Dictamen en relació amb la consulta formulada per un Ajuntament sobre la instal·lació de caixers electrònics per realitzar alguns tràmits administratius, entre d'altres l'obtenció de volants d'empadronament

Es presenta davant l'Agència Catalana de Protecció de Dades una consulta sobre si la instal·lació de caixers electrònics per realitzar alguns tràmits administratius, entre d'altres l'obtenció de volants d'empadronament pot suposar una vulneració de la legislació sobre protecció de dades.

En concret, es formulen dues qüestions: en primer lloc, si es pot considerar que l'ús d'aquests caixers per tal d'obtenir volants d'empadronament de residència i de convivència pot vulnerar la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD); en segon lloc, es consulta sobre quines mesures es consideren imprescindibles per garantir el compliment de l'esmentada normativa.

I

(...)

II

Tot i que la consulta que es formula pot referir-se a altres serveis municipals, la consulta es centra de manera concreta respecte la possibilitat d'accés al Padró municipal d'habitants. Per això en primer lloc farem algunes consideracions en relació amb la informació que s'hi conté.

Cal recordar, en primer lloc, que al padró municipal d'habitants s'han d'inscriure les persones residents en un municipi, amb una triple finalitat, d'acord amb la Llei 7/1985, de 2 d'abril, reguladora de les bases de règim local (en endavant, LRBRL): determinar la població del municipi, ésser requisit per adquirir la condició de veí i serveix per acreditar la residència i el domicili habitual (articles 15 i 16 LRBRL). A més d'aquestes funcions la Llei de Règim Electoral General (LOREG) preveu l'elaboració del cens electoral a partir de les dades incloses al padró que també serveix per elaborar estadístiques oficials. A això cal afegir, complementàriament, que el padró també pot servir per a la creació de fitxers o registres de població que tenen per finalitat la comunicació dels diferents òrgans de cada Administració pública amb els interessats residents en els territoris respectius, respecte a les relacions jurídicoadministratives derivades de les seves competències respectives (disposició addicional segona de la LOPD).

En el padró es contenen dades personals consistents en: el nom i cognoms, el domicili habitual, la data i el lloc de naixement, número del document d'identitat (o pels estrangers la tarja de residència o número del document acreditatiu de la seva identitat), certificat o títol escolar o acadèmic, a més d'aquelles dades que puguin ésser necessàries per a l'elaboració del cens electoral (article 16.2 LRBRL). La gestió del padró correspon als ajuntaments amb mitjans informàtics i han de realitzar les actuacions i operacions necessàries per a mantenir actualitzades les dades que es continguin en el padró per a que concordin amb la realitat (article 17 LRBRL).

Atès que el padró comporta el tractament de dades de caràcter personal li és d'aplicació el règim jurídic de protecció de dades de caràcter personal (LOPD) i per tant cal tenir en compte els principis i disposicions que es contenen en aquesta normativa.

L'article 3 de la LOPD, apartat d), considera tractament de dades el conjunt d'operacions i els procediments tècnics de caràcter automatitzat o no, que permetin recollir, gravar, conservar, elaborar, modificar, bloquejar i cancel•lar, així com les cessions de dades que se'n derivin. En conseqüència, qualsevol tractament que es faci per part de l'Ajuntament en tant que responsable del Padró, com ara la comunicació a través del sistema descrit a la consulta, quedarà sotmès als principis i disposicions que es contenen en la normativa de protecció de dades de caràcter personal, independentment de la naturalesa i característiques del fitxer de dades en què es puguin contenir.

Pel que fa al règim d'accés a les dades del Padró, i sens perjudici dels supòsits de cessió a l'INE o a altres administracions (arts. 16 i 17 LRBRL), l'article 40.2 del Text refós de la Llei municipal i de règim local de Catalunya (TRLMRLC), aprovat pel Decret legislatiu 2/2003, de 28 d'abril, estableix que les dades que consten al Padró són confidencials i l'accés a les mateixes es regeix per les normes que regulen l'accés administratiu dels ciutadans als arxius i als registres públics i per la Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades.

Convé tenir present, doncs, l'article 37.3 de la Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú (LRJPAC), que estableix que l'accés als documents que continguin dades de caràcter nominatiu, com seria el cas del padró, pot ser exercit pels titulars de les dades i també per aquelles altres persones que acreditin un interès legítim i directe.

Cal tenir en compte també, l'article 135.2 del Reglament de demarcació territorial i població dels ens locals (RDTPEL), aprovat pel Decret 140/1988, de 24 de maig, que limita la possibilitat d'accés a les dades del Padró a les persones interessades. Menció que cal entendre referida, en concordància amb el precepte esmentat de la LRJPAC, tant a la persona titular de les dades com també a aquelles altres persones que convisquin amb el mateix i pretenguin acreditar la convivència.

D'altra banda, l'article 61 del Reglament de Població i demarcació territorial dels ens locals (RPDTEL), aprovat pel Reial Decret 1690/1986, d'11 de juliol, estableix que es poden expedir certificacions del padró (art. 53.1) que hauran de ser expedides pel Secretari de l'Ajuntament (art. 61.1), com també volants d'empadronament amb caràcter purament informatiu en els que no seran necessàries les formalitats previstes per a les certificacions (art. 61.2).

Per tant, des d'aquesta perspectiva cap problema hi hauria en habilitar un sistema que, amb les degudes garanties i prèvia comprovació de l'existència de l'esmentat interès legítim, permeti accedir a les dades del padró per obtenir-ne un volant.

Ara bé, la resposta a la primera de les preguntes formulades en la consulta no pot fer-se deslligada de la segona, de manera que la legitimitat de la utilització dels caixers per a obtenir volants d'empadronament serà adequada o no en funció de quines siguin les mesures de seguretat aplicades.

III

Més enllà de la possibilitat apuntada en termes generals en l'apartat precedent, en la consulta es planteja l'adequació a la normativa de protecció de dades d'un sistema concret d'obtenció del volants d'empadronament basat en mitjans electrònics. En concret, pel que es desprèn de la consulta, es tractaria d'uns caixers o terminals electròniques des d'on, prèvia lectura mitjançant escàner del DNI o una fotocòpia del mateix, es facilitaria el volant.

Respecte a aquesta forma d'accés, s'ha de fer referència a la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics (LAECSP), que reconeix el dret dels ciutadans a relacionar-se amb les administracions públiques per mitjans electrònics (art. 1) i que té com una de les seves finalitats facilitar l'accés per mitjans electrònics dels ciutadans a la informació y al procediment administratiu (art. 3.2).

Des d'aquest punt de vista la iniciativa proposada s'emmarca plenament dins d'aquests objectius atès que, en definitiva, del que es tracta és de possibilitar l'obtenció de volants d'empadronament per mitjans electrònics directament per part dels interessats.

Ara bé, la consecució dels objectius previstos a la LAECSP es supedita per la pròpia llei al compliment d'un seguit de principis, entre els quals ens interessa destacar, als efectes d'aquesta consulta, el respecte al dret a la protecció de dades de caràcter personal (art. 4.a) i el principi de seguretat (art. 4.f), en virtut del qual la implantació i la utilització de mitjans electrònics per les administracions públiques s'haurà de dur a terme al menys amb el mateix nivell de garanties i seguretat que es requereix per a la utilització de mitjans no electrònics en l'activitat administrativa.

Principi de seguretat que adquireix una especial rellevança en el tractament de les dades de caràcter personal a tenor del que disposa l'article 9 de la LOPD, segons el qual, "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."

D'acord amb aquests principis, la pròpia LAECSP, als articles 14 a 16, regula els requisits d'identificació i autenticació dels ciutadans en les seves relacions amb l'administració per mitjans electrònics, permetent tant la utilització del Document Nacional d'Identitat electrònic (art. 14), com la utilització dels sistemes de signatura electrònica avançada que cada administració pública hagi admès i inclòs en una relació pública i accessible per mitjans electrònics (art. 15) o també, quan es justifiqui tenint en compte les dades i els interessos afectats, altres sistemes d'identificació com ara els basats en claus d'accés o alguna informació coneguda per ambdues parts i que ofereixi suficients garanties de confidencialitat (art. 16).

Per la seva banda, la normativa de protecció de dades, i en concret la regulació de les mesures de seguretat establertes pel Reglament de desplegament de la LOPD (RLOPD), aprovat pel Reial Decret 1720/2007, dins les mesures de nivell bàsic, i per

tant aplicables a qualsevol fitxer o tractament, estableix a l'article 93 els requisits per a la identificació i autenticació d'usuaris (entenent com a "autenticació" el procediment de comprovació de la identitat de l'usuari (art. 5.2.b) i com a "usuaris" els subjectes autoritzats per accedir a dades o recursos (art. 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."

Per tant, d'acord amb els preceptes esmentats cal que el sistema que s'instal.li en aquests caixers permeti identificar qui està sol.licitant el volant d'empadronament i que permeti comprovar que realment l'usuari és qui diu ser, als efectes de conèixer si és una de les persones legitimades per a poder sol.licitar el volant d'empadronament. I a més cal que ho faci amb suficients garanties.

A nivell teòric es consideren tres possibles factors d'autenticació:

- El que l'usuari coneix (contrasenya, PIN o una altra informació que conegui)
- El que l'usuari té (certificat digital, token USB etc.)
- El que l'usuari és (dades biomètriques)

La identificació i l'autenticació no plantejaria majors problemes, des del punt de vista de la protecció de dades si es dugués a terme mitjançant el DNI electrònic (art. 15.2 de la Llei 59/2003) o altres sistemes de signatura electrònica avançada (art. 3.2 de la Llei 59/2003), atès que aquests sistemes, que constitueixen sistemes d'identificació de doble factor (requereixen dos dels factors d'autenticació esmentats: el que és té i el que coneix) ofereixen suficients garanties.

Òbviament l'única precaució que caldria adoptar és que només sigui acceptada com a vàlida la identificació per part d'alguna de les persones que conviuen en un mateix domicili. Per altra banda, si s'utilitzen altres sistemes de signatura electrònica avançada d'acord amb el que estableix la Llei 59/2003, de signatura electrònica, cal tenir en compte que d'acord amb l'article 15.2 LAECSP l'Ajuntament hauria d'incloure els sistemes admesos en una relació pública i accessible per mitjans electrònics.

La utilització d'un sistema basat en contrasenyes ofereix menys garanties que els anteriors, però podria resultar igualment admissible, tot i que requereix però fer alguna consideració addicional.

D'acord amb l'article 16 de la LAECSP la utilització d'aquests sistemes d'identificació pot ser admesa en funció de quines siguin les dades i els interessos afectats. En el cas que ens ocupa les dades a les quals s'accediria serien el nom i cognoms, el DNI o NIE, domicili, data de naixement, nacionalitat, any d'arribada al municipi i persones amb que l'interessat conviu. Cap d'aquestes dades té la consideració de dada especialment protegida (art. 7 LOPD), ni presenta cap risc especial que impedeixi utilitzar aquests sistemes d'identificació, per la qual cosa en principi pot ser admissible un sistema d'identificació basat en una contrasenya. En canvi la utilització d'alguna una informació que coneguin ambdues parts pot presentar majors problemes per no oferir suficients garanties de seguretat, atès que la utilització d'informacions com ara el DNI o la data de naixement, per posar un exemple, poden plantejar problemes atesa la relativa facilitat amb que terceres persones poden conèixer aquestes informacions.

Quant a les dificultats de la implantació d'un sistema basat en l'assignació prèvia de contrasenyes a aquells ciutadans que ho sol·licitin, si que és cert que, d'acord amb els apartats 3 i 4 de l'article 93 RLOPD, requereix algunes mesures organitzatives addicionals (establiment d'un procediment d'assignació, distribució i emmagatzemament que en garanteixi la confidencialitat i integritat i de modificació de les contrasenyes en períodes no inferiors a un any), però cal tenir en compte que també podria ser utilitzat com a mecanisme d'autenticació en la realització d'altres tràmits municipals.

En qualsevol cas, la gestió d'aquest sistema de contrasenyes donaria lloc a un nou tractament de dades de caràcter personal que com a tal quedaria sotmès les obligacions previstes a la normativa de protecció de dades com ara, entre d'altres, l'obligació de creació d'un fitxer (art. 20 LOPD) i de notificació al Registre de Protecció de Dades de Catalunya (art. 15 de la Llei 5/2002,de 19 d'abril, de l'Agència Catalana de Protecció de Dades).

Pel que fa al sistema d'autenticació que es proposa en el text de la consulta, no sembla que un sistema d'autenticació basat exclusivament en la possessió del document nacional d'identitat, o d'una fotocòpia, sigui un mecanisme que ofereixi suficients garanties atès que pot permetre que persones diferents a les interessades accedeixin amb excessiva facilitat a les dades que faciliti el caixer.

Una possible solució seria combinar l'exigència de la identificació d'un usuari amb el DNI, amb l'element addicional d'una contrasenya. A la presentació del DNI (que actuaria com a usuari) per a ser llegit mitjançant un escàner, s'hi afegiria una contrasenya o PIN facilitada pel propi Ajuntament a tots aquells ciutadans que ho sol·licitin.

Per això, i especialment si és té en compte la progressiva implantació del DNI electrònic (R.D. 1553/2005, de 23 de desembre) com també el fet que, com s'apunta, l'Ajuntament vulgui afegir més tràmits progressivament per ser duts a terme a través d'aquests caixers, es recomana utilitzar mecanismes d'autenticació més robusts.

D'acord amb les consideracions fetes en aquests fonaments jurídics en relació amb la consulta plantejada en relació amb la possibilitat que la instal·lació de caixers electrònics per realitzar alguns tràmits administratius, entre d'altres l'obtenció de volants d'empadronament pugui suposar una vulneració de la legislació de protecció de dades personals, es fan les següents,

Conclusions

La possibilitat que les persones interessades puguin obtenir a través de mitjans electrònics volants d'empadronament no vulnera la normativa de protecció de dades de caràcter personal sempre que es garanteixi el compliment de les mesures de seguretat exigibles.

Per tal de complir les mesures de seguretat exigibles, cal implantar un sistema d'identificació i autenticació basat en el DNI electrònic, altres sistemes de signatura electrònica avançada o en un sistema basat en una contrasenya o PIN prèviament atorgat per l'Ajuntament.

L'autenticació basada exclusivament en l'escaneig del Document Nacional d'Identitat, o d'una fotocòpia d'aquest, no es considera que ofereixi suficients garanties des del punt de vista de la seguretat.