21/2008

Dictamen jurídico en relación con la consulta formulada por un ayuntamiento referente a la instalación de cajeros electrónicos para realizar algunos trámites administrativos, entre ellos la obtención de volantes de empadronamiento

Se presenta ante la Agencia Catalana de Protección de Datos una consulta sobre si la instalación de cajeros electrónicos para realizar algunos trámites administrativos, entre otros la obtención de volantes de empadronamiento puede suponer una vulneración de la legislación sobre protección de datos.

En concreto, se formulan dos cuestiones: en primer lugar, si puede considerarse que el uso de estos cajeros para la obtención de volantes de empadronamiento de residencia y de convivencia puede vulnerar la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD); en segundo lugar, se consulta qué medidas se consideran imprescindibles para garantizar el cumplimiento de la citada normativa.

Analizada la petición y vistos la normativa vigente aplicable y el informe de la Asesoría Jurídica, se emite el siguiente dictamen:

I

Pese a que la consulta formulada puede referirse a otros servicios municipales, se centra concretamente en la posibilidad de acceso al padrón municipal de habitantes. Por ello, en primer lugar realizaremos algunas consideraciones relativas a la información que contiene.

Conviene recordar, en primer lugar, que en el padrón municipal de habitantes deben inscribirse las personas residentes en un municipio, con una triple finalidad, según la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local (en adelante, LRBRL): determinar la población del municipio, ser requisito para la adquisición de la condición de vecino y servir para acreditar la residencia y el domicilio habitual (artículos 15 y 16 de la LRBRL). Además de estas funciones, la Ley Orgánica del Régimen Electoral General (LOREG) contempla la elaboración del censo electoral a partir de los datos incluidos en el padrón, que también sirve para elaborar estadísticas oficiales. Debe añadirse a todo lo anterior, complementariamente, que el padrón también puede servir para la creación de ficheros o registros de población que tienen por finalidad la comunicación de los distintos órganos de cada administración pública con las personas interesadas residentes en los respectivos territorios, en lo referente a las relaciones jurídico-administrativas derivadas de sus respectivas competencias (disposición adicional segunda de la LOPD).

El padrón contiene datos personales consistentes en el nombre y apellidos, domicilio habitual, fecha y lugar de nacimiento, número del documento de identidad (o, para extranjeros, tarjeta de residencia o número del documento acreditativo de su identidad), certificado o título escolar o académico, además de aquellos datos que puedan ser necesarios para la elaboración del censo electoral (artículo 16.2 de la LRBRL). La gestión del padrón corresponde a los ayuntamientos con medios informáticos, que deben realizar las actuaciones y operaciones necesarias para mantener actualizados los datos que contenga el padrón a fin de que se correspondan con la realidad (artículo 17 de la LRBRL).

Puesto que el padrón supone el tratamiento de datos de carácter personal, le es de aplicación el régimen jurídico de protección de datos de carácter personal (LOPD) y, por lo tanto, hay que tener en cuenta los principios y disposiciones que contienen dicha normativa.

El artículo 3 de la LOPD, en su apartado *d*, considera tratamiento de datos el conjunto de operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan recoger, grabar, conservar, elaborar, modificar, bloquear y cancelar datos, así como las cesiones de datos derivadas de los mismos. En consecuencia, cualquier tratamiento que

realice el Ayuntamiento en cuanto responsable del padrón, como por ejemplo la comunicación a través del sistema descrito en la consulta, quedará sometido a los principios y disposiciones que contienen la normativa de protección de datos de carácter personal, independientemente de la naturaleza y características del fichero de datos donde puedan contenerse.

En cuanto al régimen de acceso a los datos del padrón, y sin perjuicio de los casos de cesión al Instituto Nacional de Estadística (INE) u otras administraciones (artículos 16 y 17 de la LRBRL), el artículo 40.2 del Texto Refundido de la Ley Municipal y de Régimen Local de Cataluña (TRLMRLC), aprobado por el Decreto Legislativo 2/2003, de 28 de abril, establece que los datos que constan en el padrón son confidenciales y el acceso a los mismos se rige por las normas que regulan el acceso administrativo de los ciudadanos a archivos y registros públicos y por la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos.

Así pues, hay que tener presente el artículo 37.3 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJPAC), que establece que el acceso a los documentos que contengan datos de carácter nominativo, como sería el caso del padrón, puede ser ejercido por los titulares de los datos y también por aquellas otras personas que acrediten un interés legítimo y directo.

Debe ser considerado, asimismo, el artículo 135.2 del Reglamento de Demarcación Territorial y Población de los Entes Locales (RDTPEL), aprobado por el Decreto 140/1988, de 24 de mayo, que limita la posibilidad de acceso a los datos del padrón a las personas interesadas. Mención que debe entenderse referida, en concordancia con el citado precepto de la LRJPAC, tanto a la persona titular de los datos como también a aquellas otras personas que convivan con la misma y pretendan acreditar la convivencia.

Por otra parte, el artículo 61 del Reglamento de Población y Demarcación Territorial de las Entidades Locales (RPDTEL), aprobado por el Real Decreto 1690/1986, de 11 de julio, establece que pueden expedirse certificaciones del padrón (artículo 53.1) que deberán ser expedidas por el secretario del Ayuntamiento (artículo 61.1), así como volantes de empadronamiento, con carácter puramente informativo, en los que no serán necesarias las formalidades previstas para las certificaciones (artículo 61.2).

Por lo tanto, desde esta perspectiva no existiría ningún problema para habilitar un sistema que, con las debidas garantías y previa comprobación de la existencia del citado interés legítimo, permitiese el acceso a los datos del padrón para la obtención de un volante.

Ahora bien, la respuesta a la primera de las preguntas formuladas en la consulta no puede desvincularse de la segunda, de modo que la legitimidad de la utilización de los cajeros para la obtención de volantes de empadronamiento será adecuada o no en función de cuáles sean las medidas de seguridad aplicadas.

II

Más allá de la posibilidad apuntada en términos generales en el apartado anterior, en la consulta se plantea la adecuación a la normativa de protección de datos de un sistema concreto de obtención de volantes de empadronamiento basado en medios electrónicos. En concreto, por lo que se desprende de la consulta, se trataría de cajeros o terminales electrónicos desde donde, previa lectura mediante escáner del DNI o fotocopia del mismo, se facilitaría el volante.

En referencia a esta forma de acceso, hay que mencionar la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP), que reconoce el derecho de los ciudadanos y ciudadanas a relacionarse con las administraciones públicas por medios electrónicos (artículo 1) y que tiene como una de sus finalidades facilitar el acceso de los ciudadanos por medios electrónicos a la información y al procedimiento administrativo (artículo 3.2).

Desde este punto de vista, la iniciativa propuesta se enmarca plenamente dentro de esos objetivos, ya que, en definitiva, de lo que se trata es de posibilitar la obtención de volantes de empadronamiento por medios electrónicos directamente por parte de las personas interesadas.

Ahora bien, la consecución de los objetivos previstos en la LAECSP se supedita por la propia ley al cumplimiento de una serie de principios, entre los que nos interesa destacar, a efectos de la presente consulta, el respeto al derecho a la protección de datos de carácter personal (artículo 4.*a*) y el principio de seguridad (artículo 4.*f*), en virtud del cual la implantación y utilización de medios electrónicos por las administraciones públicas deberá realizarse al menos con igual nivel de garantías y seguridad que se requiere para la utilización de medios no electrónicos en la actividad administrativa.

Un principio de seguridad que adquiere especial relevancia en el tratamiento de datos de carácter personal, a tenor de lo dispuesto en el artículo 9 de la LOPD, según el cual «el responsable del fichero y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural».

Según estos principios, la propia LAECSP, en sus artículos 14 a 16, regula los requisitos de identificación y autenticación de los ciudadanos en sus relaciones con la Administración por medios electrónicos, permitiendo la utilización tanto del documento nacional de identidad electrónico (artículo 14) como de los sistemas de firma electrónica avanzada que cada administración pública haya admitido e incluido en una relación pública y accesible por medios electrónicos (arte. 15), o también, cuando esté justificado teniendo en cuenta los datos e intereses afectados, otros sistemas de identificación como pueden ser los basados en claves de acceso o alguna información conocida por ambas partes y que ofrezca suficientes garantías de confidencialidad (artículo 16).

Por otra parte, la normativa de protección de datos, y en concreto la regulación de las medidas de seguridad establecidas por el Reglamento de despliegue de la LOPD (RLOPD), aprobado por el Real Decreto 1720/2007, dentro de las medidas de nivel básico, y por lo tanto aplicables a cualquier fichero o tratamiento, establece en su artículo 93 los requisitos para la identificación y autenticación de usuarios (entendiendo como autenticación el procedimiento de comprobación de la identidad de la persona usuaria —artículo 5.2.*b*— y como usuarios a los sujetos autorizados para acceder a datos o recursos —artículo 5.2.*p*—):

> *«Artículo 93. Identificación y autenticación.*
>
> *»1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.*
>
> *»2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.*
>
> *»3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas, existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.*
>
> *»4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las*

contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.»

Por lo tanto, según los citados preceptos, es necesario que el sistema que se instale en estos cajeros permita identificar quién está solicitando el volante de empadronamiento y permita comprobar que realmente la persona usuaria es quien dice ser, a efectos de saber si se trata de una de las personas legitimadas para solicitar el volante de empadronamiento. Además, deberá hacerlo con las suficientes garantías.

A nivel teórico, se consideran tres posibles factores de autenticación:

— Aquello que la persona usuaria conoce (contraseña, PIN u otra información).
— Aquello que la persona usuaria tiene (certificado digital, *token*, USB, etc.).
— Aquello que la persona usuaria es (datos biométricos).

La identificación y autenticación no plantearía mayores problemas, desde el punto de vista de la protección de datos, si se llevara a cabo mediante DNI electrónico (artículo 15.2 de la Ley 59/2003) u otros sistemas de firma electrónica avanzada (artículo 3.2 de la Ley 59/2003), ya que estos sistemas, que constituyen sistemas de identificación de doble factor (requieren dos de los citados factores de autenticación: aquello que tiene y aquello que conoce), ofrecen suficientes garantías.

Obviamente, la única precaución que sería necesario adoptar es que únicamente fuese aceptada como válida la identificación por parte de alguna de las personas que conviven en un mismo domicilio. Por otra parte, si se utilizan otros sistemas de firma electrónica avanzada, según lo que establece la Ley 59/2003, de firma electrónica, hay que tener en cuenta que, de conformidad con el artículo 15.2 de la LAECSP, el Ayuntamiento debería incluir los sistemas admitidos en una relación pública y accesible por medios electrónicos.

La utilización de un sistema basado en contraseñas ofrece menos garantías que los anteriores, pero podría resultar igualmente admisible, aunque requiere alguna consideración adicional.

Según el artículo 16 de la LAECSP, la utilización de estos sistemas de identificación puede ser admitida en función de cuáles sean los datos e intereses afectados. En el caso que nos ocupa, los datos a los que se accedería serían el nombre y apellidos, DNI o NIE, domicilio, fecha de nacimiento, nacionalidad, año de llegada al municipio y personas con las que convive el interesado. Ninguno de estos datos tiene la consideración de dato especialmente protegido (artículo 7 de la LOPD), ni presenta ningún riesgo especial que impida utilizar esos sistemas de identificación, por lo que en principio puede ser admisible un sistema de identificación basado en una contraseña. En cambio, la utilización de alguna información que conozcan ambas partes puede presentar mayores problemas al no ofrecer suficientes garantías de seguridad, ya que la utilización de informaciones como el DNI o la fecha de nacimiento, por poner un ejemplo, pueden plantear problemas dada la relativa facilidad con que terceras personas pueden conocer dichas informaciones.

En cuanto a las dificultades de la implantación de un sistema basado en la asignación previa de contraseñas a aquellos ciudadanos que lo soliciten, es cierto que, según los apartados 3 y 4 del artículo 93 del RLOPD, este sistema requiere algunas medidas organizativas adicionales (establecimiento de un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad y la modificación de las contraseñas en periodos no inferiores a un año), pero hay que tener en cuenta que también podría ser utilizado como mecanismo de autenticación en la realización de otros trámites municipales.

En cualquier caso, la gestión de este sistema de contraseñas daría lugar a un nuevo tratamiento de datos de carácter personal que, como tal, estaría sometido a las obligaciones previstas en la normativa de protección de datos, como pueden ser, entre otras, la

obligación de creación de un fichero (artículo 20 de la LOPD) y de notificación al Registro de Protección de Datos de Cataluña (artículo 15 de la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos).

Sobre el sistema de autenticación que se propone en el texto de la consulta, no parece que un sistema de autenticación basado exclusivamente en la posesión del documento nacional de identidad, o de una fotocopia, sea un mecanismo que ofrezca suficientes garantías, ya que puede permitir que personas distintas de las interesadas accedan con excesiva facilidad a los datos que facilite el cajero.

Una posible solución sería combinar la exigencia de la identificación de un usuario mediante su DNI con el elemento adicional de una contraseña. A la presentación del DNI (que actuaría como usuario) para ser leído mediante escáner, se añadiría una contraseña o PIN facilitada por el propio ayuntamiento a todos aquellos ciudadanos que lo solicitasen.

Por ello, y especialmente si se considera la progresiva implantación del DNI electrónico (RD 1553/2005, de 23 de diciembre), así como el hecho de que, como se apunta, el Ayuntamiento pretenda ofrecer progresivamente más trámites para ser llevados a cabo mediante estos cajeros, se recomienda utilizar mecanismos de autenticación más robustos.

Con arreglo a las consideraciones realizadas en estos fundamentos jurídicos en relación con la consulta planteada sobre la posibilidad de que publicar las actas del Pleno y de la Junta de Gobierno en **el web municipal** pueda suponer una vulneración de la legislación de protección de datos personales, se adoptan las siguientes

Conclusiones

La posibilidad de que las personas interesadas puedan obtener por medios electrónicos volantes de empadronamiento no vulnera la normativa de protección de datos de carácter personal siempre y cuando se garantice el cumplimiento de las medidas de seguridad exigibles.

A fin de cumplir con las medidas de seguridad exigibles, es necesario implantar un sistema de identificación y autenticación basado en el DNI electrónico, otros sistemas de firma electrónica avanzada o un sistema basado en una contraseña o PIN previamente otorgado por el Ayuntamiento.

La autenticación basada exclusivamente en el escáner del documento nacional de identidad, o de una fotocopia del mismo, no se considera suficiente garantía desde el punto de vista de la seguridad.