PD 10/2016

Informe en relació amb l'Avantprojecte de llei del procediment de votació electrònica per als catalans i catalanes residents a l'estranger.

Antecedents

Es presenta davant l'Autoritat Catalana de Protecció de Dades l'Avantprojecte de llei del procediment de votació electrònica per als catalans i catalanes residents a l'estranger, als efectes que l'Autoritat emeti l'informe corresponent.

L'Avantprojecte de llei consta d'una exposició de motius, de 15 articles, de tres disposicions addicionals, i de dues disposicions finals.

Examinat l'Avantprojecte de llei, que no s'acompanya de la Memòria general i la Memòria d'avaluació d'impacte, vist l'Informe del Coordinador d'Auditoria i Seguretat de la Informació de l'Autoritat i l'informe de l'Assessoria Jurídica de l'Autoritat, i tenint en compte la normativa vigent aplicable, s'emet l'informe següent.

Fonaments jurídics

I

(...)

II

Segons l'exposició de motius de l'Avantprojecte, l'article 56 de l'Estatut d'autonomia de Catalunya (EAC) disposa, en l'apartat segon, que *"El règim electoral és regulat per una llei del Parlament aprovada en una votació final sobre el conjunt del text per majoria de dues terceres parts dels diputats.(...)."*, de manera que l'EAC reconeix de forma expressa la capacitat de Catalunya de dotar-se d'una llei que estableixi el seu règim electoral i, en conseqüència, la capacitat de dotar-se d'una llei que reguli aspectes concrets o parcials del règim electoral, com és el cas del procediment de votació electrònica per als catalans i catalanes que viuen a l'estranger.

L'exposició de motius exposa la necessitat de regular el procediment de votació electrònica en favor d'un col·lectiu específic que troba especials dificultats en l'exercici del dret de vot per via presencial, com és el dels catalans i catalanes residents a l'estranger. Segons l'Avantprojecte, la introducció de l'ús dels mitjans electrònics en el procés de vot hauria de permetre millorar la seva participació.

En relació amb el vot dels residents a l'estranger, l'exposició de motius fa esment, entre d'altres, dels Informes 580/2010 i 748/2013, de la Comissió Europea per a la Democràcia a través del Dret (Comissió de Venècia), segons els quals, l'obligació de votar en una ambaixada o un consolat pot, a la pràctica, restringir seriosament el dret de vot d'aquests ciutadans (apartat 95 de l'Informe 580/2010), i l'adopció de mesures eficaces a favor dels votants a l'estranger implica fer que tant el registre com l'exercici del dret de vot siguin tan fàcils com sigui possible, si cal, multiplicant el nombre de centres de votació i els mètodes de votació, inclosos els serveis postals, Internet i les delegacions de vot (apartat 36 de l'Informe 748/2013).

L'Avantprojecte també es refereix a l'Informe del Consejo de Estado de 24 de febrer de 2009, en el que es remarca que la votació a l'exterior és la que més es podria beneficiar de la introducció de sistemes de sufragi electrònic, bé mitjançant l'ús de l'urna electrònica, bé mitjançant la modalitat de vot per Internet, i que el model triat ha de complir com a mínim els requeriments següents: que no es pugui relacionar els vots emesos amb els votants; que cada votant pugui emetre un sol vot; que el resultat de la votació sigui el correcte; i que no es puguin emetre resultats parcials que puguin condicionar el resultat de la votació.

En relació amb l'Avantprojecte cal prendre en consideració, entre d'altres, la Recomanació (2004)11, del Comitè de Ministres del Consell d'Europa, sobre els estàndards legals, procedimentals i tècnics dels sistemes de votació electrònica –a la que es fa esment, abastament, en l'Informe 3/2010, citat, d'aquesta Autoritat (FJ II, al que ens remetem)-. Fem notar que, segons consta en el web del Consell d'Europa (www.coe.int), aquesta Recomanació de 2004 es troba en procés de revisió i d'actualització. Segons la Recomanació (2009)1, sobre democràcia electrònica (*"e-democracy"*), del Comitè de Ministres del Consell d'Europa, l'e-democràcia ha d'oferir oportunitats específiques a persones que no puguin estar físicament presents en les reunions i eleccions democràtiques (Directrius o "*Guidelines*", ap. 74). Als efectes que ens ocupen, destaquem que, segons aquesta Recomanció de 2009, el dret d'accés efectiu a l'e-democràcia i a les seves eines s'ha de ponderar amb la necessitat de protegir els drets, inclosa la intimitat i les dades personals, entre d'altres (Directrius, ap. 82); que en establir-se mètodes i eines d'e-democràcia, cal prestar especial atenció a la seguretat electrònica, que inclou la seguretat de la informació, de les dades (incloent el compliment dels requisits de la protecció de dades), i la seguretat dels documents, entre d'altres (Directrius, ap. 96).

Es fa avinent que aquesta Autoritat va emetre el Dictamen 3/2010, en relació amb la consulta formulada pel President del Parlament de Catalunya sobre el vot electrònic amb vistes a l'elaboració de la Proposició de llei electoral de Catalunya, que es pot consultar al web www.apd.cat. En aquest Dictamen s'analitzen, des de la perspectiva de la protecció de dades, però també des d'un enfocament més ampli de seguretat de la informació, diverses qüestions relacionades amb la implantació de sistemes de vot electrònic que són d'interès en relació amb l'Avantprojecte de llei que s'examina. Fem avinent que tot allò que, amb caràcter general, es va posar de manifest en el Dictamen 3/2010, segueix sent vàlid, en especial, els apartats relatius als riscos dels diferents sistemes de votació electrònica i a les conclusions del Dictamen.

III

L'Avantprojecte de llei té per objecte *"regular el procediment de votació electrònica per als catalans i catalanes residents a l'estranger"* (article 1).

El dret de vot de les persones residents a l'estranger es troba regulat a l'article 75 de la LOREG, segons el qual en eleccions a membres de les Assemblees legislatives de les Comunitats autònomes, entre d'altres, els espanyols inscrits al cens dels electors residents-absents que viuen a l'estranger han de formular la corresponent sol·licitud de vot (art. 75.1 LOREG). Els electors poden optar per exercir per correu el seu dret a vot (art. 75.4 LOREG), o bé poden optar per dipositar el vot a l'urna en les oficines o seccions consulars on consten inscrits (art. 75.5 LOREG).

En qualsevol cas, la LOREG no preveu la possibilitat, per als residents a l'estranger, d'exercir el seu vot per mitjans electrònics.

Tenint en compte això, d'entrada, cal fer avinent que la possibilitat i la viabilitat del sistema de vot electrònic a les eleccions autonòmiques, òbviament està condicionada a la regulació d'aquesta modalitat de vot mitjançant una llei electoral de Catalunya, atès que la LOREG no preveu aquest sistema de votació, ni amb caràcter general ni, específicament, per als electors residents a l'estranger.

Als efectes d'aquest informe cal abordar l'aplicabilitat de la normativa de protecció de dades, atès que en funció de quina sigui la normativa aplicable poden resultar exigibles a partir de la legislació vigent determinades garanties pel que fa al tractament de dades personals derivat del procediment de votació electrònica per als catalans i catalanes residents a l'estranger.

D'acord amb l'article 2.3.a) de l'LOPD, els fitxers regulats per la legislació electoral es regeixen per la seva normativa específica i per allò que, si escau, preveu expressament la mateixa LOPD per a aquests fitxers.

Per tant l'LOPD i la seva normativa de desplegament només resulten d'aplicació en aquelles previsions expressament previstes a la mateixa LOPD. I el cert és que en la LOPD no figura cap altra referència expressa a la matèria electoral -tret de la ja esmentada de l'article 2.3.a)-, que una referència colateral inclosa a la disposició addicional segona per tal d'habilitar que l'Administració General de l'Estat i les administracions de les Comunitats Autònomes puguin sol·licitar a l'Institut Nacional d'Estadística (INE) una còpia actualitzada del fitxer format amb les dades de nom, cognoms, domicili, sexe i data de naixement que consten en el padró municipal d'habitants i en el cens electoral corresponents als territoris en què exerceixen les seves competències.

Ara bé, que no resulti d'aplicació l'LOPD ni la seva normativa de desplegament no implica que no s'hagi de respectar el dret fonamental a la protecció de dades. Ans al contrari, trobem previsions tant a nivell constitucional (art. 18.4 CE, i jurisprudència constitucional –STC 292/2000-), com a nivell estatutari (art. 156 EAC), com també en la normativa electoral general, que porten a considerar que una eventual llei que incorpori un sistema de vot electrònic, com seria l'Avantprojecte examinat, ha de preveure les garanties necessàries per a la protecció d'aquest dret.

Més enllà de referències ja fetes (Recomanacions del Consell d'Europa, de 2004 i 2009), cal tenir en compte que la Convenció 108 per a la protecció de les persones pel que fa al tractament automatitzat de dades de caràcter personal (28 de gener de 1981), ratificada per Espanya el 30 de gener de 1994, que vincula igualment l'Estat espanyol, i en conseqüència també la Generalitat de Catalunya, pel que fa al dret a la

protecció de dades de caràcter personal sense que es prevegi cap exclusió o reserva pel que fa a la matèria electoral.

Des de la perspectiva de la protecció de dades cal tenir també en compte el Reglament general de protecció de dades (UE) 2016/679 (en endavant, RGPD), que va entrar en vigor el 25 de maig de 2016, i que serà aplicable a partir del 25 de maig de 2018 (art. 99 RGPD). El RGPD (art. 2) no exclou expressament del seu àmbit d'aplicació material la matèria electoral tot i que no s'aplica al tractament de dades personals en l'exercici d'una activitat no compresa en l'àmbit d'aplicació del Dret de la Unió (art. 2.2.a) RGPD).

En qualsevol cas, el RGPD disposa que el tractament de dades sobre les opinions polítiques de les persones, només pot produir-se per raons d'interès públic i sempre que s'ofereixin les garanties adequades (Considerant 56 RGPD).

En qualsevol cas, com ha reconegut la STC 292/2000, mitjançant el dret a la protecció de dades es tracta no només de la protecció del dret a la intimitat de les persones -en la mesura que es pot considerar que l'opció política pot formar part de la intimitat-, sinó també de la protecció d'altres drets fonamentals, en especial el dret de sufragi o el dret a la no-discriminació. Per tant, la no-existència de garanties adequades que garanteixin el secret del vot pot actuar com a mecanisme dissuasiu que acabi afectant la participació en el procés electoral, i de retruc la seva pròpia legitimitat, com també que pèrdues d'informació o tractaments inadequats de la informació vinculada al procés electoral poden donar lloc a pràctiques discriminatòries (en aquest sentit, el Considerant 71 del RGPD).

Atesa la naturalesa dels processos electorals, ens trobem davant d'informació que el Conveni 108 (art. 6) – i també l'LOPD (art. 7) tot i no ser aplicable en aquest cas- considera com a dades que requereixen una protecció especial, atès que en la informació tractada amb ocasió del vot electrònic ens trobarem no només les dades identificatives de les persones incloses al cens, sinó també altra informació més sensible com el fet d'haver exercit el dret de vot o no i, en especial, el sentit del vot. Ens trobem doncs, clarament, davant de dades que revelen l'opinió política dels ciutadans i que per tant requereixen una especial protecció. L'especial naturalesa, mereixedora de protecció reforçada, de les dades relatives a les opinions polítiques dels ciutadans, també queda palesa en el RGPD (Considerant 75, i article 9 RGPD).

Per tot l'exposat, és clar que que en relació amb les previsions de l'Avantprojecte, caldrà aplicar garanties adequades en relació amb el dret fonamental a la protecció de dades de caràcter personal.

En aquest punt, cal referir-se al Considerant 84 del RGPD, segons el qual:

> *"A fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una* ***evaluación de impacto relativa a la protección de datos,*** *que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento."*

L'avaluació d'impacte sobre la privacitat està regulada a l'article 35 del RGPD, i interessa destacar en aquest moment que l'apartat 10 d'aquest article estableix que si en el procediment d'aprovació de la norma es sotmet el projecte a una avaluació d'impacte sobre la privacitat, després no serà necessari fer una avaluació d'impacte quan es duguin a terme els tractaments que se'n derivin.

Com ha quedat exposat, l'Avantprojecte suposa el tractament d'informació personal relacionada amb la ideologia política de les persones, especialment protegida per l'ordenament jurídic, informació que afecta drets com ara l'exercici del sufragi. En cas de ser utilitzada fraudulentament, no només pot afectar el resultat del procés (per la possibilitat real d'alteració del resultat o per la manca de confiança generada en els ciutadans) sinó que fins i tot comportar situacions discriminatòries o de coacció per als afectats.

Per tot això, tenint en compte que el RGPD ja ha entrat en vigor i serà d'aplicació a partir del proper 25 de maig de 2018, i vist que l'Avantprojecte pot implicar el tractament de dades especialment protegides, i que aquest tractament afectarà un nombre molt ampli de persones, seria convenient la realització d'una avaluació d'impacte de les previsions de l'Avantprojecte, i haver-ne disposat en el moment d'emetre aquest informe.

IV

Ens referim a continuació al model de procediment de votació electrònica que configura l'Avantprojecte.

Com fa avinent aquesta Autoritat en el seu Dictamen 3/2010 (FJ IV):

> *"(...) malgrat que s'acostumi a utilitzar una mateixa denominació, vot electrònic, per referir-se als diferents sistemes possibles, existeixen profundes diferències entre uns i altres sistemes que aconsellen distingir, com a mínim, entre els sistemes de vot electrònic presencial i els sistemes de vot electrònic remot.*
>
> *En els primers, és a dir entre els sistemes presencials, s'hi inclourien tant els sistemes que es limiten a facilitar la lectura electrònica de les paperetes com els que permeten introduir l'opció de vot directament a través d'un terminal ubicat als col·legis electorals (sistemes RED o de Registre Electrònic Directe), com també aquells en els quals el terminal facilita el vot incorporat en un suport electrònic que és introduït a la urna electrònica.*
>
> *Els sistemes de vot remot, en canvi, seguint la definició que en dóna la Recomanació 2004 (11) del Consell d'Europa, són aquells sistemes en els que el sufragi es registra a través d'un dispositiu no controlat per l'autoritat electoral. L'element clau no és doncs la llunyania del lloc on s'exerceix el vot (el vot en una ambaixada no seria un vot remot) sinó l'absència de control presencial per part de l'autoritat electoral en el moment d'expressar-se el vot. (...)"*

Així, per al cas que ens ocupa, els sistemes de vot electrònic presencial possibilitarien l'emissió del vot electrònic des d'un lloc llunyà respecte de l'espai on es realitza la votació, però aquesta es fa a través de terminals facilitats i controlats per l'autoritat electoral (consolats o ambaixades, o altres espais habilitats per l'administració electoral).

En els sistemes de vot remot, el sufragi es registra a través d'un dispositiu no controlat per l'autoritat electoral. En aquest cas l'element clau no és la llunyania del lloc on s'exerceix el vot (el vot en una ambaixada no seria un vot remot) sinó l'absència de control presencial per part de l'autoritat electoral en el moment d'expressar-se el vot.

Com exposa l'Informe del Consejo de Estado, citat:

> *"Las modalidades de voto electrónico más frecuentes hoy en día son la votación mediante urna electrónica y el voto por Internet. Los sistemas de* ***urna electrónica*** *son sistemas de votación parecidos a los actuales pues requieren que el elector se desplace al colegio electoral. Una vez allí, sin embargo, la votación se realiza directamente en una máquina que, por lo general, está dotada de pantalla táctil y con funciones adaptadas para personas mayores o con determinadas discapacidades (aunque también pueden emplearse las tarjetas con banda magnética de votación que serán después leídas en las urnas electrónicas). El voto se realiza directamente en la urna y se contabiliza sobre la marcha, aunque algunos sistemas, como el belga y el de algún estado norteamericano, imprimen una papeleta de control que se deposita en una urna para garantizar que los resultados sean correctos.*
>
> *El* ***voto por Internet*** *permite un ejercicio no presencial o "remoto" del voto. Para ello se ha de disponer de un ordenador conectado a la red a través de una conexión cifrada y segura y es imprescindible la articulación de controles de fiabilidad y autenticidad mayores que los requeridos para cualquier otro tipo de voto electrónico.(...)".*

Es tracta, doncs, de dos models clarament diferenciats i que, com es fa avinent en el Dictamen 3/2010, des de la perspectiva de la protecció de dades poden presentar riscs i característiques diferents (en relació amb la identificació i l'autenticació de l'afectat, entre d'altres).

Per la informació disponible, sembla que l'Avantprojecte configura un sistema de vot electrònic remot. Com exposa l'article 8.1 de l'Avantprojecte, l'elector que opti per exercir el dret de vot per mitjans electrònics, accedeix a la *"Plataforma de votació electrònica per Internet"* mitjançant unes credencials que li hauran estat prèviament assignades. Segons l'article 7.4 de l'Avantprojecte, l'elector rep les credencials necessàries per exercir el dret de vot per mitjans electrònics en la seva adreça de correu electrònic o en el seu dispositiu mòbil. Segons l'article 8.3 de l'Avantprojecte, l'elector pot exercir el dret de vot per mitjans electrònics un cop s'hagi identificat a la Plataforma de votació electrònica per Internet, i fins i tot descarregar-se un justificant *"des de la pròpia Plataforma de votació electrònica per Internet".*

Per aquestes i altres referències fetes en l'Avantprojecte a la *"Plataforma de votació electrònica per Internet",* sembla que el procediment de votació es configura com un sistema de vot electrònic remot, que l'afectat podrà exercir a través d'aquesta "Plataforma", a la que podrà accedir a través d'Internet, per tant, es dedueix, a través dels propis dispositius de l'elector (un ordinador, etc). En definitiva, sembla que el procediment de votació electrònica previst en l'Avantprojecte no es produiria a través de terminals facilitats i controlats per l'autoritat corresponent en un espai determinat (ambaixada...), sinó a través de dispositius del propi interessat.

Ara bé, cal fer avinent que l'Avantprojecte conté diverses referències expresses a la *"urna electrònica"* que, com hem vist, és un element propi dels sistemes presencials de vot electrònic i, per tant, de sistemes clarament diferents de la votació electrònica per Internet.

Així, l'article 8 de l'Avantprojecte, en els seus apartats 7 i 8, expliciten que l'elector, un cop emès el vot, pot descarregar-se un justificant de la Plataforma de votació electrònica per Internet, *"que indiqui que el seu vot ha estat emès i dipositat a l'urna electrònica".* L'article 9 de l'Avantprojecte fa referència *als "vots emesos per mitjans electrònics a l'urna electrònica".* L'article 10.2 de l'Avantprojecte, en relació amb l'escrutini dels vots emesos per mitjans electrònics, preveu que el President de la Mesa Electoral accedeix a l'urna electrònica amb les claus de seguretat que li facilita la Comissió de garantia (art. 11.4 Avantprojecte). De fet, les previsions de l'article 10 de l'Avantprojecte, referides a l'urna electrònica, sembla que reprodueixen l'esquema de l'article 75 LOREG, apartats 10 i 11.

Des de la perspectiva de la protecció de dades i del model de seguretat, un i altre sistema poden presentar riscos particulars, en les diverses fases clau de desenvolupament del procediment de votació (fase d'identificació i autenticació; fase d'emissió del vot; fase d'escrutini i destrucció de la informació; fase de control o verificació). Així es posa de manifest en el FJ VI del Dictamen 3/2010, en relació amb els sistemes de vot electrònic presencial, i en el FJ VII del mateix Dictamen, en relació amb els sistemes de vot electrònic remot, consideracions que, com ha quedat dit, segueixen vigents.

Per tot l'exposat es fa avinent que si, com sembla, l'Avantprojecte configura un procediment de votació electrònica per Internet com a sistema de vot remot, convindria revisar les referències fetes a la urna electrònica i substituir-les, si escau, per les que corresponguin, als efectes de clarificar el model configurat per l'Avantprojecte.

Feta aquesta consideració prèvia, i partint de la premissa que l'Avantprojecte configura un sistema de vot electrònic remot a través de la Plataforma de vot electrònic per Internet, fem avinent el següent.

V

L'article 2 de l'Avantprojecte, disposa que el procediment de votació electrònica té un caràcter complementari respecte les previsions de l'article 75 LOREG, així com un *"Caràcter facultatiu, atès que l'elector pot escollir entre votar electrònicament o votar mitjançant papereta."* És a dir, l'afectat (art. 3.e) LOPD), podrà escollir entre exercir el seu dret a vot electrònicament o mitjançant papereta.

L'Informe citat del Consejo de Estado posa de manifest, respecte el vot per Internet, la conveniència que "*al menos en un primer momento, dicho procedimiento de votación tenga carácter alternativo al procedimiento de voto por correo, configurándose ambos como dos opciones frente al voto en urna."*

Cal valorar positivament que l'Avantprojecte configuri el procediment de votació electrònica per als catalans i catalanes residents a l'estranger com a facultatiu i, per tant, com a sistema alternatiu a l'exercici de vot mitjançant papereta, sense condicionar així l'exercici del dret a vot a la necessària utilització d'aquest procediment.

L'article 2 de l'Avantprojecte també preveu, lògicament, el *"caràcter excloent"* del procediment, atès que l'elector que triï votar electrònicament no podrà votar mitjançant papereta i viceversa.

En relació amb aquest caràcter excloent, l'article 6.4 de l'Avantprojecte disposa que, sempre que l'elector hagi sol·licitat l'exercici del dret de vot per mitjans electrònics, les

delegacions provincials de l'OCE (oficina del cens electoral) no trametran a l'elector la documentació detallada per la normativa estatal vigent en aquesta matèria (entenent que aquesta referència es fa a la documentació prevista en l'article 75.2 LOREG). Aquesta previsió pretén, doncs, evitar duplicitats en el vot, i per tant es considera adequada. Ara bé, cal apuntar que l'article 6.4 de l'Avantprojecte es refereix només *"als casos previstos"* a l'apartat 3 de l'article 6 de l'Avantprojecte (referit a una adaptació dels impresos oficials que es podria produir en el futur). Sembla que la previsió de l'article 6.4 s'hauria de referir a tots els casos en què l'elector sol·licita exercir el vot per mitjans electrònics, i no només a la possibilitat de l'article 6.3 de l'Avantprojecte.

VI

L'article 4 de l'Avantprojecte, detalla l'àmbit subjectiu, en els següents termes: *"El procediment de votació electrònica s'aplica als catalans i catalanes residents a l'estranger inscrits en el Cens Electoral dels Residents Absents (CERA)."*

Segons disposa l'article 6.1 de l'Avantprojecte, la sol·licitud del vot per part dels electors catalans inscrits al CERA, es regeix per la normativa estatal vigent en aquesta matèria. L'article 6.2 de l'Avantprojecte afegeix que:

"D'acord amb la normativa vigent en matèria de protecció de dades de caràcter personal, l'Oficina del Cens Electoral (OCE) posarà a disposició de l'òrgan competent en matèria electoral de l'Administració de la Generalitat de Catalunya les dades que figuren en el CERA, relatives als electors catalans residents a l'estranger que hagin presentat la sol·licitud de vot, (...), a l'únic efecte d'habilitar la Plataforma de votació electrònica per Internet."

Segons disposa l'article 31 de la LOREG:

> *"(...)*
> *2. El censo electoral está compuesto por el censo de los electores residentes en España y por el censo de los electores residentes-ausentes que viven en el extranjero. Ningún elector podrá figurar inscrito simultáneamente en ambos censos.*
> *3. El censo electoral es único para toda clase de elecciones, (...)."*

Segons l'article 30 de la LOREG, l'Oficina del Cens Electoral té, entre les seves competències, la coordinació i la supervisió de l'elaboració del cens electoral. Segons disposa l'article 32.3 de la LOREG, les oficines consulars i seccions consulars tramiten d'ofici la inscripció dels espanyols residents a la seva demarcació en la forma que es disposi reglamentàriament.

En definitiva, el cens d'electors residents-absents (CERA) és la base de dades que conté les dades personals dels afectats per l'Avantprojecte, que és responsabilitat de l'Oficina del Cens Electoral (enquadrada en l'INE, segons disposa l'article 29 LOREG).

A aquests efectes l'Avantprojecte, que és norma amb rang de llei, preveu la comunicació de dades personals del CERA a l'òrgan competent de la Generalitat, de manera que, sobre la base de la previsió de la disposició addicional segona de l'LOPD, citada, l'Avantprojecte que informem habilitaria la comunicació prevista, per bé que la LOREG no prevegi la dita comunicació.

Cal tenir en compte que el CERA és únic per a totes les eleccions i engloba tots els residents a l'estranger de l'Estat (art. 31 LOREG), de manera que, òbviament, el procediment de votació electrònica previst en l'Avantprojecte implicarà un previ

tractament de dades personals que necessàriament haurà de dur a terme l'Oficina del Cens Electoral, responsable del CERA, per tal de comunicar, només, les dades pertinents, adequades i no excessives (art. 4 LOPD), és a dir, les corresponents als afectats inclosos al CERA amb dret de vot en eleccions al Parlament de Catalunya i, si escau, en altres processos electorals (art. 3 Avantprojecte).

Fem notar que, segons l'Avantprojecte (disposició addicional tercera, apartat 2), en els protocols o convenis de col·laboració que es subscriuran amb l'Administració General de l'Estat, l'Administració Electoral i l'Oficina del Censo Electoral (OCE) enquadrada a l'Institut Nacional d'Estadística, s'establiran, entre d'altres aspectes, *"La posada a disposició de l'òrgan competent en matèria electoral de l'Administració de la Generalitat de Catalunya de les dades del CERA relatives als electors catalans residents a l'estranger que hagin presentat la sol·licitud de vot; i el termini i la forma de posada a disposició de les dades esmentades".*

Per tot l'exposat, per bé que, com s'ha apuntat, el flux informatiu (comunicació de determinades dades personals del CERA a l'òrgan competent de la Generalitat), es pot considerar habilitat, l'Avantprojecte no concreta determinats elements del dit flux informatiu, que hauran de concretar-se necessàriament en els dits acords o protocols.

En concret, aquests hauran de concretar les dades personals que hauran de ser objecte de comunicació a l'òrgan competent de la Generalitat. També caldrà que els acords o protocols explicitin la comunicació de dades del CERA únicament en relació amb les persones afectades per l'Avantprojecte (art. 4 Avantprojecte), és a dir, únicament les que hagin formalitzat prèviament la seva sol·licitud conforme el que disposa l'article 75.1 de la LOREG. També seria pertinent que els acords o protocols incloguessin alguna referència a la seguretat en la transmissió o lliurament de la informació extreta del cens electoral.

Sens perjudici que en aquests acords o protocols es puguin concretar certes qüestions, des de la perspectiva del principi de qualitat cal estar al que preveu el Reial decret 157/1996, de 2 de febrer, que disposa l'actualització mensual del Cens electoral i regula les dades necessàries per a la inscripció en el cens. L'article 2.2 del dit Reial decret concreta les dades dels residents a l'estranger que tracta el CERA i, per tant, cal entendre que la comunicació de dades entre el CERA i l'òrgan competent de la Generalitat es referiria a les dades que hi constin que siguin necessàries per al procés electoral, respecte dels electors que hagin sol·licitat exercir el vot electrònic.

VII

Resulta especialment rellevant l'article 5 de l'Avantprojecte, que enumera els principis del procediment de votació electrònica.

Aquests principis fan referència expressa, entre d'altres, a la seguretat en totes les fases del procediment de votació electrònica, i la seguretat tècnica dels procediments de transmissió i d'emmagatzematge de la informació, amb mesures que garanteixin la traçabilitat i mesures contra manipulacions o suplantacions en el procediment de votació. També es fa esment de l'autenticació robusta, en el sentit que el procediment de votació electrònica es fonamenta en l'aprovisionament segur de credencials i en l'autenticació basada en certificats digitals i claus d'un sol ús, entre moltes altres qüestions.

D'entrada, cal valorar positivament aquestes previsions en què es fonamenta l'Avantprojecte, des de la perspectiva del la protecció de dades i dels elements de

seguretat que cal tenir en compte en el disseny i la implantació del procediment de votació electrònica que ens ocupa.

En aquest sentit, fem avinent que la normativa de protecció de dades estableix la protecció de dades des del disseny i per defecte (Considerant 78 i article 25 RGPD).

L'article 14.1 de l'Avantprojecte disposa que l'òrgan competent *"ha d'adoptar les mesures de seguretat necessàries per evitar l'alteració, la pèrdua, el tractament o l'accés no autoritzat del vot electrònic i, atenent a la naturalesa de les dades, ha d'aplicar mesures de seguretat de nivell alt, d'acord amb la normativa vigent de protecció de dades de caràcter personal."*

Cal valorar positivament la menció expressa, en l'Avantprojecte, de la necessitat d'aplicar mesures de seguretat de nivell alt, que en qualsevol cas s'han d'estendre a les diferents fases del procediment de votació electrònica objecte de regulació.

Ara bé, cal tenir en compte que el RGPD, aplicable a partir del 25 de maig de 2018, configura un sistema de seguretat que no es basa en els nivells de seguretat bàsic, mitjà i alt, previstos a l'LOPD i que segueixen temporalment vigents, sinó en determinar, arran d'una prèvia valoració dels riscos, quines mesures de seguretat són necessàries en cada cas, tenint en compte el tipus d'informació tractada (Considerant 83 RGPD). Segons l'article 24.1 RGPD:

> *"Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario."*

Atès que l'Avantprojecte de llei regula un procediment de votació electrònica que es preveu que tingui continuïtat en el temps, i que el RGPD serà aplicable a partir del 25 de maig de 2018, enlloc de referir-se a mesures de seguretat "de nivell alt", es podria emprar una terminologia adaptada al RGPD, en relació amb les mesures de seguretat que caldrà implantar.

Per exemple, l'article 14.1 de l'Avantprojecte es podria redactar en el sentit que l'òrgan competent *"ha d'adoptar les mesures de seguretat necessàries per evitar l'alteració, la pèrdua, el tractament o l'accés no autoritzat del vot electrònic, i totes les que resultin necessàries d'acord amb la normativa de protecció de dades de caràcter personal, atenent a la naturalesa de les dades i a la gravetat i la probabilitat dels riscos per als drets i llibertats de les persones electores."*

Dit això, convé les següents consideracions, en relació amb les diferents fases del procediment de votació electrònica previst en l'Avantprojecte.

1.- Fase d'identificació i autenticació

Com es fa avinent en el Dictamen 3/2010, en aquesta fase s'han d'extremar les precaucions per evitar que el sistema de presentació i verificació de credencials sigui vulnerat, i que un tercer pugui accedir al sistema fent-se passar per un altre, per tant suplantant la seva identitat i accedint als seus drets en relació a la informació o funcions autoritzades.

El procediment de votació electrònica s'inicia en el moment que un elector inscrit al CERA presenta la seva sol·licitud de vot, seguint la normativa estatal en la matèria (art. 6.1 Avantprojecte). Segons l'article 7.1 de l'Avantprojecte, un cop formulada la sol·licitud de vot, l'elector s'ha d'identificar a la Plataforma mitjançant les seves dades personals (nom, cognoms, DNI, data de naixement, adreça postal, adreça de correu electrònic i dispositiu mòbil) i la clau de tramitació telemàtica (CTT) que figura en l'imprès que prèviament li ha tramès l'OCE. Ara bé, no es fa referència a les mesures de seguretat relacionades amb la identificació per sol·licitar el vot, o per fer la tramesa de l'imprès. (Això, sens perjudici que l'article 7.1 preveu, alternativament, l'ús del DNI electrònic o de certificats reconeguts a la *"Llista de confiança de prestadors qualificats de serveis electrònics de confiança"* (Reglament UE 910/2014)).

Aquest tràmit de la identificació de l'afectat és especialment crític, ja que és en el moment que un elector sol·licita votar electrònicament i es registra a la Plataforma, que cal assegurar que es tracta efectivament de l'elector, i no d'una altra persona que es registra en nom seu.

Si en aquesta primera fase la identificació no compta amb suficients garanties, la resta del procediment –les fases posteriors, inclòs el propi acte d'emissió de vot- no pot considerar-se segur.

Per tant, és en aquesta primera fase, especialment crítica, d'identificació de l'afectat, que cal extremar les precaucions de seguretat.

Atenent a la redacció de l'article 7, sembla que l'accés a la Plataforma es faria a través de la clau de tramitació telemàtica que figura en l'imprès que l'OCE trametria a les persones que ho hagin sol·licitat. L'article no es refereix expressament a la manera com es farà la tramesa d'aquesta clau. Però sembla deduir-se que es podrà fer a través del correu electrònic o el dispositiu mòbil que hagi indicat la persona interessada.

En cas de ser així, seria bo preveure que per accedir a la Plataforma es requerís de manera cumulativa una informació tramesa al correu electrònic (p. ex. un identificador personal) i una altra informació tramesa al telèfon mòbil (la clau d'accés). Així es reduiria els riscos derivats de la possibilitat de sostracció o accés indegut a alguna d'aquestes vies de comunicació.

Cal assegurar que aquests mecanismes (correu electrònic i dispositiu mòbil) estiguin realment sota el control exclusiu de l'afectat mitjançant mecanismes de garantia que permetin optimitzar la seguretat que cadascun d'aquests dos canals ofereixen.

Amb aquest o altres mètodes que enviïn informació separada, diferent i complementària a l'adreça de correu electrònic i al dispositiu mòbil, per poder exercir el vot, s'incrementaria la seguretat en la fase d'identificació i registre de l'afectat, de la qual depèn que les fases posteriors del procediment siguin segures.

Per altra banda l'article 7.4 de l'Avantprojecte estableix que, un cop identificat, l'elector rep les credencials necessàries per exercir el dret de vot "*en la seva adreça de correu electrònic i en el seu dispositiu mòbil*".

En aquest moment serien d'aplicació les mateixes consideracions respecte la necessitat de combinar la informació rebuda en ambdós dispositius.

Tenint en compte l'especial sensibilitat de la informació tractada, l'afectació per drets fonamentals dels afectats, i les característiques de cadascun dels dos canals de

comunicació (comunicació a través del telèfon mòbil i del correu electrònic), en cas que l'Avantprojecte plantegi el seu ús com a alternatiu, cal fer avinent que la utilització del dispositiu mòbil ofereix més garanties que el correu electrònic.

El dispositius mòbils, a banda que estan dotats de contrasenyes i altres mecanismes de protecció que permeten a l'usuari controlar-ne l'accés, es troben habitualment en poder de l'usuari, de manera que, davant d'una pèrdua o robatori, l'afectat n'és més conscient i pot detectar fàcilment el risc d'un mal ús per part de tercers. En canvi, una adreça de correu electrònic pot ser més fàcilment accessible per tercers, i el seu ús inadequat per tercers pot ser més indetectable per part de l'afectat.

Per tant, en cas que els dos canals de comunicació es configurin com a alternatius, caldria prioritzar, des de la perspectiva de la seguretat, la utilització d'un dispositiu mòbil de contacte.

2.- Fase d'emissió de vot

En relació amb l'exercici del dret a vot, l'article 8.2 de l'Avantprojecte disposa que *"el procediment de votació per mitjans electrònics és xifrat en totes les seves fases, des del moment d'accés a la Plataforma de votació electrònica per Internet fins al moment que l'elector confirma el seu vot."* En el mateix sentit, l'article 8.9 preveu la transmissió xifrada dels vots.

Des de la perspectiva de la protecció de dades, d'entrada, cal valorar positivament la previsió de xifratge (article 104 RLOPD).

En qualsevol cas, i atesa la conveniència d'estendre el xifratge al llarg de les diferents fases del procediment, seria recomanable especificar que els vots emesos s'emmagatzemen també xifrats (art. 8.9 de l'Avantprojecte), sens perjudici d'aplicar altres mesures de seguretat en l'emmagatzemament dels vots, qüestió que ja s'apunta en l'article 9 de l'Avantprojecte.

Sens perjudici d'això, l'article 8.5 de l'Avantprojecte disposa el següent:

"L'elector, en el moment d'exercir el dret de vot a través de la Plataforma de votació electrònica per Internet, ha d'adjuntar el fitxer de la imatge d'un dels documents següents: document nacionalitat d'identitat (DNI), passaport expedit per autoritats espanyoles, certificat de nacionalitat espanyola expedit pel consolat d'Espanya en el país de residència, o certificat d'inscripció en el Registre de Matrícula Consular expedit pel consolat d'Espanya en el país de residència.

No serà necessari que l'elector adjunti els fitxers de la imatge dels documents esmentats quan així s'estableixi en els protocols o convenis de col·laboració regulats a la disposició addicional tercera."

Aquesta previsió de tramesa de la imatge de documents (que podria ser a través de l'enviament escanejat del document, tot i que l'Avantprojecte no ho detalla), resulta un mecanisme vulnerable, ja que una simple imatge, sense cap mecanisme de protecció addicional, difícilment està garantint la seva autenticitat, més enllà de que pugui coincidir amb les dades identificatives de la persona que realitza l'accés a la plataforma de votació, que de fet ja ha estat prèviament autenticada. La necessitat d'aquesta tramesa no encaixa en un model de vot electrònic i no aporta cap mena de seguretat addicional, inclús podria arribar a considerar-se una recollida excessiva de dades des de la perspectiva de la normativa de protecció de dades –principi de

qualitat-, ja que incorpora informació (com la fotografia o altres dades de filiació en el cas del DNI), que no sembla necessària en un vot no presencial.

A més, cal tenir en compte que la fotografia d'una persona física esdevé dada biomètrica i per tant especialment protegida, quan s'adreça a la identificació i autenticació d'una persona, com seria el cas que ens ocupa (Considerant 51 i arts. 4.14 i 9.1 RGPD).

En conseqüència, atès que el propi article 8.5 i la disposició addicional tercera de l'Avantprojecte preveuen la possibilitat que no sigui necessari adjuntar *"els fitxers d'imatge",* convindria estudiar alternatives a la necessitat de trametre'ls per Internet.

Respecte el justificant de vot previst (art. 8.7), -a banda de revisar la menció feta a que el dit justificant indicarà que el vot ha estat dipositat a la *"urna electrònica"* en els termes apuntats-*,* cal fer notar que la finalitat del justificant és permetre a l'elector verificar amb posterioritat *"que el seu vot ha estat computat adequadament en la fase d'escrutini".* (En relació amb això, l'article 5.l) de l'Avantprojecte preveu que *"l'elector pot verificar tot el procediment d'emissió del seu vot.")*

Vista la literalitat de l'article 8.7, sembla que l'Avantprojecte preveu que el justificant permeti que l'afectat, *"amb posterioritat"* (sense que es concreti el moment del procés electoral al que es refereix aquesta menció), verifiqui no només que el vot ha estat emès, sinó "computat adequadament", en el sentit que pugui comprovar que el vot s'ha comptat com a vot d'una determinada candidatura.

Cal advertir que la previsió de l'article 8.7 de l'Avantprojecte, entesa en aquests termes, comportaria que en el justificant aparegui el sentit del vot (candidatura escollida o vot en blanc), cosa que suposaria un risc evident per al secret del vot, i per a d'altres drets i interessos de l'afectat, com ara el risc de ser coaccionat en base al sentit del seu vot.

La traçabilitat ha de permetre verificar que un elector ha exercit el seu dret de vot pel procediment de votació electrònica, però no pot anar més enllà. La traçabilitat no ha de permetre establir cap vincle entre l'elector i el sentit del seu vot. Per això la verificació del fet que el vot a estat realment computat a la candidatura escollida, s'ha de poder dur a terme a través de la verificació per part dels organismes de supervisió independents que es determini del codi de programació emprat, tant amb una anàlisi prèvia com a posteriori.

Per tot això, no es pot considerar adequada, des de la perspectiva de la protecció de dades i de la resta de drets dels afectats, una traçabilitat en els termes de l'article 8.7 de l'Avantprojecte. Caldria substituir l'expressió de l'article 8.7 de l'Avantprojecte: *"(...) verificar que el seu vot ha estat computat adequadament en la fase d'escrutini."* per la de: *"(...) verificar que l'emissió del seu vot ha estat computada adequadament en la fase d'escrutini.",* o una expressió similar que, en qualsevol cas, clarifiqui l'abast de la traçabilitat.

En definitiva, cal aclarir el contingut del justificant, la informació que conté, i la significació i abast de la capacitat de l'elector de controlar que el vot s'ha computat adequadament en la fase d'escrutini.

3.- Fase d'escrutini, custòdia i destrucció de la informació

En la fase d'escrutini, a banda de les referències ja fetes, fem notar que l'article 10.4 disposa que, en detectar-se una duplicitat de vots, preval el vot emès mitjançant papereta i *"resta sense efecte el vot emès per mitjans electrònics."* Vinculant aquesta previsió amb la traçabilitat del procediment per part de l'elector arran del corresponent justificant (art. 8.7 Avantprojecte), convindria aclarir si l'elector ha de rebre alguna informació o comunicació respecte el fet que s'hagi deixat sense efecte el vot (o constatat la duplicitat), si escau, en els termes de la legislació general de procediment electoral.

L'article 9 de l'Avantprojecte fa referència a que es prendran les "*mesures tècniques necessàries"* per a la correcta custòdia dels vots emesos. D'entrada, cal valorar positivament aquesta previsió. No obstant això, cal fer notar que un model integral de seguretat, en què es determini quines mesures de seguretat cal aplicar a partir d'una anàlisi de riscos en els termes del RGPD (Considerants 83 i 84), no només exigirà la implantació de mesures tècniques, sinó també organitzatives, de formació del personal que ha de tractar les dades, etc. Per això, la menció de l'article 9 de l'Avantprojecte, només, a "mesures tècniques", podria substituir-se per una més general, referida a les *"mesures de seguretat necessàries".*

Pel que fa a la destrucció de la informació, l'article 14.2 de l'Avantprojecte preveu que l'òrgan competent *"garanteix la destrucció de la informació personal de l'elector un cop finalitzat el procediment en què s'han emprat mitjans electrònics de votació."*

Per tal d'assegurar que el tractament de la informació personal es duu a terme en termes adequats a la normativa de protecció de dades, i per tal de dotar de major seguretat jurídica els electors, convindria clarificar o concretar, en la mesura del possible, en quin moment es considera finalitzat el procediment, als efectes de cancel·lar, suprimir o destruir la informació personal.

4.- Fase de control i de verificació.

El principi de l'article 5.m) de l'Avantprojecte, fa referència a l'auditabilitat del procediment objecte de regulació, i precisa que *"El procediment de votació electrònica és auditable mitjançant eines estàndard amb la finalitat de comprovar que tot el procés de votació és correcte. L'Administració pública, els partits polítics i la ciutadania poden comprovar l'objectivitat del sistema i la fiabilitat dels resultats."*

Tenint en compte els principis de transparència i d'auditabilitat consagrats en l'article 5, apartats i) i m) de l'Avantprojecte, podria preveure's la inclusió de les aplicacions, plataformes i sistemes involucrats en el procediment de votació electrònica, com a elements susceptibles d'auditoria (art. 13 Avantprojecte), incloent el codi utilitzat en el programari. Sobre aquestes qüestions, ens remetem a les consideracions fetes en el Dictamen 3/2010.

L'article 13.2 disposa que *"Una entitat pública o privada, externa i independent, prestadora de serveis d'auditoria i certificació de vot electrònic, designada per l'Administració convocant del procediment on s'hagi d'implementar el vot electrònic, ha de certificar, amb caràcter previ que la Plataforma de votació compleix amb els principis (...)."* El fet que aquesta auditoria es faci amb caràcter previ, dóna a entendre que no es durà a terme en totes les fases del procediment, al menys per part d'aquesta entitat, com hem vist que disposa l'article 5.m) de l'Avantprojecte, sinó només de forma prèvia.

Si ens atenim al que disposa l'article 13.3 de l'Avantprojecte, qui podrà "*auditar*" les diferents fases del procediment ja no serà aquesta entitat de l'article 13.2, sinó la Junta Electoral competent, *"amb l'assessorament i el suport continu dels òrgans, ens o entitats de l'Administració de la Generalitat de Catalunya competents en matèria d'administració electrònica, TIC i ciberseguretat".*

Sigui com sigui, en relació amb l'auditabilitat del procediment, fem avinent que convindria fer referencia a que el sistema generarà informació que permeti la traçabilitat de tot el que s'ha fet amb la informació relacionada amb el procediment electrònic (requisit per garantir l'auditabilitat), tant des de la perspectiva funcional com de l'accés per part de perfils tècnics. És a dir, caldria preveure la implantació de mecanismes de registre de l'accés i activitat del conjunt del sistema, en base a deixar traça de l'activitat de cadascun dels subsistemes en que estigui composat, òbviament prèvia identificació i acreditació de tothom que hagi d'accedir al sistema en raó de les diferents funcions que preveu que es realitzin en el conjunt del procediment de vot electrònic. Aquesta informació d'activitat del sistema ha de ser el més granular possible, a fi de facilitar l'auditoria efectiva del sistema.

VIII

Finalment fem avinent el següent, respecte la informació als electors afectats.

En línia amb les consideracions del FJ V del Dictamen 3/2010, caldria considerar la conveniència d'explicar als ciutadans el sistema de votació, el procediment, les mesures de seguretat aplicades i les altres garanties establertes. Cal tenir en compte que la transparència del sistema, entesa com informació als ciutadans sobre les seves característiques i funcionament en especial sobre el tractament de les seves dades personals i la seva traçabilitat, resulta un requisit essencial, segons es desprèn de la normativa aplicable (art. 43 EAC, i art. 50 LOREG), segons les Recomanacions del Consell d'Europa, i segons el propi Avantprojecte (art. 5.i) Avantprojecte).

Això vindria exigit no només pel que acabem d'exposar sinó també des del punt de vista de la normativa de protecció de dades. Així es desprèn dels raonaments del Tribunal Constitucional en relació amb l'article 5 de la LOPD que regula el dret de informació de les persones respecte del tractament de les seves dades personals: "*sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (art. 5 LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales, pues es claro que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental al que estamos haciendo referencia*.". El dret a ser informat del destí i del tractament que es donarà a les dades de caràcter personal forma part del nucli essencial del dret fonamental a la protecció de dades i adquireix encara més importància quan es tracta de dades especialment protegides com són les referents a l'opció política. Per això, tot i que en matèria electoral no resulti aplicable l'article 5 LOPD, resultarà igualment exigible assegurar pels mitjans adequats que el ciutadà té coneixement de com seran tractades les seves dades.

Barcelona, 20 de setembre de 2016