Informe en relació amb el Projecte de decret d'establiment del sistema de vot electrònic en els processos d'eleccions a òrgans de representació del personal d'administració i tècnic al servei de l'Administració de la Generalitat de Catalunya

Es presenta a l'Autoritat Catalana de Protecció de Dades el Projecte de decret d'establiment del sistema de vot electrònic en els processos d'eleccions a òrgans de representació del personal d'administració i tècnic al servei de l'Administració de la Generalitat de Catalunya, per tal que l'Autoritat emeti el seu parer al respecte.

El Projecte de decret consta d'un preàmbul, sis articles i dues disposicions addicionals. S'acompanya de la Memòria justificativa.

Examinat aquest Projecte de decret i la documentació que l'acompanya, i vist l'informe de l'Assessoria Jurídica, s'informa el següent.

Antecedents

L'article 44 del Text refós de l'Estatut bàsic de l'empleat públic, aprovat mitjançant el Reial decret legislatiu 5/2015, de 30 d'octubre, disposa que el procediment per a l'elecció de les Juntes de Personal i per a l'elecció dels Delegats de Personal es determinarà reglamentàriament, tenint en compte, entre d'altres criteris generals, que l'elecció s'ha de fer mitjançant sufragi personal, directe, lliure i secret que es pot emetre per correu o per altres mitjans telemàtics (apartat 1.a)).

Actualment, els processos electorals a òrgans de representació del personal al servei de l'Administració de la Generalitat de Catalunya són objecte de regulació a la Llei 9/1987, de 12 de juny, d'òrgans de representació, determinació de les condicions de treball i participació del personal al servei de les administracions públiques i, de manera supletòria, és aplicable el Reial decret 1846/1994, de 9 de setembre, pel qual s'aprova el Reglament de les eleccions a òrgans de representació del personal al servei de l'Administració General de l'Estat.

L'article 21 de la Llei 9/1987 disposa que l'administració pública corresponent facilitarà el cens de funcionaris i els mitjans personals i materials per a la celebració de les eleccions.

El Decret té per objecte exclusivament implantar el sistema de votació electrònica en aquests processos electorals, amb la finalitat de fomentar la participació i l'exercici del dret de sufragi als electors, eliminar significativament els costos en mitjans personals i materials, proporcionar l'accessibilitat evitant desplaçaments, facilitar l'exercici del dret a les persones discapacitades o amb mobilitat reduïda, prevenir els errors en el procés de votació i assegurar la rapidesa i la precisió en els escrutinis.

Fonaments jurídics

I

(...)

II

El Projecte de decret que s'examina té per objecte *"l'establiment del sistema de votació electrònica per a les eleccions a òrgans de representació del personal d'administració i tècnic al servei de l'Administració de la Generalitat de Catalunya*" (article 1).

Tal com ha posat de manifest aquesta Autoritat en ocasions anteriors, des de la perspectiva de la protecció de dades personals, en qualsevol procés electoral que se celebri emprant mecanismes de votació electrònica adquireix especial importància una adequada gestió de la informació tractada. De fet, d'això en depèn que la participació sigui real i efectiva. Només si les condicions en què es desenvolupa el procés electoral garanteixen la correcta identificació de les persones que hi participen, la confidencialitat de la seva informació –i, en especial, del seu vot- i la seguretat de tota la informació que hi està relacionada, queda garantida la llibertat de participar-hi i la fiabilitat del resultat.

En aquest sentit, cal fer especialment menció al Dictamen 3/2010 (disponible al web http://apdcat.gencat.cat/), en què 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 el Projecte de decret que s'examina. Assenyalar que tot allò que, amb caràcter general, es va posar de manifest en aquell dictamen, segueix sent vàlid, en especial, els apartats relatius als riscos dels diferents sistemes de votació electrònica.

Dit això, fer avinent la conveniència de valorar en el present cas la realització de l'avaluació d'impacte en la protecció de dades a què es refereix l'article 35 del Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (en endavant, RGPD).

L'RGPD requereix fer una avaluació d'impacte sobre la privacitat *"cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas"* (article 35.1).

En relació amb aquesta avaluació d'impacte, la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (en endavant, LOPDGDD), enumera, en llur article 28.2, alguns supòsits en què s'entén probable l'existència d'un alt risc per als drets i llibertats de les persones, tals com *"cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, (…)"* (lletra a)), *"cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales"* (lletra b)), o *"cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (...)"* (lletra c)), entre d'altres.

Cal tenir en consideració que, en el present cas, el Projecte suposa el tractament d'informació personal que, si bé estrictament no revelaria l'afiliació sindical dels afectats, sí pot comportar la revelació de llur ideologia. Per tant, suposaria el tractament de dades mereixedores d'especial protecció (article 9.1 RGPD).

Tenint en compte la naturalesa de les dades tractades, que el seu tractament pot afectar altres drets com ara l'exercici del dret de sufragi, que pèrdues d'aquesta informació o tractaments inadequats de la informació vinculada al procés electoral podrien no només afectar el resultat del mateix sinó donar lloc a situacions discriminatòries o de coacció per als afectats, i que el

tractament podria afectar un nombre ampli de persones, caldria dur a terme aquesta avaluació d'impacte.

L'article 35.10 de l'RGPD estableix que si en el procediment d'aprovació de la norma se sotmet el Projecte a una avaluació d'impacte sobre la privacitat després no serà necessari realitzar-la quan es duguin a terme els tractaments que se'n derivin.

Ara bé, fer avinent que, en el present cas, la dita avaluació d'impacte hauria de comprendre l'avaluació no només de les previsions normatives sobre el sistema de votació electrònica establertes en el Projecte sinó especialment l'avaluació de la concreta solució tecnològica escollida per dur a terme tal votació. És a dir, amb caràcter previ a l'adopció d'un sistema de votació electrònica, caldria dur a terme una avaluació de l'afectació que pot tenir el dit sistema per a la privacitat de les persones afectades i una anàlisi de les diferents alternatives disponibles per assolir la finalitat perseguida, de manera que es pugui optar per aquella que ofereixi més garanties per als drets de les persones.

Dit això, convé assenyalar que, per tal d'efectuar un examen acurat de les implicacions que, per a la protecció de dades dels afectats, poden derivar-se de la implementació d'un sistema de votació electrònica en el procés d'elecció a què fa esment el Projecte, hagués estat convenient haver disposat de la dita avaluació d'impacte en el moment d'emetre el present informe.

Finalment, cal advertir que el Projecte contempla, principalment, aspectes i característiques pròpies dels sistemes de votació electrònica existents però no descriu pròpiament l'opció tecnològica escollida, per la qual cosa l'examen se centrarà únicament en aquests aspectes generals.

III

Fetes aquestes consideracions inicials, ens referim a continuació al model de procediment de votació electrònica que configura el Projecte.

D'acord amb l'article 2.2 del Projecte, el sistema de votació electrònica consisteix *"en l'emissió del vot en suport electrònic de forma remota a través d'un dispositiu connectat a Internet (...)".* Pel que s'infereix de l'article 6 del Projecte, l'elector pot exercir el dret de vot mitjançant una *"Plataforma de votació electrònica per Internet".*

D'aquestes previsions i d'altres contemplades en la Memòria justificativa que l'acompanya (apartats III a V) sembla desprendre's que el procediment de votació es configura com un sistema de vot electrònic remot, que l'elector podrà exercir a través d'aquesta "Plataforma", a què podrà accedir a través d'Internet, per tant, a través dels seus propis dispositius (per exemple, un ordinador) i no de terminals facilitats i controlats per l'autoritat corresponent en un espai determinat.

Ara bé, el Projecte també conté diverses referències expresses a la *"urna digital"* i a la *"urna electrònica"*, que seria un element propi dels sistemes presencials de vot electrònic.

Així, el mateix article 2.2 del Projecte disposa que el vot *"és emmagatzemat en una urna digital protegida criptogràficament"*. L'article 3.i) del Projecte explicita que l'elector, un cop emès el vot, pot descarregar-se un justificant del sistema *"que deixi constància de l'efectiva emissió del vot i del seu dipòsit a l'urna electrònica (...)".* I l'article 5.1 del Projecte, en relació amb les funcions atribuïdes a les Meses coordinadores, preveu que aquestes supervisin *"el procés de creació de la urna digital"* (lletra a)), així com que s'encarreguin de *"la custòdia de les claus*

criptogràfiques d'accés a la urna digital que permeten l'escrutini dissociat de vots electrònics" (lletra b)).

Com ha fet avinent aquesta Autoritat en el Dictamen 3/2010, abans citat, els sistemes presencials i els sistemes de vot remot són dos models de sistemes de votació electrònica clarament diferenciats (FJ IV), que, des de la perspectiva de la protecció de dades i del model de seguretat, 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 (FJ VI i VII).

Per aquest motiu, si, com sembla, el Projecte configura un procediment de votació electrònica per Internet com a sistema de vot remot, convindria revisar les referències fetes a la urna electrònica o digital i substituir-les, si escau, per les que corresponguin, als efectes de clarificar el model configurat pel Projecte.

IV

Des de la perspectiva de la protecció de dades, resulta especialment rellevant l'article 3 del Projecte, que enumera les garanties del sistema de votació electrònica.

Aquestes garanties fan referència expressa, entre d'altres qüestions, a la identificació i l'autenticació de l'elector; al caràcter secret del vot i a la seva integritat i unicitat; a la seguretat del procediment de votació electrònica; o a la possibilitat de verificar el seu correcte funcionament, així com d'auditar-lo.

D'entrada, cal valorar positivament aquestes previsions en què es fonamenta el Projecte des de la perspectiva de 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 s'examina, tal com exigeix el propi RGPD, que estableix la protecció de dades des del disseny i per defecte (considerant 78 i article 25).

Prenent com a punt de partida aquestes garanties, atès que el Projecte no descriu pròpiament el procediment de votació electrònica, es considera pertinent assenyalar:

- La importància d'implementar mecanismes i procediments prou segurs a l'hora d'identificar les persones amb dret a vot i de proporcionar-los la credencial que els ha de permetre votar per Internet, als efectes d'evitar la votació de persones sense dret a fer-ho, la suplantació de les persones que sí hi tenen dret, així com la duplicitat de vots. És a dir, d'establir mecanismes que garanteixin la correcta identificació i autenticació dels votants.

Sobre això, l'article 3 del Projecte disposa que es garanteix, per una banda, la identificació de l'elector *"mitjançant els procediments d'identificació del directori corporatiu"* (lletra c)), i, per l'altra, la seva autenticació robusta, emprant "*l'aprovisionament segur de credencials de directori corporatiu"* (lletra g)).

En la Memòria justificativa que l'acompanya s'explicita, al respecte, que *"cada votant censat disposa d'un certificat/codi d'accés a l'aplicació on es realitza la selecció personalitzada d'opcions i candidats"* (apartat III).

D'aquestes previsions sembla desprendre's que el sistema únicament permetrà l'accés a la plataforma de votació a aquelles persones prèviament donades d'alta al directori corporatiu de la Generalitat, aspecte que cal valorar positivament. Ara bé, pel que fa al procés d'autenticació dels electors, no queda suficientment clar si aquesta es durà a terme mitjançant sistemes

basats en certificats electrònics o bé a través de mecanismes basats en l'atribució d'un usuari i contrasenya.

En un cas com l'examinat, si bé la identificació i autenticació de les persones amb dret a participar en el procés electoral no plantejaria majors problemes, des del punt de vista de la protecció de dades, si es dugués a terme mitjançant sistemes basats en certificats electrònics o segells electrònics, atès que aquests mecanismes ofereixen suficients garanties, tampoc es pot descartar la utilització de mecanismes basats en l'atribució d'un usuari i contrasenya.

Aquest tipus de mecanismes és el mètode més estès per impedir accessos no autoritzats vers sistemes o continguts dins un sistema d'informació. Es tracta d'una mesura establerta en estàndards internacionals i en certificacions en matèria de seguretat informàtica (com ara, la Norma ISO/IEC 27001 sobre la gestió de la seguretat de la informació) i també reconeguda pel nostre ordenament jurídic (per exemple, a la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques (article 9)).

Apuntar que, en cas que s'optés per aquest mecanisme d'identificació i d'autenticació dels electors, caldria vetllar per establir un procediment de gestió de les contrasenyes que garanteixi la confidencialitat i la integritat de les mateixes.

- La importància d'adoptar les mesures adients per garantir que el vot que emet la persona que participa en el procés electoral és únic, secret i anònim.

Sobre això, l'article 3 del Projecte disposa expressament que el sistema *"no permet establir un vincle entre el sentit del vot i la persona que l'ha emès"* (lletra b)), garanteix així mateix que *"la voluntat expressada per l'elector és autèntica, inequívoca i que no ha estat alterada ni qualitativament ni quantitativament"* (lletra d)) i que *"l'elector pot emetre un sol vot i s'elimina tota possibilitat de duplicitat o multiplicitat de vot per part d'una mateixa persona"* (lletra e)).

També preveu que es garanteix *"la seguretat tècnica dels procediments de transmissió i emmagatzematge de la informació, amb mesures que garanteixin la traçabilitat i mesures contra addicions, sostraccions, manipulacions, suplantacions o tergiversacions del procediment de vot"* (article 3.f)).

I, alhora, que es garanteix *"el compliment de la normativa de protecció de dades personals, aplicant les mesures de seguretat de nivell alt en atenció a la naturalesa de les dades"* (article 3.k)).

Per la seva part, en la Memòria justificativa s'explicita (apartat III), al respecte, que *"els vots són xifrats en els dispositius de votació i només la Mesa electoral única pot reconstruir la clau privada i desxifrar els vots. El procés garanteix que es trenqui la correlació entre la identitat dels votants i els vots desxifrats (...). (...) els vots que s'emmagatzemen en els servidors estan protegits criptogràficament -xifrats i signats digitalment- en tot moment, per tant, ningú pot manipular-los, ni tan sols els administradors dels sistemes amb accessos privilegiats -no tenen accés a la clau privada-. (...) També es garanteix el vot lliure -evitant la coerció o venda de vots- amb el rebut de vot que és un codi alfanumèric que no revela l'opció del vot, és a dir, cap votant pot acreditar davant tercers quin és el sentit del seu vot. (...)".*

Des de la perspectiva de la protecció de dades, cal valorar positivament la previsió d'implementar aquest conjunt de mesures de seguretat que abastarien les diferents fases del procés de votació electrònica.

Tot i així, cal advertir, pel que fa específicament a l'adopció de *"mesures que garanteixin la traçabilitat"* (article 3.f)), que aquestes únicament i exclusivament han de permetre verificar que

un determinat elector ha exercit el seu dret de vot pel procediment de votació electrònica. És a dir, en cap cas han de permetre establir un vincle entre la identitat de l'elector i el sentit del seu vot.

Si bé, cal dir, el Projecte preveu que el sistema no permet establir tal vincle (article 3.b)), la manca de concreció sobre l'abast de la traçabilitat en el present cas fa necessari advertir d'aquest eventual risc 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.

Dit això, fer avinent, en aquest punt, que l'RGPD configura un sistema de seguretat que no es basa en els nivells de seguretat bàsic, mitjà i alt que es preveien al Reglament de desplegament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, aprovat pel Reial decret 1720/2007, de 21 de desembre, sinó en determinar, arran d'una prèvia valoració dels riscos, quines mesures de seguretat són necessàries en cada cas (considerant 83 i article 32).

Per aquest motiu, convindria modificar la redacció donada a la lletra *k)* de l'article 3 del Projecte, en què es preveu l'aplicació de *"mesures de seguretat de nivell alt"*, als efectes d'emprar una terminologia adaptada a l'RGPD.

En aquest sentit, se suggereix una redacció similar a la següent:

"k) Compliment de la normativa en matèria de protecció de dades personals, aplicant les mesures tècniques i organitzatives que resultin necessàries, 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."

Fer també avinent que, en el cas de les administracions públiques, l'aplicació de les mesures de seguretat estarà marcada pels criteris establerts a l'Esquema Nacional de Seguretat, aprovat pel Reial Decret 3/2010, de 8 de gener, que, actualment, està sent objecte de revisió.

En aquest sentit, l'LOPDGDD, abans citada, disposa que:

> *"Disposición adicional primera. Medidas de seguridad en el ámbito del sector público.*
>
> *1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos de carácter personal, para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.*
> *2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.*
> *En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad."*

Assenyalar que, entre els responsables del tractament inclosos a l'article 77.1 de l'LOPDGDD, a què expressament fa referència aquesta DA1a, hi trobem les administracions de les comunitats autònomes, així com llurs organismes públics i entitats de dret públic, entre d'altres.

Per tant, cal tenir present que, en el present cas, en què el Projecte preveu el tractament de dades del personal d'administració i tècnic al servei de l'Administració de la Generalitat de Catalunya, l'aplicació de les mesures de seguretat establertes a l'Esquema Nacional de Seguretat resultarà obligatòria.

V

Encara en relació amb aquest article 3 del Projecte, convé també fer avinent que aquest precepte no concreta les condicions en què s'emmagatzemaran les dades personals vinculades al procediment de votació electrònica, més enllà d'indicar l'adopció de mesures de seguretat *"tècniques"* al respecte (lletra f)), que, pel es desprèn de la Memòria justificativa, consisteixen en protegir criptogràficament els servidors. Es desconeix però si es tracta de servidors propis o de tercers, així com la seva ubicació.

Per aquest motiu, es fa avinent la necessitat de valorar l'existència d'un possible encàrrec del tractament (article 4.8) RGPD), per exemple, en cas de contractar amb un tercer la prestació de serveis d'allotjament o emmagatzematge de la informació relacionada amb el procediment de votació electrònica, inclosos serveis que operen en el núvol. D'ésser així, s'hauria de formalitzar un contracte d'encàrrec del tractament en els termes establerts a l'article 28.3 de l'RGPD.

També caldria valorar l'existència de possibles transferències internacionals de dades (en endavant, TID), per exemple, en cas que les dades s'emmagatzemin en servidors ubicats fora de l'àmbit territorial d'aplicació de l'RGPD (article 3). D'ésser així, caldria tenir en consideració que les TID es trobarien sotmeses al règim previst en els articles 44 a 50 de l'RGPD.

Apuntar, al respecte, que l'RGPD preveu que la Comissió de la UE pot decidir que un tercer país, un territori o un o varis sectors específics d'un país, garanteix un nivell de protecció adequat (article 45), per la qual cosa no hi hauria inconvenients en poder realitzar la TID, sempre que es compleixin també la resta de principis i obligacions de l'RGPD i de l'LOPDGDD.

A manca d'aquesta decisió de la Comissió, només es podria transmetre dades personals a un tercer país si s'ofereixen garanties adequades i els interessats disposen de drets exigibles i d'accions legals efectives (l'RGPD estableix, en aquest sentit, diferents mecanismes per considerar que s'ofereixen garanties adequades, tals com normes corporatives vinculants, clàusules tipus, mecanismes de certificació, etc. (article 46.2 RGPD)) o bé si concorre alguna de les excepcions previstes a l'article 49 de l'RGPD.

Per a més informació sobre aquesta qüestió en concret, pot ser d'interès consultar els dictàmens CNS 5/2018 o CNS 6/2018, disponibles al web de l'Autoritat (http://apdcat.gencat.cat/).

VI

L'article 5 del Projecte estableix, en el seu apartat 1, les funcions que, en relació amb el sistema de votació electrònica, correspondran a les meses coordinadores, que inclouen actuacions com la supervisió del procés de creació de la urna digital (lletra a)), la custòdia de les claus criptogràfiques d'accés a la urna digital (lletra b)) o la resolució de les incidències tecnològiques (lletra c)).

Alhora, preveu que les meses coordinadores comptaran amb el suport d'un equip d'experts, als efectes d'obtenir l'assessorament tècnic que requereixin (apartat 2).

Sens perjudici de valorar positivament aquesta previsió, cal tenir present la necessitat de garantir que el personal que conformi les dites meses coordinadores (article 10 Reial decret 1846/1994) disposarà dels coneixements tècnics suficients per poder desenvolupar correctament les funcions que tenen assignades. Cal recordar 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 de l'RGPD (considerants 83 i 84), exigeix també l'adopció de les mesures organitzatives necessàries i la implantació de mesures de formació del personal que ha de tractar les dades personals.

VII

L'article 6 del Projecte disposa que *"l'Administració de la Generalitat de Catalunya, a través dels òrgans, ens o entitats que tenen atribuïdes les competències en matèria d'administració electrònica, TIC i ciberseguretat, dóna assessorament i suport continu en aquestes matèries per tal de garantir la seguretat i el correcte funcionament de la Plataforma de votació electrònica per Internet en totes les fases del procediment de votació electrònica".*

Fer avinent, al respecte, la necessitat de definir les condicions en què participaran aquests tercers en el procediment de votació electrònica i les conseqüències d'aquesta participació des del punt de vista de la protecció de dades.

Així, cal tenir present que, en la mesura que la prestació d'aquests serveis d'assessorament i suport comporti el tractament de dades personals per compte del responsable del procés electoral, s'haurà de formalitzar un contracte d'encàrrec del tractament en els termes establerts a l'article 28.3 de l'RGPD.

VIII

Finalment, valorar positivament la previsió d'informar als electors del sistema de votació electrònica, del procediment d'ús i de les mesures de seguretat aplicables mitjançant la web oficial del procés electoral (disposició addicional segona).

Fer avinent, al respecte, que aquesta informació també haurà de comprendre el conjunt d'aspectes a què fa esment l'article 13 de l'RGPD i que haurà de proporcionar-se de forma concisa, transparent, intel·ligible i de fàcil accés, en un llenguatge clar i senzill (article 12 RGPD).

Per tot això es fan les següents,

Conclusions

Examinat el Projecte de decret d'establiment del sistema de vot electrònic en els processos d'eleccions a òrgans de representació del personal d'administració i tècnic al servei de l'Administració de la Generalitat de Catalunya, es considera adequat a les previsions establertes a la corresponent normativa sobre protecció de dades de caràcter personal, sempre que es tinguin en compte les consideracions fetes en aquest informe.

Barcelona, 16 de gener de 2019