda que indexan los contenidos de boletines y páginas Web haciendo accesible la información sobre cualquier persona simplemente introduciendo su nombre en uno de estos buscadores.

La Agencia de Protección de Datos de la Comunidad de Madrid, por su propio análisis de la situación y por las reclamaciones que muchos ciudadanos le han hecho llegar, es consciente de los problemas que este hecho puede causar ya que datos a veces muy sensibles (sanciones, multas, resultados de exámenes, subvenciones, minusvalías, etc.) quedan muy a menudo expuestos a la luz pública sin que exista ya una necesidad para ello.

En este sentido, la APDCM ha publicado la ***Recomendación 2/2008, de 25 de abril, sobre publicación de datos personales en boletines y diarios oficiales en Internet, en sitios webs institucionales y en otros medios electrónicos y telemáticos***[2], en la que aborda de un modo sistemático la aplicación de los principios de protección de datos a este tipo de tratamientos y el estudio pormenorizado de las diferentes categorías de información que las AA.PP. publican en Internet y los distintos tipos de procedimientos que justifican dicha publicación.

En este trabajo no resulta posible hacer un estudio pormenorizado del contenido de dicha Recomendación pero sí se mencionarán los puntos esenciales que habrán de tenerse en cuenta cuando se pretenda publicar datos personales en Internet.

El primer aspecto que debe considerarse es que no será necesario el consentimiento del interesado para la publicación de datos personales cuando la misma se fundamente en alguno de los supuestos regulados en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común; en la existencia de una norma con rango de ley o en una norma comunitaria de aplicación directa que ofrezcan cobertura legal a la cesión de datos derivada de dicha publicación o cuando responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la utilización de dichos medios de publicación. En el resto de situaciones, será necesario contar con el consentimiento de los ciudadanos.

En cualquier caso, la publicación de los datos personales será conforme con la normativa sobre protección de datos cuando la difusión de aquellos a través del medio elegido resulte necesaria en consideración a los hechos y a las circunstancias concurrentes, en aras del interés general, resultando la elección de este tipo de publicación de datos personales la medida más adecuada, pertinente y proporcional de las que puedan adoptarse en orden a la satisfacción del interés público.

Igualmente, deberá elegirse el sistema o medio de publicidad que suponga un menor nivel de injerencia en el derecho a la intimidad y a la protección de los datos de carácter personal del afectado teniendo en cuenta, a estos efectos, que la publicación en boletines y diarios oficiales, por su regulación específica y por su condición de garantes del principio de legalidad, supone una injerencia mayor que la publicación en un sitio Web puesto que la cancelación o bloqueo es mucho más compleja jurídicamente.

Así pues, como se apuntaba en el párrafo anterior, en relación con los niveles de publicidad, siempre que sea posible, se preferirá la publicación de los datos personales en un área restringida de un sitio Web que requiera la identificación y autenticación de los usuarios con derecho a acceder a la información.

La publicación de datos de carácter personal en boletines o diarios oficiales a través de Internet supone un mayor nivel de injerencia sobre el derecho fundamental a la protección de datos de carácter personal que la publicación de los mismos a través de sitios Web institucionales, o de cualquier otro medio electrónico o telemático administrativo, al constituir dichos Boletines o Diarios oficiales "fuentes accesibles al público". Por ello, se recomienda que dicha publicación, y, en consecuencia, el acceso no identificado de cualquier ciudadano a los datos así publicados, se produzca únicamente en aquellos supuestos contemplados por una norma con rango de ley o por una norma comunitaria de aplicación directa.

La publicación no restringida de datos de carácter personal, con acceso no identificado y universal en sitios Web institucionales, en cualquier otro medio electrónico o telemático administrativo, o a través de tablones de anuncios o edictos electrónicos de acceso no limitado, supone un menor nivel de injerencia sobre el derecho fundamental a la protección de datos de carácter personal que la publicación de dichos datos personales en boletines y diarios oficiales.

En consecuencia, se recomienda que, siempre que una norma con rango de ley o una norma comunitaria de aplicación directa no establezcan lo contrario, la Administración pública u Órgano administrativo competente que deba proceder a la publicación no restringida de datos de carácter personal que posibilite el acceso no identificado y universal a los mismos, lo realice a través de un sitio Web institucional o mediante cualquier otro medio electrónico o telemático, sin acudir a la publicación de los datos a través de boletines o diarios oficiales.

En todo caso, se recomienda que en la Orden, u otra Disposición de carácter general, en la que establezca la publicidad de los datos personales derivados del procedimiento administrativo correspondiente, se indique -de manera concreta y específica- el medio de publicación elegido por el Órgano competente para la consecución de los correspondientes efectos jurídicos perseguidos con dicha publicación.

Por otra parte, un aspecto esencial para garantizar los derechos de los ciudadanos es la obligación de que los datos de carácter personal publicados en Internet se cancelen cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido publicados, teniendo en cuenta los plazos máximos establecidos por la normativa sectorial específicamente aplicable. Todo ello sin perjuicio del posible ejercicio, en cualquier momento, por parte de los afectados de su derecho de cancelación sobre los datos publicados en Internet.

Un caso particular que requiere especial consideración es la cancelación de datos personales publicados en boletines o diarios oficiales a través de Internet. De acuerdo con lo dispuesto en el apartado 1 del artículo 11 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, la publicación de los diarios o boletines oficiales en las sedes electrónicas de la Administración, Órgano o Entidad competente tiene, en las condiciones y garantías que cada Administración Pública determine, los mismos efectos que los atribuidos a su edición impresa.

A su vez, de acuerdo con el apartado 2 de dicho artículo 11, la publicación del boletín oficial en la sede electrónica del organismo competente tendrá carácter oficial y auténtico en las condiciones y con las garantías que se determinen

reglamentariamente, derivándose de dicha publicación los efectos previstos en el título preliminar del Código Civil y en las restantes normas aplicables.

No obstante, la APDCM recomienda que la conservación de los datos de carácter personal publicados en boletines o diarios oficiales a través de Internet se realice sin perjuicio de la obligación de bloqueo de dichos datos personales cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido publicados y, muy especialmente, impidiendo, en la medida de lo posible, la accesibilidad a los datos personales que han de ser bloqueados por parte de los motores de búsqueda.

La recomendación de bloqueo permite limitar la publicidad de los datos personales, al mismo tiempo que se garantiza la autenticidad, integridad e inalterabilidad de los contenidos del diario oficial que se publique en sede electrónica.

La decisión sobre el bloqueo de los datos de carácter personal en un boletín o diario oficial corresponderá siempre al órgano u organismo responsable que ordenó la publicación de los mismos, estando el boletín o diario oficial obligado al bloqueo de la información solicitado por el responsable.

En consecuencia, se recomienda que la conservación de los datos personales publicados en boletines o diarios oficiales a través de Internet se realice mediante el bloqueo de los mismos, manteniéndolos a disposición de los interesados y de las Administraciones Públicas y los Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento.

Alternativamente, en el momento de ordenar la inserción de la información con datos de carácter personal en el boletín o diario oficial, la Administración Pública u Órgano administrativo competente podrá establecer las instrucciones precisas que deba seguir el gestor del boletín o diario oficial para el bloqueo de los datos de carácter personal.

Por lo que respecta al acceso de los motores de búsqueda, externos e internos, a los datos personales contenidos en boletines o diarios oficiales o en sitios Web institucionales, cuando la publicación suponga un tratamiento de datos de carácter personal y se haya cumplido con la finalidad perseguida por la misma, se recomienda que la Administración pública u Órgano administrativo competente adopte las medidas técnicas necesarias para impedir la indexación automática de los datos personales contenidos en boletines o diarios oficiales en Internet, o en los sitios Web y otros canales electrónicos o telemáticos institucionales.

A dichos efectos, se sugiere la utilización de etiquetas "NO ROBOT" que minimicen, hasta donde sea posible, la diseminación de la información de carácter personal a la que se pueda acceder a través de los motores de búsqueda.

Asimismo, habida cuenta del estado de la tecnología en cada momento, se recomienda que, para impedir la indexación automática de los datos personales en los motores de búsqueda, se impulse la incorporación e implementación de cualquier otro tipo de medidas técnicas que resulten adecuadas, dirigidas a evitar dicha indexación de contenidos con datos de carácter personal.

Para concluir este apartado hay que reseñar que la Comunidad de Madrid se ha mostrado sensible a esta problemática y en el Decreto 2/2010, de 28 de enero, del

Consejo de Gobierno, por el que se regula la edición electrónica del Boletín Oficial de la Comunidad de Madrid, ha introducido una serie de garantías para el correcto tratamiento de los datos personales publicados en el BOCM.

Así, en su artículo 9, sujeta a lo establecido en la legislación de protección de datos los servicios prestados mediante la base de datos gratuita que configura el BOCM al disponer que *"… El Organismo Autónomo Boletín Oficial de la Comunidad de Madrid ofrecerá en su sede electrónica una base de datos gratuita que permita la búsqueda, recuperación e impresión de las disposiciones y actos publicados en la edición digital del BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID, con sujeción a lo establecido en la legislación de protección de datos de carácter personal".*

Igualmente, y de forma más específica, en su Disposición Adicional Segunda sobre Protección de datos de carácter personal, determina que *"En el ámbito de sus respectivas competencias, corresponde a los responsables del tratamiento de datos de carácter personal que promuevan la inserción de anuncios en la edición electrónica del BOLETÍN OFICIAL DE LA COMUNIDAD DEMADRID determinar la finalidad, contenido y uso de los datos de carácter personal publicados, así como la posibilidad de bloqueo de los mismos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubiera sido efectuada dicha publicación"*, con lo que no solo establece de manera obligatoria y vinculante la posibilidad del ejercicio del derecho de cancelación mediante el bloqueo de los datos sino que insta a los responsables que ordenan la publicación de datos personales a establecer el periodo de tiempo durante el cual los datos deben de permanecer a disposición de los usuarios del BOCM y el momento a partir del cual los mismos deben bloquearse.

7. Conclusión

La Recomendación 3/2008 de la Agencia de Protección de Datos de la Comunidad de Madrid intenta ser un instrumento que guíe a las AA.PP. sometidas a su supervisión en la adopción de medidas que, salvaguardando la eficacia y eficiencia de los servicios electrónicos públicos y el deseable despegue de estas indispensables herramientas de comunicación y cercanía con los ciudadanos, permitan, al mismo tiempo, garantizar una utilización de los mismos respetuosa con los derechos de los ciudadano y, en particular, con su privacidad.

En la misma se dan orientaciones generales sobre los principios esenciales de la protección de datos y los derechos de los ciudadanos para finalizar analizando algunos de los servicios más comunes que las AA.PP. prestan a través de medios electrónicos para poner de manifiesto sus especialidades y proponer medidas adaptadas a la singularidad de cada uno.

Por otra parte, en la Recomendación 2/2008 se aborda la protección de datos personales en Internet y se establecen los criterios que permiten establecer el necesario equilibrio entre la ineludible obligación de transparencia y publicidad de las AA.PP. con la salvaguardia de la privacidad de las personas que sufren la publicación de sus datos.

La APDCM espera que estas Recomendaciones sean una contribución útil para la mejora de la protección de la privacidad de los ciudadanos y sirvan como un instrumento de concienciación de las AA.PP. para prestar un servicio público de calidad a lo que sin duda contribuirá el respeto a los derechos de los ciudadanos usuarios de los servicios electrónicos de las Administraciones Públicas.