CNS 3/2010

Dictamen en relació amb la consulta formulada sobre els sistemes de vot electrònic

Es sol·licita a l'Agència Catalana de Protecció de Dades un dictamen sobre vot electrònic , especialment sobre la seguretat i el manteniment del secret de vot, sobre la viabilitat, avantatges, inconvenients i garanties, especialment respecte a la seguretat i el secret, que podria comportar incorporar el vot electrònic, vot remot per internet i urna electrònica.

El present dictamen s'emet doncs des del punt de vista de la protecció de les dades de caràcter personal i no s'estén a totes les implicacions que per a la protecció de dades pot tenir la celebració d'un procés electoral, sinó, simplement, en relació amb el vot electrònic en qualsevol de les seves modalitats.

Analitzada la consulta, i vist l'informe de l'Assessoria Jurídica s'emet el dictamen següent:

I

(...)

II

El primer que cal abordar en el present dictamen és 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 amb ocasió de la incorporació de mecanismes de vot electrònic.

D'acord amb l'article 2.3.a) de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (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 la 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 continguda a 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 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 la 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 com a nivell estatutari, com també en la normativa

electoral general que requereixen que una eventual llei que incorpori el sistema de vot electrònic hagi de preveure les garanties necessàries per a la protecció d'aquest dret. D'altra banda a nivell internacional trobem també un tractat internacional, la Convenció 108 per a la protecció de les persones pel que fa al tractament automatitzat de dades de caràcter personal, feta a Estrasburg el 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.

A nivell constitucional, cal tenir en compte l'article 18.4 CE, el qual estableix un mandat al legislador per tal que limiti l'ús de la informàtica per tal de garantir, entre d'altres, el dret a la intimitat de les persones i el ple exercici dels seus drets. En aquest sentit, cal recordar que la jurisprudència constitucional ha declarat però que el dret a la protecció de dades constitueix un dret fonamental de caràcter instrumental, és a dir, es tracta d'un dret que actua com un instrument per a la plena efectivitat d'altres drets fonamentals, com és el cas del dret a la intimitat (art. 18) però també altres com seria el cas del el dret de sufragi reconegut a l'article 23.1 CE i concretat en el 152 pel que fa a les assemblees legislatives autonòmiques.

D'altra banda, cal remarcar que, atesa la naturalesa dels processos electorals, ens trobem davant d'informació que el Conveni 108 (art. 6) – i també la 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 ciutadanes 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.

En qualsevol cas mitjançant el dret a la protecció de dades es tracta, tal com apunta l'art. 18.4 CE i com ha reconegut també el Tribunal Constitucional (STC 292/00), 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. Resulta obvi en aquest sentit que la no-existència de garanties adequades que garanteixin el secret del vot pot actuar com a mecanisme dissuasori 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.

A Catalunya cal destacar a més que l'Estatut d'Autonomia (EAC) ha incorporat per primera vegada a nivell estatutari el dret a la protecció de dades a l'article 31 respecte dels fitxers que són competència de la Generalitat (art. 156 EAC). Previsió que cal completar per una banda amb la de l'article 37.1 EAC segons el qual les disposicions dictades pels poders públics de Catalunya han de respectar els drets reconeguts als capítols I, II i III del Títol I de l'Estatut i que han d'interpretar-se i aplicar-se en el sentit més favorable a la seva plena efectivitat; per altra banda, cal completar-la amb la previsió de l'article 56.1 EAC que exigeix que el sistema electoral al Parlament de Catalunya ha de ser mitjançant sufragi universal, lliure, igual, directe i secret.

Essent com és el cas que ens trobem davant de fitxers que han de ser considerats responsabilitat de l'administració electoral de Catalunya –bé sigui adoptant la forma de la Sindicatura Electoral de Catalunya proposada en l'Informe que s'adjunta a la consulta, o amb una altra forma o denominació- resulta exigible la protecció d'aquest dret per part de la futura llei que reguli el vot electrònic a Catalunya.

D'altra banda, la mateixa legislació electoral general, tot i que no preveu cap sistema de votació electrònica (llevat de la incorporació dels mitjans electrònics per consultar el cens, qüestió a la qual més endavant ens referirem), conté algunes previsions, aplicables a les eleccions a les assemblees legislatives de les Comunitats Autònomes en virtut del que estableix la disposició Addicional Primera de la Llei Orgànica 5/1985, de 19 de juny, del règim electoral general (LOREG), encaminades a la protecció de les dades de caràcter personal i en especial el caràcter secret del vot. En aquest sentit resulten aplicables els principis de transparència, objectivitat i igualtat establerts a l'article 8, com també la prohibició d'obligar o coaccionar per tal que es reveli el sentit del vot (art. 5), la prohibició que es pugui donar fe, per part de notaris presents als col.legis electorals d'actes que s'oposin al secret de la votació (91.3) o el delicte de descobriment del secret de vot (146.1.c).

Finalment, i per tal de completar el marc legal aplicable, cal fer referència també a diferents instruments de caire internacional que reconeixen el caràcter secret del dret a vot, com és el cas de la Declaració Universal dels Drets Humans de 10 de desembre de 1948 (art. 21.3) o el Pacte Internacional de Drets Civils i Polítics de 19 de desembre de 1966 (art. 25.b).

També en l'àmbit internacional cal fer una referència al Codi de bones pràctiques en matèria electoral de la Comissió Europea per la Democràcia i pel Dret (Comissió de Venècia), en el si del Consell d'Europa, com a instrument que recull diferents previsions en ordre a assegurar el caràcter igual, lliure i secret del dret de sufragi.

D'altra banda, cal tenir en compte de manera específica, malgrat estar mancada de caràcter vinculant, la Recomanació (2004) 11 del Consell d'Europa als estats membres, sobre estàndards legals, operacionals i tècnics per al vot electrònic (e-voting), adoptada pel Comitè de Ministres de 30 de setembre de 2004. D'acord amb aquesta Recomanació, es defineix els sistemes electrònics de votació com a tota elecció o referèndum que impliqui el recurs a mitjans electrònics al menys en el moment de registrar el sufragi, i s'estableixen determinats principis a tenir en compte en la regulació a nivell legal en relació, entre d'altres, amb el caràcter secret del sufragi , com també garanties procedimentals:

A) Principis lligats amb el caràcter secret del sufragi (principis 16 a 19):

- El vot electrònic s'organitzarà de manera que es pugui excloure en qualsevol fase del procés de votació i, en particular en l'autenticació de l'elector, tot allò que posi en perill el secret del vot.

- El sistema de vot electrònic ha de garantir que els vots introduïts a l'urna i els vots comptats són, i es mantenen, anònims, i que no és possible reconstruir un vincle entre el vot i el votant.

- El sistema de vot electrònic ha d'estar dissenyat de manera que el nombre de vots esperat en cada urna electrònica no permeti relacionar el resultat amb votants individuals.

- S'ha de prendre les mesures necessàries per tal d'assegurar que la informació necessària durant el procés electrònic no pot ser usada per trencar el secret de vot.

B) Garanties de transparència (apartats 20 a 23):

- Els estats membres prendran mesures per assegurar que els votants entenguin i tinguin confiança en l'ús del sistema de vot electrònic.

- La informació sobre el funcionament d'un sistema de vot electrònic ha de ser públicament disponible.

- Els votants han de tenir oportunitat de practicar qualsevol mètode nou de vot electrònic abans, i separadament, del moment d'emetre un vot electrònic.

- Alguns observadors, amb l'abast previst per la llei, han de poder ser presents per observar i fer comentaris sobre les eleccions amb vot electrònic, incloent-hi l'obtenció dels resultats.

C) Garanties de verificabilitat i responsabilitat del sistema (principis 24 a 27):

- Els components del sistema de vot electrònic es revelaran, com a mínim a les autoritats electorals competents, amb la finalitat de comprovació i certificació.

- Abans que qualsevol sistema de vot electrònic s'introdueixi, i a intervals apropiats després, i en particular després que alguns canvis es facin al sistema, un ens independent, designat per les autoritats electorals, ha de verificar que el sistema de vot electrònic estigui funcionant correctament i que s'hagin adoptat totes les mesures de seguretat necessàries.

- Ha d'haver-hi la possibilitat d'un segon escrutini. Els altres elements del sistema de vot electrònic que puguin influir en la correcció dels resultats han de ser verificables.

- El sistema de vot electrònic no ha d'impedir la repetició parcial o completa d'una elecció o un referèndum.

D) Garanties de fiabilitat i seguretat del sistema (principis 28 a 35):

- Les autoritats de l'estat membre han d' assegurar la fiabilitat i seguretat del sistema de vot electrònic.

- S'han d'adoptar totes les mesures possibles per evitar la possibilitat de frau o intervenció desautoritzada que afectin el sistema durant el procés de votació sencer.

- El sistema de vot electrònic ha de contenir mesures per conservar la disponibilitat dels seus serveis durant el procés de vot. En particular, ha de ser resistent al funcionament defectuós, avaries o atacs de denegació de servei.

- Abans que qualsevol elecció amb vot electrònic, l'autoritat electoral competent ha de comprovar que el sistema de vot electrònic és genuí i opera correctament.

- Només les persones designades per l'autoritat electoral han de tenir accés a la infraestructura central, els servidors i les dades de l'elecció. Hi haurà regles clares establertes sobre això. Les activitats tècniques crítiques seran fetes per equips de com a mínim dues persones. La composició dels equips es canviarà regularment. Tals activitats es faran a fora de períodes d'elecció, al més lluny possible.

- Mentre que una urna electrònica és oberta, qualsevol intervenció autoritzada que afecta el sistema serà feta per equips de com a mínim dues persones, ser objecte d'un informe, ser controlat per representants de l'autoritat electoral competent i observadors de les eleccions.

- El sistema de vot electrònic mantindrà la disponibilitat i integritat dels vots. També mantindrà la confidencialitat dels vots i els mantindrà impermeabilitzats fins al procés de recompte. Si s'emmagatzema o es comunica a fora d'ambients controlats, els vots s'encriptaran.

- Els vots i informació de votants romandran impermeabilitzats mentre les dades estiguin d'una manera en què puguin ser associats. La informació d'autenticació estarà separada de la decisió del votant en una fase predefinida en l'elecció per vot electrònic.

A més, la recomanació preveu també dos apartats dedicats respectivament a les normes operacionals (forma d'utilització i manteniment del software i del material emprat en el vot electrònic) i normes tècniques (referides al desenvolupament i al funcionament del software i material, permetent la seguretat tècnica, l'accessibilitat i la interoperabilitat dels sistemes de vot).

D'altra banda també poden ser d'interès altres documents com ara els Estàndards per als sistemes de vot electrònic, aprovats per la Comissió Electoral Federal dels Estats Units d'Amèrica el 30 d'abril de 2002.

III

En la consulta formulada es demana a aquesta Agència que s'elabori un informe sobre el vot electrònic, sobre la viabilitat, avantatges, inconvenients i garanties, especialment sobre la seguretat i el manteniment del secret del vot.

Pel que fa a la viabilitat del sistema de vot electrònic a les eleccions autonòmiques òbviament aquesta possibilitat està condicionada a la regulació d'aquesta modalitat de vot mitjançant la llei electoral de Catalunya, atès que la LOREG no preveu aquest sistema de votació. Així ho va fer el País Basc, que de fet és l'única Comunitat Autònoma de l'Estat espanyol que preveu mecanismes de vot electrònic en l'elecció de càmeres legislatives, mitjançant la Llei 5/1990, de

15 de juliol, Electoral del País Basc (a partir de la reforma operada per la Llei 15/1998, de 19 de juny) que malgrat portar ja més de 10 anys de vigència encara no ha estat aplicada en cap procés electoral del Parlament Basc, atès que la Disposició Addicional Primera de la Llei 15/98 condiciona l'aplicabilitat de les seves previsions sobre vot electrònic a què el Parlament Basc declarés, a proposta del Govern, l'aplicabilitat del sistema, determinant les circumscripcions electorals, seccions o municipis en què hagi d'aplicar-se, la compatibilitat o no del vot per papereta i, si escau, la progressiva implantació del sistema.

D'altra banda, tot i que s'han dut a terme diferents proves tant a nivell d'eleccions autonòmiques (p. ex. les eleccions al Parlament de Catalunya dels anys 1995 i 2003, o al Parlament de Galícia de l'any 1997), com també en eleccions a nivell estatal (p. ex. les eleccions generals de 2004 o les eleccions europees de 2009) s'ha tractat sempre de proves que, tot i estar autoritzades per la Junta Electoral Central, no tenien valor oficial, sinó que s'ha utilitzat de forma paral.lela al sistema tradicional. En canvi sí que s'han dut a terme experiències en altres països per exemple als Estats Units d'Amèrica, a països sud-americans (Brasil, Veneçuela) o països europeus (Bèlgica o França, en aquest darrer cas només per als residents a l'estranger).

En qualsevol cas, altres països han previst aquests sistemes a les seves legislacions i existeixen nombrosos projectes en marxa sobre aquesta matèria tant en l'àmbit de Catalunya, com l'observatori del vot electrònic (http://www.votobit.org/), de la Unió Europea (www.eucybervote.org) o dels Estats Units (estudi sobre el vot electrònic per internet de la Fundació Nacional de Ciència Nord-americana (www.interpolicy.org)).

Des del punt de vista de la protecció de dades no es plantegen en principi obstacles que permetin concloure la inviabilitat de forma absoluta de l'aplicació de sistemes de vot electrònic, especialment perquè, com veurem, sota aquesta denominació s'hi engloben diferents sistemes de vot amb uns graus d'impacte en la privacitat que poden ser molt diversos. No obstant això resulta evident que l'aplicació de mecanismes de vot electrònic comporta l'aparició de nous riscos que poden acabar afectant alguns dels elements essencials del procés electoral.

En especial poden aparèixer riscos per al caràcter secret del vot, però també respecte del caràcter lliure del dret de sufragi o el caràcter igual. En aquest sentit la manca de garanties adequades pel que fa al secret del vot, pot ser clarament un element dissuasori pel que fa a la participació, amb les conseqüències que això pot tenir en la formació de la voluntat democràtica, atès que acabarà afectant la llibertat d'acudir a votar o d'expressar el vot en un determinat sentit.

D'altra banda, el caràcter d'igual, que també s'ha de predicar del dret de sufragi es pot veure afectat per una manca de garanties que o bé impedeixin la participació de determinats ciutadans, per errades en el sistema electrònic d'identificació, que provoquin duplicitats de vot o permetin suplantacions d'identitat.

La funció que compleix el procediment electoral com instrument de legitimació del poder legislatiu requereix que es revesteixi de totes les garanties que permetin la més àmplia consecució d'aquesta finalitat legitimadora. La incorporació de les tecnologies al procés d'elecció política ha de ser acollida amb cautela i implantada amb les degudes garanties per tal d'evitar que un instrument auxiliar (els mitjans electrònics) introdueixi elements i condicionants

que puguin subvertir l'ordre de valors inherents al dret de sufragi. Per tant, qualsevol que sigui el sistema emprat, el sufragi ha de seguir sent universal, lliure, igual, directe i secret.

És per això que, des del punt de vista de la protecció de la dada relativa a l'opció política de les persones que participen en el procés electoral –dada que ja hem vist que d'acord amb la normativa de protecció de dades mereix la consideració de dada especialment protegida-, tot i no resultar d'aplicació, en sentit estricte, la LOPD cal adoptar les mesures de seguretat escaients per tal d'evitar-ne l'alteració, pèrdua, tractament o accés no autoritzat (art. 9 LOPD). Al respecte, l'article 81 del Reglament de desplegament de la LOPD (RLOPD), aprovat pel Reial Decret 1720/2007, de 21 de desembre, regula l'aplicació dels nivells de seguretat als tractaments de dades de caràcter personal, i concretament l'art. 81.3 a la seva lletra a) preveu que s'apliquin les mesures de seguretat de nivell alt als fitxers o tractaments que revelin dades d'ideologia.

Ara bé l'aplicació d'aquestes mesures pot no ser suficient a la vista dels riscos generats per aquest peculiar procés i la seva importància per a la legitimitat de les pròpies institucions públiques.

Sense entrar en els detalls de les mesures de protecció concretes que caldria aplicar, ja que això dependrà dels sistemes i dispositius de votació electrònica que siguin utilitzats, sí que es pot avançar que caldrà donar resposta efectiva al que es desprèn del contingut al principi de seguretat. És a dir, amb independència de les mesures concretes que seran aplicades, aquestes hauran d'evitar l'alteració, la pèrdua, i el tractament o l'accés no autoritzat de les dades personals relacionades amb el procés de votació electrònica.

En els processos de votació concorren dos conceptes a priori antagònics, que per al cas de processos on intervenen tecnologies la seva sincronització resulta especialment complexa, com ara el fet que d'una banda cada persona que participa emetent el seu vot ha d'estar perfectament identificada, a fi d'evitar suplantacions o duplicitat de vots, i a la vegada s'ha de garantir el secret del vot emès, es a dir, identificació i anonimat han de quedar salvaguardats en el conjunt del procés de votació. Òbviament tot això tenint en compte les necessàries garanties que han d'envoltar el procés d'escrutini final i de lliure emissió del vot.

En definitiva des de l'òptica de la normativa de protecció de dades de caràcter personal caldrà implantar totes les mesures de seguretat previstes al títol VIII del Reglament ja esmentat, tant les de caràcter automatitzat com no automatitzat, ja que com ja s'ha fet referència els sistemes de votació electrònica resultaran complexos i no seran exclusivament automatitzats a totes les fases del cicle de votació electrònica.

Per tal d'analitzar-ho exposarem a continuació els avantatges i desavantatges dels sistemes de votació electrònica, sempre des de la perspectiva de la protecció de dades, tal com es sol.licita en la consulta.

IV

El primer que cal aclarir, per tal d'analitzar els avantatges i desavantatges dels sistemes electrònics de votació és que 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.

D'acord amb això alguns sistemes com ara la possibilitat d'emetre el vot electrònic des d'un lloc llunyà respecte de l'espai on es realitza la votació, però que es realitzi a través de terminals facilitats i controlats per l'autoritat electoral (p. ex. als consolats, o en altres espais habilitats per l'administració electoral) no tindrien, d'acord amb aquesta Recomanació, la consideració de vot remot, tot i que el fet que la informació es transmeti a través de la xarxa incorpora, com veurem, alguns riscos que fan que s'hagi de tractar en determinades qüestions com a un sistema de vot remot. D'altra banda a l'Informe adjuntat a la sol·licitud de dictamen de Agència, es descriuen dos mecanismes de vot electrònic, un de caràcter presencial, mitjançant la utilització d'urnes electròniques, i un altre de caràcter no presencial o a distància, basat en l'ús de xarxes públiques de telecomunicacions. Concretament es fa referència al "vot remot per internet". Per això, malgrat que d'acord amb aquella Recomanació aquest supòsit no tindria la consideració de vot remot, nosaltres ho inclourem en aquesta categoria als efectes de donar resposta a la pregunta plantejada, atès que en qualsevol cas es tracta de sistemes que utilitzen internet en el procés d'emissió del vot.

La distinció és important perquè els riscos generats per a la protecció de dades en uns i altres sistemes presenten profundes diferències que aconsellen tractar-les separadament. Per tant, dedicarem els següents epígrafs a l'anàlisi de cadascun d'aquests sistemes, presencial i remot, distingint dins de cadascun les diverses fases del procés electoral.

V

Abans però d'entrar en l'anàlisi dels avantatges i desavantatges, distingint entre els sistemes de vot electrònic presencial o remot, escau fer algunes consideracions generals que encara que no són referides pròpiament a l'acte de votació i escrutini, sí que formen part del procés electoral i plantegen algunes qüestions d'interès des del punt de vista de la protecció de dades, que pot convenir tenir en compte també amb vistes a una futura llei electoral catalana.

La incorporació dels mitjans electrònics per a la formació del Padró gaudeix ja d'una consolidada experiència en el nostre país des de que la modificació de l'article 17 de la Llei 7/1985, de 2 d'abril reguladora de les bases del règim local, efectuada l'any 1996 per la Llei

4/1996, de 10 de gener, va establir que el padró municipal s'havia de portar pels ajuntaments amb mitjans informàtics, i que es preveiés reglamentàriament la transmissió telemàtica de les dades del padró a l'Oficina del Cens per a l'elaboració del cens electoral.

Però més enllà d'això, des del punt de vista de la protecció de dades resulta rellevant la possibilitat d'incorporar els mitjans electrònics com a sistema de consulta de les llistes electorals. La incorporació, a partir de la Llei Orgànica 1/2003, de 10 de març, per la garantia de la democràcia dels ajuntaments i la seguretat dels regidors, de la possibilitat que la consulta de les llistes pugui fer-se a través de mitjans informàtics, prèvia identificació de l'interessat, llevat que l'Ajuntament no compti amb mitjans informàtics per a fer-ho, ha suposat una mesura que ha de ser valorada positivament des del punt de vista de la protecció de dades, atès que evita accessos indeguts a dades de la resta dels electors, tot i que una plena garantia del dret requeriria que aquest mitjà s'estengués de forma obligatòria a tots els casos, suprimint doncs la possibilitat de l'exposició de les llistes, especialment a partir de l'exigència d'incorporació dels mitjans electrònics prevista a la Llei 11/2007, de 22 de juny, accés electrònic dels ciutadans als serveis públics (LAECSP). Aquesta possibilitat ha estat desplegada pel Reial Decret 1799/2003, de 26 de desembre, i ha estat objecte també de la Instrucció de 20 de gener de 2004, de la Junta Electoral Central. De l'esmentat Reial decret destacar que tot i que preveu els sistemes d'identificació dels votants quan efectuïn la consulta davant l'Ajuntament o oficina consular (DNI, passaport o permís de conduir, i la tarjeta de residència pels estrangers) no recull la forma d'identificació per mitjans electrònics, per la qual cosa caldrà estar al que estableix l'article 13 LAECSP. En qualsevol cas i per tal d'evitar discriminacions derivades de la manca d'accés als mitjans informàtics necessaris per efectuar la consulta, seria necessari no només preveure la possibilitat de fer aquesta consulta per internet, amb les garanties necessàries de identificació, sinó també establir punts d'atenció presencial on es posin a disposició dels ciutadans els mitjans electrònics necessaris per fer aquestes consultes (art. 8.2.a LAECSP).

En segon lloc, una altra qüestió a analitzar en aquest apartat seria el relatiu a l'administració electoral, tant des del punt de vista de la seva composició com de les seves funcions. Respecte aquesta qüestió s'ha de tenir en compte que la regulació de les juntes electorals continguda a la LOREG, d'acord amb la D.A. 1ª de la mateixa llei orgànica, resulta aplicable també als processos electius a les assemblees de les comunitats autònomes. Tal com ha manifestat el Tribunal Constitucional, no es pot alterar "aspectes rellevants que alterin la seva posició institucional" però en canvi "les comunitats autònomes poden regular, respecte les seves pròpies eleccions parlamentàries, aspectes específics de les Juntes actuants en el seu territori" (STC 154/88).

Pel que fa a la composició, s'ha de tenir en compte que tradicionalment han format part de les juntes electorals persones amb un marcat perfil jurídic, o dels àmbits de la sociologia o les ciències polítiques (arts 9.1, 10.1 i 11.1 LOREG) mentre que la incorporació dels mitjans tecnològics requeriria també la incorporació de membres d'aquestes òrgans amb un perfil clarament tecnològic o, com a mínim, la dotació a l'administració electoral de mitjans personals que permetin atendre de forma adequada les noves funcions que en l'àmbit tecnològic els han de correspondre.

Pel que fa a les funcions, l'Estatut de Autonomia de Catalunya, estableix que l'administració electoral és independent i que garanteix la transparència i objectivitat del procés electoral. Coincideix amb això amb la LOREG que a l'article 8 estableix que les Juntes electorals

garanteixen la transparència i l'objectivitat, i també del principi d'igualtat. Però més enllà d'això, en la regulació de les funcions de les Juntes (arts. 19, 20 i altres) no es preveu expressament, per exemple, la intervenció de la junta electoral a l'hora de la supervisió i o control dels sistemes electrònics de votació a diferència del que passa, per exemple amb les paperetes i sobres en la votació manual (art. 70.1). Convindria per tant regular les funcions de l'administració electoral tenint en compte les exigències derivades dels sistemes electrònics de votació.

En qualsevol cas, aquesta verificació o homologació a priori dels sistemes electrònics que es pretenguin utilitzar hauria de permetre una anàlisi completa tant dels equips com del software, incloent-hi la possibilitat d'accedir al codi font i als programes emprats, qüestió aquesta darrera que ha resultat problemàtica en algunes experiències realitzades fins ara atesa la incidència de qüestions relatives a la propietat intel·lectual. En aquest sentit, la Llei brasilera de vot electrònic (Llei núm. 9504, de 30 de setembre de 1997), que després ha estat seguida per altres països de sud-amèrica, a part de preveure aquest control per part de l'administració electoral preveu també la participació de representants acreditats dels partits polítics en aquest control (art. 66). També en aquest sentit, la Recomanació relativa a la seguretat dels sistemes de vot electrònic elaborada per la Comission National d'Informatique et Libertés, autoritat francesa de protecció de dades, recomana tant el caràcter accessible del codi font, com l'establiment de mecanismes per evitar l'alteració o modificació del sistema amb posterioritat al seu control.

En tercer lloc, juntament amb aquestes qüestions relatives a l'administració electoral cal cridar l'atenció sobre els riscos que es poden generar en el procés electoral com a conseqüència de l'encàrrec de determinades funcions a empreses privades per part de l'administració electoral. Ens estem referint, a les empreses que faciliten el maquinari necessari per dur a terme el procés, com també les que desenvolupen les aplicacions informàtiques que seran utilitzades o les que han d'intervenir en les incidències que es produeixin en el dia de la votació. En aquest sentit és freqüent que puguin aparèixer impediments vinculats a la protecció de la propietat intel·lectual que puguin acabar afectant la transparència del sistema, per la qual cosa cal establir les mesures adients que permetin una verificació completa dels mateixos, accedint si escau, al codi font utilitzat. Igualment, tal com estableix la recomanació del Consell d'Europa citada, sobre les intervencions que s'hagin de dur a terme durant el funcionament del mecanisme electoral, cal establir garanties per tal d'assegurar que es duen a terme per part només de personal autoritzat, i que a més es compleixen altres garanties addicionals com la necessitat de canviar periòdicament aquest personal o de la conveniència que intervinguin en equips de més d'una persona. D'altra banda, aquestes operacions de manteniment s'haurien de dur a terme a poder ser fora del temps en què es desenvolupi l'elecció, sempre que sigui possible.

En quart lloc, una altra possibilitat, mentre existeixi el sistema de votació presencial, seria la d'incorporar la possibilitat d'incorporar la sol·licitud de vot per correu a través de mitjans electrònics. En aquest cas caldrà establir les garanties adequades pel que fa a la identificació i autenticació de les persones que ho sol·liciten, com també per assegurar la confidencialitat de les trameses que es realitzin.

Però sense cap mena de dubte l'aspecte sobre el qual cal cridar més l'atenció en aquesta fase preparatòria és la importància de facilitar informació adequada i suficient als futurs votants sobre el sistema de votació electrònic.

Veurem més endavant que l'existència de riscos addicionals creats per la utilització de mitjans electrònics requereix adoptar mesures per tal de preservar els principis que ha de reunir el dret de sufragi, això és, el seu caràcter universal lliure, igual i secret. Això és essencial per a la legitimitat del procés de votació. Ara bé l'adopció d'aquestes mesures no és suficient per a garantir l'assoliment d'aquests principis atès que el desconeixement o la desconfiança dels futurs votats envers els nous sistemes implantats pot acabar afectant aquells trets essencials que ha de complir el procés de votació. Tot i haver adoptat les mesures de seguretat necessàries, cal generar confiança en els ciutadans en la utilització del sistema per tal que el sufragi sigui realment universal, lliure i igual.

En un procés de votació tradicional, la presència humana i el control realitzat directament pel votant en el moment de la introducció el sobre en la urna, com també el control humà realitzat directament en el moment de l'escrutini, no només pels integrants de les meses sinó també pels interventors i apoderats designats pels partits polítics, contribueixen a generar aquesta confiança en els electors de què el seu vot serà secret i que el recompte serà correcte.

Per això resulta essencial una adequada informació als ciutadans. En aquest sentit l'article 43 de l'Estatut d'Autonomia de Catalunya estableix que els poders públics han de procurar que les campanyes institucionals que s'organitzin amb ocasió dels processos electorals tinguin com a finalitat promoure la participació ciutadana i que els electors rebin dels mitjans de comunicació una informació veraç, objectiva, neutral i respectuosa del pluralisme polític. En el mateix sentit es manifesta també l'article 50 de la LOREG en preveure que els poders públics poden dur a terme una campanya institucional dedicada a informar els ciutadans de la data de la votació, el procediment per votar i els requisits i tràmits del vot per correu. Doncs bé, en el cas de la utilització de mitjans tecnològics, la realització d'una companya per explicar els sistemes de votació, el procediment i les mesures de seguretat aplicades i les altres garanties establertes no hauria de se només una opció dels poders públics sinó que hauria de constituir un autèntic mandat. Tal com posa de manifest la Recomanació del Consell d'Europa esmentada, la transparència del sistema, entesa com informació als ciutadans sobre les seves característiques i funcionament, resulta un requisit essencial.

I 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 per exemple 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.

VI

Pel que fa als avantatges de la implantació d'un sistema de vot electrònic presencial, s'acostumen a citar la menor càrrega de treball dels membres de les meses, la rapidesa de l'escrutini i posterior transmissió de les dades, la reducció de la conflictivitat en el recompte, l'ampliació de les formes d'expressió del dret de sufragi (en el supòsit que sigui un sistema opcional), la introducció de les noves tecnologies en aquest àmbit contribuint a l'educació del cos electoral en les noves tecnologies, o fins i tot una reducció del vot nul.

No obstant això, estrictament des del punt de vista de la protecció de dades, això és de la protecció del dret fonamental de les persones a què la informació sobre la seva persona, en aquest cas relacionada amb la seva opció política sigui tractada adequadament, no sembla que plantegi avantatges significatius respecte el sistema tradicional de votació. Potser l'avantatge més rellevant seria les majors garanties de seguretat que ofereixen els mitjans electrònics per a una identificació segura dels votants, però el cert és que fins ara aquesta tampoc havia estat una qüestió especialment conflictiva en el sistema de vot tradicional.

Pel que fa als desavantatges del sistema, és obvi que la incorporació de mitjans electrònics porta aparellats nous problemes com ara els derivats d'errades en el software, o com el risc d'una manipulació indeguda ja sigui de forma intencionada per les entitats que participen en la seva elaboració o manteniment o com a conseqüència de l'actuació de terceres persones. En qualsevol cas però els problemes que es puguin generar dependran de la tecnologia escollida, de manera que previsiblement haurien de ser menors en sistemes que es limitin a la lectura electrònica de la papereta en suport paper que en aquells altres que incorporin altres elements en suport electrònic. Aquests problemes es poden deduir a partir dels riscos generats per la implantació d'aquests nous sistemes de votació. Per analitzar-ho distingirem 4 fases claus en aquest cicle:

- Fase d'identificació i autenticació de la persona amb dret a vot
- Fase d'emissió del vot
- Fase d'escrutini i destrucció de la informació
- Fase de verificació o control del vot emès

1.- Fase d'identificació i autenticació

En aquesta fase s'identifica a la persona amb dret a vot amb la finalitat de proporcionar-li algun tipus de "credencial" per procedir a la votació electrònica, com també la seva posterior autenticació, això és, l'acreditació per mitjans electrònics de la identitat d'una persona. En el cas d'urna electrònica no té per què aparèixer aquest element d'identificació prèvia i assignació de credencial de vot electrònic, ja que el fet de ser presencial permet aplicar els protocols d'identificació que s'apliquen en els sistemes de vot tradicional. De fet en funció del tipus de sistema de vot electrònic presencial de què es tracti, la identificació seguirà realitzant-se amb el que podríem anomenar sistemes tradicionals, atès que la incorporació dels mitjans electrònics es referiria només a l'emissió del vot i el posterior recompte.

Ara bé, la incorporació de mitjans electrònics en aquesta fase en una votació presencial podria comportar que es permeti la identificació per mitjans electrònics a través, per exemple, del DNI

electrònic. Però això no ha d'introduir necessàriament riscos addicionals respecte els procés d'identificació tradicional, llevat que el sistema de votació electrònic es dugui a terme de manera que permetés vincular un determinat vot (el seu sentit) amb una determinada persona. Una mancança d'aquest tipus afectaria el caràcter secret del dret a vot. Però això de fet no seria un problema de la fase de identificació sinó de la fase posterior d'emissió del vot.

En qualsevol cas, en funció de quina sigui la tecnologia emprada, sí que cal posar una especial cura en aquells processos que comportin l'atribució de codis o claus als futurs votants per a poder exercir el seu dret de vot, perquè el caràcter secret no només es pot veure compromès en el moment de l'escrutini sinó en el moment de l'atribució o la comunicació d'aquests codis o claus.

2.- Fase d'emissió del vot

En el cas de votació electrònica basada en "urnes electròniques" s'han de tenir en compte aspectes relacionats amb la protecció dels sistemes que emmagatzemen els vots emesos, de manera que no puguin ser accedits (consulta o alteració), ja no només des de xarxes externes de caràcter públic, si no des de xarxes internes. Les mesures de seguretat han d'evitar que ningú pugui conèixer el contingut del vot d'una persona concreta, ni tampoc mitjançant processos d'explotació de la informació a partir de l'exportació de bases de dades o la còpia d'aquesta informació a altres ubicacions que permetin un accés fora dels canals habituals d'explotació de la informació. En aquest sentit s'han d'extremar les mesures de seguretat no només en relació als usuaris d'aplicacions informàtiques relacionades amb l'explotació de les dades, sinó també les relacionades amb el personal tècnic o administradors de sistemes que puguin tenir relació amb els servidors i infraestructures tècniques de suport al procés de votació electrònica, en definitiva sota cap circumstància ningú diferent a la persona que ha emès el vot pot conèixer el seu contingut. El secret del vot ha d'estar salvaguardat en tot moment.

Al marge d'això,les mesures encaminades a preservar el caràcter secret del dret de vot que ja es venien aplicant en el sistema tradicional, com ara les cabines o espais similars, com també l'adequada orientació de les pantalles –en el cas que s'emprin pantalles tàctils-, poden seguir essent plenament exigibles per als sistemes de votació electrònica presencial.

En qualsevol cas s'ha d'eliminar qualsevol possibilitat de vincular un vot amb una determinada persona directament o indirecta (així per exemple les paperetes electròniques s'han de conservar de forma que no coincideixi amb l'ordre en què han estat emesos els vots).

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

En aquesta fase s'ha de garantir que la informació sobre els vots no és accessible fins que no finalitzi el termini de votació del conjunt del procés electoral, per tant la informació ha d'estar convenientment custodiada fins que els sistemes d'escrutini puguin començar a comptabilitzar els vots rebuts.

En el cas d'urnes electròniques s'ha de custodiar el suport que ha rebut el vot de manera que la informació sobre el sentit del vot no pugui ser accedida (consultada o manipulada) fins al final

de la votació i, a poder ser, amb algun mecanisme que requereixi la participació dels diferents membres de la mesa (p. ex. atribuint a cadascun d'ells una part d'un codi). També s'hauran de preveure mesures per al transport de la informació des d'aquests dispositius fins als sistemes d'escrutini o de consolidació de resultats, tant si el transport es basa en xarxes de telecomunicacions, com en el trasllat físic de dispositius digitals d'emmagatzemament.

Tot i que no tingui un impacte directe en les dades personals com a tals, també convé que a fi de salvaguardar la no-alteració de la informació en els processos d'escrutini, es puguin preveure sistemes que permetin reproduir de diferents maneres el procés d'escrutini (recompte). Aquest control pot servir per detectar possibles errades a nivell les aplicacions informàtiques. Amb aquesta finalitat alguns autors apunten la possibilitat que l'elector obtingui un comprovant del seu vot, que en alguns sistemes s'hauria d'introduir en una urna paral·lela que permetria un recompte manual paral·lel, cas de ser necessari (mètode Mercuri), i en altres en què actuaria com una mena de resguard del vot exercit. De ser així, i per tal d'evitar que l'existència d'aquests comprovants pugui facilitar la utilització de mesures de coacció (permetria al coaccionador verificar l'eficàcia real de la coacció) que acabin afectant la llibertat i el secret del vot, cal que de les mateixes no es pugui deduir el sentit del vot, sense la intervenció de l'autoritat electoral.

Els riscos que apareixen en aquesta fase estan relacionats amb l'emmagatzemament i explotació de la informació, és a dir, s'ha de determinar una vegada tancat oficialment el procés de votació i finalitzat l'escrutini, en quina situació queda la informació fins a l'esgotament dels terminis de recurs contenciosos electorals. S'ha de concretar si ha de quedar bloquejada i de quina manera, i els mecanismes de destrucció segura de la informació, i condicions de recuperació si fos el cas.

Per tant les mesures de seguretat tindran a veure amb el control d'accés i integritat de la informació, i de gestió dels suports on es trobi emmagatzemada, i amb els mecanismes d'esborrat segur de la informació.

4.- Fase de control o verificació

Habitualment els sistemes de votació electrònica incorporen mecanismes que permeten a la persona que va emetre el vot, verificar a posteriori si el seu vot ha estat correctament recollit i comptabilitzat, per descomptat això requereix no només de mecanismes tècnics si no també organitzatius que garanteixin aquesta part del cicle de votació.

A banda del que ja hem assenyalat en la fase anterior, els riscos, deriven de la possibilitat de que amb aquests sistemes de verificació o control a posteriori algú pugui accedir al sentit del vot de persones identificades o identificables, ja sigui per suplantació de credencials o per sostracció de la informació dels servidors que emmagatzemen la informació.

Des de la perspectiva de protecció de dades ens situaríem en el context de l'obligació que té el responsable del tractament de salvaguardar la informació que té emmagatzemada, i els suports que la contenen (sistemes de còpies de seguretat, per exemple) i de garantir que només pot accedir a aquesta informació la persona a la qual correspon el vot emès.

VII

En el cas del vot electrònic remot, pel que fa als avantatges, als que ja s'han exposat en l'epígraf anterior respecte el vot electrònic presencial s'acostuma a afegir que incrementa les possibilitats de participació atès que per una banda facilita el dret de vot d'aquelles persones que no poden o tenen dificultats per accedir als col.legis electorals (p. ex persones residents a l'estranger o persones amb discapacitats o malalties) o aquells col.lectius que per la seva familiaritat amb l'ús de les noves tecnologies, especialment les persones joves, es poden sentir més atrets per aquest canal. D'altra banda, també s'al·lega una reducció de despeses a mig termini, que sembla previsible en el sistema de vot remot (sempre, és clar, depenent de l'estabilitat del sistema i de la possibilitat d'utilització en diferents tipus d'eleccions) i que en canvi no sembla que es pugui predicar en el cas del vot electrònic presencial, o fins i tot arguments vinculats a la sostenibilitat ambiental.

Però al marge de la major o menor exactitud d'aquests suposats avantatges, especialment pel que fa al suposat augment de participació (de fet les experiències pilot que s'han realitzat, amb els condicionants, és clar, de ser proves sense valor vinculant, no sembla que permetin arribar a aquesta conclusió) el cert és que des del punt de vista de la protecció de dades tampoc s'observa cap avantatge significatiu per a la protecció de les dades de caràcter personal, més enllà del que ja hem exposat en l'epígraf anterior respecte l'autenticació dels electors.

Pel que fa als desavantatges, i a banda dels derivats de l'eliminació dels aspectes rituals associats tradicionalment a l'emissió del vot, des del punt de vista de la protecció de dades, a banda de les errades en el software o la manipulació d'aquest, aspectes en els quals es donen per reproduïdes les consideracions formulades respecte els sistemes de vot electrònic presencial, adquireixen especial rellevància els problemes derivats de la utilització de la xarxa d'Internet com a canal de transmissió del vot. Com en el cas anterior els analitzarem a partir de la detecció dels riscos generats en cadascuna de les fases del procés de votació:

1.- Fase d'identificació i autenticació

Aquesta fase és d'especial rellevància quan es tracti d'un sistema de votació "remota" o no presencial. Aquesta fase s'identifica a l'informe d'experts com el registre previ que permet el vot per internet, com també la posterior autenticació del votant.

Els perills que es poden donar en aquesta fase poden aparèixer vinculats a l'articulació de mecanismes i procediments que no siguin 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 o remotament.

Algunes de les conseqüències d'una mala definició d'aquest protocol podrien ser:

- Proporcionar una credencial de vot a algú que no té dret a votar
- Proporcionar una credencial de vot d'una persona a una altra de diferent
- Proporcionar més d'una credencial de vot a una mateixa persona

En aquest sentit, la tramesa de credencials que permetin l'exercici del dret a vot, que en principi haurien de ser anònimes, ha d'assegurar que la persona que realment rep aquella credencial és qui se suposa que és, com també establir-se algun mecanisme complementari que permeti assegurar l'autenticació en el moment de la votació.

Des de la perspectiva de la protecció de dades de caràcter personal, segons quin sigui el sistema que es dissenyi, ens podem trobar davant d'una vulneració del principi de qualitat si, per exemple, pot existir verificació posterior del vot per part del votant amb una credencial compromesa produint-se un accés o tractament no autoritzat.

En aquesta fase també resulta d'especial rellevància la robustesa de la credencial que permet votar electrònicament, de manera que no s'ha de poder reproduir, ni ha de ser coneguda per terceres persones, ja que també ens podríem trobar amb situacions d'accés o tractaments no autoritzats.

Hi ha models de gestió com el de les entitats de certificació, que emeten certificats digitals que permeten tant l'autenticació en sistemes informàtics con la generació de signatures electròniques, que tenen processos de registre orientats a garantir que el certificat digital i les claus criptogràfiques relacionades li son proporcionades a la persona correcta, habitualment utilitzen una estructura de gestió basada en entitats de registre, que realitzen les tasques d'identificació de les persones i de lliurament segur dels certificats digitals i claus.

A Catalunya tenim experiència en aquest model de lliurament de credencials electrònics a partir de les activitats del Consorci Administració Oberta de Catalunya i específicament de l'Agència Catalana de Certificació (Catcert).

En qualsevol cas, pel que fa a l'autenticació, en tot procés que impliqui accés remot a sistemes d'informació o aplicacions informàtiques ha d'existir una verificació de que qui vol accedir a la informació o realitzar una acció és realment qui té dret a fer-ho (control d'accés), per tant en aquest procés d'autentificació 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.

En el cas del vot electrònic mitjançant internet les mesures de seguretat han d'evitar els efectes descrits, garantint en tot moment que qui accedeix a emetre el vot és realment qui té dret a fer-ho, i que no es dona ni suplantació, ni la possibilitat de votar més d'una vegada.

2.- Fase d'emissió del vot

El fet d'utilitzar xarxes públiques de telecomunicacions (internet) o xarxes privades fora del control de l'autoritat electoral afegeix riscos derivats de la possibilitat de que algú capturi la comunicació, ja sigui com a conseqüència de, per exemple, la instal·lació de programari maliciós als ordinadors dels usuaris (típicament els "troians"), l'ús de xarxes de comunicacions privades sense fils no suficientment protegides (típicament l'accés a encaminadors ADSL sense fils) o l'existència de suplantacions de servidor ("phising").

Tal com hem exposat abans respecte els sistemes basats en una urna electrònica, cal vetllar per tal que el vot arribi correctament al seu destí final, i no es produeixin suplantacions. D'altra banda en aquest sistema de votació adquireix encara més rellevància la protecció dels sistemes que emmagatzemen els vots emesos, de manera que no puguin ser accedits (consulta o alteració), en la mesura que s'utilitzen xarxes, públiques o privades, no controlades per l'autoritat electoral.

Igualment, les mesures de seguretat han d'evitar que ningú pugui conèixer el contingut del vot d'una persona concreta, ni tampoc mitjançant processos d'explotació de la informació a partir de l'exportació de bases de dades o la còpia d'aquesta informació a altres ubicacions que permetin un accés fora dels canals habituals d'explotació de la informació. En aquest sentit, com en els sistemes de vot electrònic presencial, s'han d'extremar les mesures de seguretat no només en relació als usuaris d'aplicacions informàtiques relacionades amb l'explotació de les dades, sinó també les relacionades amb el personal tècnic o administradors de sistemes que puguin tenir relació amb els servidors i infraestructures tècniques de suport al procés de votació electrònica.

També el fet d'utilitzar internet com a mecanisme d'accés al sistema de votació implica que els servidors en els quals resideix la informació i el propi procés de votació poden ser objecte de diferents tipus d'atacs, des de la saturació dels servidors mitjançant la generació de tràfic de dades que nomes té per objecte col·lapsar el sistema, el que equivaldria a evitar l'accés al col·legi electoral en els processos de votació presencial (típicament conegut com atacs de denegació de servei, DOS) o atacs de suplantació del servidor (el conegut com a "phising") en els que es simula l'aparença de la pàgina "web" que ha de recollir el vot, de manera que el votant estaria revelant el sentit del seu vot a tercers sense saber-ho i el seu vot es perdria.

D'altra banda tot i que en analitzar els riscos inherents als sistemes de votació remota, en quant a que l'individu vota des d'una ubicació sense les mesures de protecció física que poden existir a un col·legi electoral, certament es poden plantejar riscos relacionats amb la violència o la coacció sobre les persones en el moment de l'emissió del vot o també d'ús fraudulent de credencials electròniques basat en relacions d'abús de poder que cal valorar.

En qualsevol cas però, tant respecte d'aquesta fase com en l'anterior, si bé és innegable que els sistemes de vot electrònic remot presenten considerables riscos, tampoc resulten majors que els que porta associat per exemple el sistema de vot per correu actualment existent.

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

En aquesta fase s'ha de garantir que la informació sobre els vots no és accessible fins que no finalitzi el termini de votació del conjunt del procés electoral. Per tant la informació ha d'estar convenientment custodiada fins que els sistemes d'escrutini puguin començar a comptabilitzar els vots rebuts, un cop tancada la votació.

En els cas del vot electrònic remot també resulten especialment rellevants en aquesta fase els riscos derivats de la utilització de xarxes públiques o privades per a la transmissió del vot, adquirint una especial importància la utilització de mecanismes d'encriptació segura.

D'altra banda, com en el vot mitjançant urna electrònica, també apareixen en aquesta fase riscos relacionats amb l'emmagatzemament i explotació de la informació. És a dir, s'ha de determinar una vegada finalitzat l'escrutini i tancat oficialment el procés de votació en quina situació queda la informació, i s'ha de concretar si ha de quedar bloquejada i de quina manera, els mecanismes de destrucció segura de la informació, i les condicions de recuperació si fos el cas.

Per tant les mesures de seguretat tindran a veure amb el control d'accés i integritat de la informació, i de gestió dels suports on es trobi emmagatzemada, i amb els mecanismes d'esborrat segur de la informació, tot i que pot resultar més difícil la implantació de mesures encaminades a garantir la seguretat de les xarxes utilitzades per a la transmissió, atès que la pròpia dinàmica de funcionament d'Internet impedeix saber a priori quin serà el recorregut que seguirà la informació incorporada al vot electrònic.

4.- Fase de control o verificació

En aquesta fase cal diferenciar per la possibilitat de diversos tipus de controls tots ells amb l'objecte de garantir un adequat funcionament del sistema.

En un sistema de votació tradicional, i també en determinats sistemes de vot presencial, aquest control es duu a terme a través de la mateixa composició de les meses electorals, com també de la presència dels representants dels partits politics (interventors i apoderats) durant la jornada electoral i en el moment de l'escrutini. Però aquests controls no resulten possibles en un sistema remot de votació electrònica. Per això es poden preveure diferents mecanismes de control o verificació.

En primer lloc, cal tenir en compte la possibilitat d'un control institucional a través d'un sistema d'auditories realitzat per alguna entitat independent sota la supervisió de l'administració electoral per tal de determinar si l'aplicació concreta duta a terme del sistema de votació ha estat correcte o no.

En segon lloc caldria regular també la participació de les formacions polítiques en aquest procés d'auditoria.

En tercer lloc, i des de la perspectiva del control individual que pugui fer cada ciutadà respecte el seu propi vot, s'ha de tenir en compte que es tracta d'un control que en el sistema de votació tradicional no existeix, sens perjudici, és clar, del recurs contenciós electoral. Ara bé, la necessitat de transparència i de reforçar la confiança de l'elector en el sistema pot fer convenient l'adopció d'un sistema d'aquest tipus. Aquest control es pot estendre bàsicament a dos aspectes: comprovació que s'ha registrat el vot emès; comprovació que el sentit del vot registrat ha estat el correcte.

Pel que fa al primer aspecte, no sembla que la seva implementació hagi de comportar majors problemes que els que es poden plantejar actualment amb l'anotació dels votants que han exercit el seu vot en la llista de votants de les meses electorals. Al respecte es pot plantejar una publicació d'una llista amb els codis alfanumèrics assignats a cada votant en el moment de la

votació i que permetrien que ell mateix identifiqués si el seu vot ha estat registrat, sense que aquesta circumstància sigui identificable per terceres persones.

En canvi, pot plantejar més problemes la segona de les comprovacions apuntades en la mesura que la dissociació de les dades del votant respecte del vot emès no ha de poder ser reconstruïda. No obstant això, poden implementar-se mecanismes en què això sí que pugui fer-se a través de mecanismes que requereixin la participació conjunta del votant i de l'administració electoral sota certes garanties (p. ex. un codi compost en què l'administració electoral en tingui una part i el votant electrònic una altra).

Tal com apuntàvem abans, els riscos, vénen derivats de la possibilitat que amb aquests sistemes de verificació o control a posteriori algú pugui accedir al sentit del vot de persones identificades o identificables, ja sigui per suplantació de credencials o per sostracció de la informació dels servidors que emmagatzemen la informació.

Com en els sistemes presencials, des de la perspectiva de protecció de dades ens situaríem en el context de l'obligació que té el responsable del tractament de salvaguardar la informació que té emmagatzemada, i els suports que la contenen (sistemes de copies de seguretat per exemple) i de garantir que només pot accedir a aquesta informació la persona a la qual correspon el vot emès.

VII

L'avaluació concreta dels riscos generats per un determinat sistema caldrà fer-la a la vista de la solució tecnològica adoptada en cada cas. I la tecnologia, és clar, resultat canviant. Per això, caldrà tenir en compte l'evolució tecnològica, tant dels nous sistemes de votació electrònica o de mecanismes específics d'identificació electrònica (per exemple sistemes biomètrics, dispositius mòbils, televisió digital, etc.), com els nous riscos derivats de l'aplicació d'aquestes noves tecnologies, que implicarà l'aparició de noves vulnerabilitats.

En aquest sentit qualsevol que sigui el sistema emprat, aquest ha de garantir la seva solidesa tècnica (disponibilitat, fiabilitat i seguretat), la seva verificació per part d'un autoritat independent, i la facilitació d'informació suficient als futurs electors sobre les característiques, el funcionament i les garanties del sistema.

No obstant això, sí que es poden avançar en aquest dictamen algunes recomanacions que caldria tenir en compte en una futura llei electoral catalana, amb independència de quin sigui el sistema concret escollit.

En aquest sentit la llei electoral, quant a la seguretat de la informació, hauria d'anar encaminada d'una banda a preveure uns grans principis de protecció de la informació, principis als que hauran de donar resposta les tecnologies, seguint l'exemple de l'art. 9 de la LOPD que dóna contingut al principi de seguretat i per una altra banda la regulació haurà de ser neutra tecnològicament, sense lligar les solucions de seguretat a unes tecnologies concretes.

Per això, sens perjudici que les solucions finals de tipus tècnic i organitzatiu puguin afegir altres elements de reflexió als que conté aquest dictamen podem destacar les següents qüestions o recomanacions a tenir en compte:

a) Als sistemes de vot electrònic, siguin presencials o remots, se'ls hauria d'aplicar les mesures de seguretat de nivell alt previstes a la normativa de protecció de dades de caràcter personal, per tal de fer efectiu el principi de seguretat.

b) El sistema que s'implanti ha de garantir la identificació i l'autenticació del votant, evitant la suplantació o la duplicitat de vots, el secret del vot, el caràcter lliure del dret de sufragi, com també l'existència d'un nivell de transparència i verificabilitat del sistema que, tot i preservant el caràcter secret del vot permeti controlar-ne l'adequat funcionament.

c) Cal informar adequadament els ciutadans de les característiques i el funcionament del sistema, com també de les garanties del seu correcte funcionament.

d) Cal fer una anàlisi de riscos detallada i adaptada a cada procés electoral, en funció de les seves característiques i especialment de les tecnologies utilitzades.

e) Cal aplicar metodologies d'avaluació del impacte sobre la privacitat, a fi de triar en cada cas les opcions que siguin més respectuoses, o menys "perilloses" per a la informació de caràcter personal relacionada amb el procés de votació, i seguint el model habitual d'aquests avaluacions fer arribar a l'opinió pública el resultat d'aquesta reflexió (avaluació d'impacte), a fi de donar confiança en el sistema.

f) En general serà útil l'aplicació de tècniques de dissociació de la informació en algunes fases de cicle de vot electrònic, encara que sigui necessari preveure sistemes reversibles, tot i requerint la concurrència de més d'una persona o sistema per tornar a associar les dades a persones, però que en cap cas permetin que ningú diferent al votant pugui conèixer el contingut del seu vot. El secret del vot s'ha de garantir en qualsevol circumstància.

g) El xifrat de la informació també serà una tècnica a tenir present en tot el procés, tant en les qüestions relacionades amb les xarxes de telecomunicacions com en l'accés i emmagatzemament de la informació.

h) Cal establir previsions per tal de verificar que les empreses que participin en la implementació del sistema de votació electrònic compleixen amb tots els requisits de seguretat i també la resta de les garanties establertes per la normativa de protecció de dades, com ara, si escau, la formalització d'un contracte en els termes de l'article 12 LOPD, com també el retorn de tots els fitxers que es tinguin en la seva possessió a la finalització del procés. Igualment caldrà vetllar perquè es compleixin les esmentades exigències en els simulacres que es puguin dur a terme.

i) En general s'ha de preveure el control de la integritat de tot el sistema a base d'auditories de seguretat per entitats independents tant a priori, és a dir, abans de l'inici dels processos de votació, verificant que cap dels elements del sistema d'informació que dóna suport al procés electrònic de votació altera la informació i que en definitiva compleix amb els requisits de seguretat definits, i auditories a posteriori, per verificar que realment han estat eficaces les mesures de seguretat implantades.

j) En la definició de l'arquitectura tècnica i procediments operatius, el principi de segregació de funcions en matèria de seguretat de la informació ha d'estar present en tots els sistemes d'informació que donin suport al vot electrònic.

D'acord amb les consideracions fetes en aquests fonaments jurídics, es fan les següents,

Conclusions

Tot i que des del punt de vista estricte de la protecció de dades la implantació de sistemes de vot electrònic no aporta avantatges significatius, tot i que sí que pugui comportar-los des d'altres perspectives, la implantació d'aquests sistemes no resulta contrària al dret a la protecció de les dades personals si s'implanten amb les degudes garanties a què s'ha fet referència en aquest dictamen.

No obstant això, i atès l'estat actual de la tècnica, sembla que la incorporació d'aquests mitjans només pot dur-se a terme amb plenes garanties de seguretat en sistemes de vot electrònic presencial, mentre que el vot electrònic remot no sembla que pugui oferir suficients garanties. Per això, especialment mentre els canals de vot electrònic remot no siguin universalment accessibles, sembla que un sistema d'aquestes característiques s'hauria de limitar a la seva utilització com a mitjà alternatiu als actuals sistemes de votació per correu.