Recomandarea CM/Rec(2017)5 a Comitetului Miniștrilor către statele membre privind standardele pentru votul electronic

Linii directoare privind implementarea prevederilor Recomandării CM/Rec(2017)5 privind standardele pentru votul electronic

Traducere neoficială realizată de Departamentul legislativ – Biroul pentru documentare legislativă și relația cu Parlamentul din cadrul Autorității Electorale Permanente

Recomandarea CM/Rec(2017)5
a Comitetului Miniștrilor către statele membre privind standardele pentru votul electronic

(Adoptată de Comitetul Miniștrilor la 14 iunie 2017, la cea de-a 1289-a reuniune a reprezentanților miniștrilor)

Preambul

Comitetul Miniștrilor, în conformitate cu articolul 15.b din Statutul Consiliului Europei,

Considerând că scopul Consiliului Europei este de a realiza o unitate mai puternică între membrii săi, în scopul protejării și promovării idealurilor și principiilor care constituie patrimoniul lor comun;

Reafirmând convingerea că democrația reprezentativă și directă face parte din acest patrimoniu comun și reprezintă fundamentul participării cetățenilor la viața politică la nivelul Uniunii Europene, precum și la nivel național, regional și local;

Având în vedere obligațiile și angajamentele asumate în cadrul instrumentelor și documentelor internaționale existente, respectiv:

- Declarația universală a drepturilor omului;
- Pactul internațional privind drepturile civile și politice;
- Convenția Organizației Națiunilor Unite privind eliminarea tuturor formelor de discriminare rasială;
- Convenția Organizației Națiunilor Unite privind eliminarea tuturor formelor de discriminare împotriva femeilor;
- Convenția Organizației Națiunilor Unite privind drepturile persoanelor cu handicap;
- Convenția Organizației Națiunilor Unite împotriva corupției;
- Convenția pentru apărarea drepturilor omului și a libertăților fundamentale (ETS nr. 5), în special Protocolul aceasteia (ETS nr. 9);
- Carta europeană a autonomiei locale (ETS nr. 122);
- Convenția privind criminalitatea informatică (ETS nr. 185);
- Convenția pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal (ETS nr. 108);
- Protocolul adițional la Convenția pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal, privind autoritățile de supraveghere și fluxurile transfrontaliere de date (ETS No. 181);
- Convenția privind standardele alegerilor democratice, ale drepturilor electorale și ale libertăților în statele membre ale CSI (CDL-EL (2006) 031rev);

- Recomandarea Rec(99)5 a Comitetului Miniștrilor către statele membre privind protecția vieții private pe internet;
- Recomandarea Rec(2004)15 a Comitetului Miniștrilor către statele membre privind guvernanța electronică (e-guvernare);
- Recomandarea CM/Rec(2009)1 a Comitetului Miniștrilor către statele membre privind democrația electronică (e-democrația);
- Documentul reuniunii de la Copenhaga a Conferinței privind dimensiunea umană a OSCE;
- Carta Drepturilor Fundamentale a Uniunii Europene;
- Codul bunelor practici în materie electorală, adoptat de Consiliul pentru Alegeri Democratice al Consiliului Europei și Comisia Europeană pentru Democrație prin Drept (Comisia de la Veneția) și susținut de Comitetul Miniștrilor, Adunarea Parlamentară și Congresul autorităților locale și regionale ale Consiliului Europei;

Având în vedere faptul că dreptul de vot se află la temelia democrației și că, în consecință, toate metodele de vot, inclusiv votul electronic, trebuie să respecte principiile alegerilor democratice și ale referendumurilor;

Recunoscând că utilizarea tehnologiilor informației și comunicațiilor în alegeri de către statele membre a crescut considerabil în ultimii ani;

Luând act de faptul că unele state membre utilizează deja sau intenționează să utilizeze votul electronic pentru mai multe scopuri, printre care:

- crearea posibilității, pentru alegători, de a vota dintr-un alt loc decât la secția de votare din circumscripția electorală de care aparțin;
- facilitarea exercitării votului de către alegători;
- facilitarea participării la alegeri și la referendumuri a cetățenilor cu drept de vot și/sau de ședere în străinătate;
- sporirea accesului la procesul de votare pentru alegătorii cu dizabilități sau cei care întâmpină alte dificultăți de a se prezenta la o secție de votare și de a utiliza dispozitivele disponibile acolo;
- creșterea numărului de participanți la vot prin furnizarea de metode de vot suplimentare;
- alinierea procesului de votare la recentele evoluții ale societății și utilizarea tot mai mare a noilor tehnologii ca mijloc de comunicare și de implicare civică în urmărirea democrației;
- reducerea, în timp, a costului total al organizării alegerilor sau referendumurilor de către autoritățile electorale;
- furnizarea rezultatelor votului în mod fiabil și rapid;
- furnizarea unor servicii mai performante alegătorilor, punându-le la dispoziție o varietate de metode de exprimare a votului;

Evaluând experiența dobândită de către statele membre care au utilizat votul electronic în ultimii ani și lecțiile învățate în urma acestei experiențe;
Conștientizând, de asemenea, experiența rezultată din aplicarea recomandării Rec(2004)11 a Comitetului Miniștrilor către statele membre privind standardele juridice, operaționale și tehnice pentru votul electronic, Ghidul pentru dezvoltarea proceselor care confirmă respectarea cerințelor și standardelor recomandare (Certificarea sistemelor de vot electronic) și Liniile directoare privind transparența alegerilor electronice;
Reafirmând convingerea că încrederea publică în autoritățile responsabile cu gestionarea alegerilor este o condiție prealabilă introducerii votului electronic;
Conștientizând preocupările legate de posibilele probleme de securitate, fiabilitate sau transparență ale sistemelor de vot electronic;
Conștientizâmd, prin urmare, că doar acele sisteme de vot electronic care sunt sigure, fiabile, eficiente și robuste din punct de vedere tehnic, deschise spre verificare independentă și ușor accesibile alegătorilor, vor consolida încrederea publică, care este o condiție prealabilă pentru desfășurarea alegerilor electronice;
Conștientizând necesitatea ca statele membre să țină seama de mediul în care este implementat votul electronic;
Conștientizând faptul că, în lumina recentelor evoluții tehnice și juridice privind alegerile electronice în statele membre ale Consiliului Europei, este necesară revizuirea și actualizarea amănunțită a dispozițiilor din Recomandarea Rec(2004)11;
Având în vedere activitatea Comitetului ad-hoc de experți privind standardele juridice, operaționale și tehnice pentru votul electronic (CAHVE), înființat de Comitetul Miniștrilor în vederea actualizării Recomandării Rec(2004)11,
1. Recomandă guvernelor statelor membre ca atunci când doresc să introducă, să revizuiască sau să actualizeze, după caz, legislația și practicile interne în domeniul votului electronic, să aibă în vedere următoarele:

i. Să respecte toate principiile alegerilor și referendumurilor democratice;

ii. Să evalueze și să contracareze riscurile prin măsuri adecvate, în special în ceea ce privește riscurile specifice votului electronic;

iii. Legislația, politicile și practicile lor în domeniu să fie în concordanță cu standardele incluse în Anexa I la prezenta recomandare. Trebuie luată în considerare interconectarea dintre standardele menționate mai sus și cele incluse în Liniile directoare privind punerea în aplicare a prezentei recomandări;

iv. Să evalueze permanent politicile și experiența în domeniul votului electronic și, în special, maniera și măsura în care dispozițiile prezentei recomandări sunt puse în aplicare, pentru a oferi Consiliului Europei o bază pentru organizarea de reuniuni de examinare privind transpunerea în practică a acestei recomandări, cel puțin o dată la doi ani după adoptarea acesteia;

v. Să-și împărtășească experiența în acest domeniu;

vi. Să se asigure că această recomandare, Memorandumul Explicativ și Liniile directoare însoțitoare sunt traduse și diseminate pe cât posibil pe scară largă și mai ales în rândul organismelor de management electoral, oficialilor electorali, cetățenilor, partidelor politice, observatorilor naționali și internaționali, ONG-urilor, mass-media, cadrelor universitare, specialiștilor în soluții privind votul electronic și al autorităților cu atribuții în gestionarea votului electronic;

2. Este de acord să actualizeze în mod regulat dispozițiile Liniilor directoare care însoțesc această recomandare;

3. Se abrogă Recomandarea Rec(2004)11 privind standardele juridice, operaționale și tehnice pentru votul electronic și Liniile directoare ale acesteia.

ANEXA I – STANDARDELE VOTULUI ELECTRONIC

I. Sufragiul universal

1. Interfața electorală a unui sistem de vot electronic trebuie să fie ușor de înțeles și de folosit de către toți alegătorii.

2. Sistemul de vot electronic trebuie conceput, în măsura în care este posibil, astfel încât să permită persoanelor cu handicap și nevoi speciale să voteze independent.

3. Cu excepția cazului în care metodele de vot electronic de la distanță sunt universal accesibile, acestea ar trebui să constituie doar o modalitate suplimentară și opțională de exercitare a dreptului de vot.

4. Înainte de a opta pentru exercitarea dreptului de vot prin intermediul unui sistem electronic de votare la distanță, alegătorii trebuie să conștientizeze faptul că alegerile la care își exercită dreptul de vot prin mijloace electronice sunt alegeri sau referendumuri reale.

II. Sufragiul egal

5. Toate informațiile oficiale privind votarea trebuie prezentate în mod egal, în cadrul și prin toate canalele de vot.

6. În cazul în care se utilizează atât metode de vot electronice, cât și neelectronice în cadrul aceluiași scrutin, trebuie să existe o metodă sigură și fiabilă de a agrega toate voturile și de a calcula rezultatul.

7. Trebuie să se asigure o identificare unică a alegătorilor**,** într-un mod care să permită distincția clară și sigură a persoanei.

8. Sistemul de vot electronic trebuie să acorde accesul unui utilizator doar după autentificarea acestuia ca persoană cu drept de vot.

9. Sistemul de vot electronic va permite exercitarea, stocarea în urna electronică și includerea în rezultatul final al alegerilor doar a numărului corespunzător de voturi la care are dreptul un alegător.

III. Sufragiul liber

10. Intenția de vot a alegătorului nu va fi afectată de sistemul de votare sau de orice altă influență nejustificată.

11. Sistemul de vot electronic va prezenta alegătorului un buletin autentic și informații autentice.

12. Modul în care alegătorii sunt ghidați prin procesul de votare electronică nu trebuie să-i determine să voteze pripit sau fără confirmare.

13. Sistemul de vot electronic trebuie să-i ofere alegătorului posibilitatea de a participa la alegeri sau la referendum, fără ca acesta să-și exprime preferința pentru una dintre opțiuni.

14. Sistemul de vot electronic va acorda asistență alegătorului dacă el sau ea transmite un vot electronic nevalabil.

15. Alegătorul trebuie să poată verifica dacă intenția sa este reprezentată cu precizie, iar votul sigilat a intrat în urna electronică fără a fi modificat. Orice influență nejustificată care a modificat votul trebuie să fie detectabilă.

16. Alegătorul primește confirmarea din partea sistemului că votul a fost exprimat cu succes și că întreaga procedură de vot a fost încheiată.

17. Sistemul de vot electronic oferă dovezi solide că fiecare vot autentic este inclus în mod corect în rezultatele alegerilor respective. Dovezile trebuie să poată fi verificate prin mijloace independente de sistemul de vot electronic.

18. Sistemul trebuie să furnizeze dovezi solide că numai voturile alegătorilor eligibili au fost incluse în rezultatul final. Dovezile trebuie să poată fi verificate prin mijloace independente de sistemul de vot electronic.

IV. Sufragiul secret

19. Votarea electronică este organizată astfel încât secretul votului să fie respectat în toate etapele procedurii de votare.

20. Sistemul de vot electronic elaborează și stochează, cât timp este necesar, numai datele cu caracter personal necesare desfășurării alegerilor electronice.

21. Sistemul de vot electronic și orice actor autorizat trebuie să protejeze datele de autentificare, astfel încât părțile neautorizate să nu poată utiliza, intercepta, modifica sau obține cunoștințe despre aceste date.

22. Registrele alegătorilor stocate sau comunicate de sistemul de vot electronic sunt accesibile numai părților autorizate.

23. Un sistem de vot electronic nu oferă alegătorului dovezi privind conținutul votului exprimat, pentru a fi utilizat de către terți.

24. Sistemul de vot electronic nu permite divulgarea numărului de voturi exprimate decât după închiderea urnei electronice de vot. Aceste informații nu vor fi divulgate publicului decât după încheierea perioadei de votare.
25. Votarea electronică asigură respectarea secretului alegerilor anterioare înregistrate și șterse de către alegător, înainte de a-și exprima votul final.
26. Procesul de votare electronică, în special etapa de numărare, trebuie să fie organizat astfel încât să nu fie posibilă reconstituirea unei legături între votul deschis și alegător. Voturile sunt și rămân anonime.

V. Cerințe de reglementare și organizare

27. Statele membre care introduc votul electronic fac acest lucru într-o manieră treptată, progresivă.
28. Înainte de a introduce votul electronic, statele membre fac modificările necesare în legislația relevantă.
29. Legislația relevantă reglementează responsabilitățile pentru funcționarea sistemelor de vot electronic și asigură controlul organismelor electorale asupra acestora.
30. Orice observator trebuie să poată lua parte la numărarea voturilor. Organismul de management electoral este responsabil pentru procesul de numărare.

VI. Transparență și observare

31. Statele membre sunt transparente în toate aspectele legate de votul electronic.
32. Publicul, în special alegătorii, va fi informat, cu mult timp înainte de începerea votării, în limbaj clar și simplu, despre:
- orice măsuri pe care un alegător ar trebui să le ia pentru a vota;
- utilizarea și funcționarea corectă a unui sistem de vot electronic;
- calendarul votului electronic, incluzând toate etapele.
33. Componentele sistemului de vot electronic trebuie să poată fi dezvăluite în scopuri de verificare și certificare.
34. Orice observator, în măsura permisă de lege, va putea să observe și să comenteze alegerile electronice, inclusiv stabilirea rezultatelor.
35. Vor fi utilizate standarde deschise, pentru a permite interoperabilitatea diferitelor componente sau servicii tehnice, eventual derivate dintr-o varietate de surse.

VII. Responsabilitatea

36. Statele membre vor elabora cerințe tehnice, de evaluare și certificare și se vor asigura că acestea reflectă pe deplin principiile juridice și democratice relevante. Statele membre vor actualiza permanent aceste cerințe.
37. Înainte de introducerea unui sistem de vot electronic și la intervale corespunzătoare după aceea, în special după modificarea semnificativă a sistemului, un organism

independent și competent va evalua onformitatea sistemului de vot electronic și a oricărei componente a tehnologiei informației și comunicațiilor (TIC) cu cerințele tehnice. Aceasta poate fi o formă de certificare formală sau o altă formă adecvată de control.
38. Certificatul sau orice alt document corespunzător emis trebuie să identifice în mod clar obiectul evaluării și să includă garanții pentru a preveni modificarea sa în mod secret sau în mod accidental.
39. Sistemul de vot electronic poate fi supus auditului. Sistemul de audit trebuie să fie deschis și cuprinzător și să raporteze în mod activ posibilele probleme și amenințări.

VIII. Fiabilitatea și securitatea sistemului

40. Organismul de management electoral este responsabil cu respectarea tuturor cerințelor, chiar și în caz de erori și atacuri. Organismul de management electoral răspunde de disponibilitatea, fiabilitatea, utilitatea și securitatea sistemului de vot electronic.
41. Numai persoanele autorizate de organismul de management electoral au acces la infrastructura centrală, serverele și datele electorale. Numirea persoanelor autorizate să opereze în sistemul de vot electronic trebuie să fie clar reglementată.
42. Înainte ca orice alegeri electronice să aibă loc, organismul de management electoral se va asigura că sistemul de vot electronic este autentic și funcționează corect.
43. Trebuie să se instituie o procedură pentru instalarea regulată a versiunilor actualizate și corectarea tuturor software-urilor relevante.
44. Dacă sunt stocate sau comunicate în afara mediului controlat, voturile sunt criptate.
45. Voturile și informațiile alegătorilor se păstrează sigilate până la începerea procesului de numărare.
46. Organismul de management electoral va opera în siguranță toate materialele criptografice.
47. În cazurile în care apar incidente care ar putea amenința integritatea sistemului, persoanele responsabile cu exploatarea echipamentului informează imediat organismul de management electoral.
48. Trebuie păstrată autenticitatea, disponibilitatea și integritatea registrelor electorale și a listelor de candidați. Sursa datelor trebuie autentificată. Dispozițiile privind protecția datelor trebuie respectate.
49. Sistemul de vot electronic identifică voturile care sunt afectate de o iregularitate.

ANEXA II - GLOSARUL TERMENILOR

În această recomandare și în expunerea de motive, se utilizează următorii termeni cu următoarele semnificații:

- controlul accesului: prevenirea utilizării neautorizate a unei resurse;

- evaluarea: o evaluare a persoanelor, hardware-ului, software-ului și procedurilor pentru a verifica dacă acestea sunt adecvate pentru îndeplinirea anumitor sarcini;
- audit: o evaluare independentă pre sau post-electorală a unei persoane, organizații, sistem, proces, entitate, proiect sau produs care include analiza cantitativă și calitativă;
- autentificare: asigurarea identității unei persoane sau date;
- disponibilitate: starea de a fi accesibil și utilizabil la cerere;
- buletinul de vot: mijloacele recunoscute legal prin care alegătorul își poate exprima votul;
- candidat: o opțiune de vot constând dintr-o persoană, un grup de persoane și/sau un partid politic;
- exercitarea votului: introducerea votului în urna de vot;
- certificat: un document care este rezultatul unei certificări oficiale, prin care un fapt este certificat sau atestat;
- certificare: un proces de confirmare a faptului că un sistem de vot electronic este în conformitate cu cerințele și standardele prescrise și că include, cel puțin, dispoziții pentru a se asigura funcționarea corectă a sistemului. Acest lucru se poate realiza prin măsuri precum testări și audit și până la certificări formale. Rezultatul final este un raport și/sau un certificat;
- organism de certificare (sau certificator): o organizație autorizată să efectueze un proces de certificare și să emită un certificat la finalizarea procesului;
- raport de certificare: un document care explică ce se certifică prin certificat și modul în care se certifică;
- lanțul de încredere: un proces în domeniul securității calculatorului, care este stabilit prin validarea fiecărei componente hardware și software de jos în sus. Intenția este să se asigure că pot fi utilizate numai software și hardware de încredere, păstrându-se însă flexibiltatea;
- testarea componentelor: o metodă prin care unitățile individuale ale codului sistemului sunt testate pentru a determina dacă sunt adecvate pentru utilizare;
- confidențialitate: starea care caracterizează informațiile care nu ar trebui să fie puse la dispoziție sau dezvăluite persoanelor, entităților sau proceselor neautorizate;
- mediu controlat: spații supravegheate de funcționari electorali, de ex. secții de votare, ambasade sau consulate;
- alegeri electronice: alegeri politice sau referendum în care se utilizează votul electronic;
- organismul de management electoral: instituția responsabilă de gestionarea alegerilor într-o anumită țară la nivel național sau regional;

- urna de vot electronică: mijloacele electronice prin care sunt stocate voturile în așteptarea numărării;
- vot electronic: vot exprimat electronic;
- votare electronică: utilizarea mijloacelor electronice de exprimare și/sau de numărare a voturilor;
- sistemul de vot electronic: hardware-ul, software-ul și procesele care permit alegătorilor să voteze prin mijloace electronice la alegeri sau referendumuri;
- certificare formală: certificare efectuată de autorități, numai înainte de ziua alegerilor și care conduce la emiterea unui certificat;
- linii directoare: orice document care vizează eficientizarea anumitor procese în conformitate cu o rutină stabilită. Prin definiție, liniile directoare nu sunt obligatorii din punct de vedere juridic;
- acordul de nedivulgare: un contract juridic între două sau mai multe părți care prezintă materiale, cunoștințe sau informații confidențiale, pe care părțile doresc să le împărtășească în anumite scopuri, dar doresc să limiteze accesul părților care nu sunt legate de contract;
- acces liber: accesul online la materialele gratuite pentru citire și, eventual, utilizare (sau refolosire) în anumite limite;
- profil de protecție: un set de cerințe de securitate independente de punerea în aplicare pentru o categorie de produse, care satisface nevoile specifice de securitate ale consumatorilor;
- cerința: o necesitate documentată singulară a ceea ce ar trebui să fie sau să îndeplinească un anumit produs sau serviciu;
- vot electronic de la distanță: utilizarea mijloacelor electronice de a vota în afara locurilor unde are loc votul în general;
- sigilare: protejarea informațiilor astfel încât să nu poată fi utilizate sau interpretate fără ajutorul altor informații sau mijloace, disponibile numai persoanelor sau autorităților autorizate, inclusiv prin criptare;
- persoana interesată: o persoană, grup, organizație sau sistem care are un impact asupra sau poate fi afectată de acțiunile unui guvern sau organizație. Acestea includ cetățeni, oficiali electorali, partide politice, guverne, observatori naționali și internaționali, mass-media, cadre universitare, ONG-uri, organizații anti-votul electronic și organisme specifice de certificare a votării electronice;
- standard (legal): se referă la dispozițiile din anexa I la Recomandarea CM/Rec(2017)5;
- standard (tehnic): o normă stabilită, de obicei, sub forma unui document formal care prevede criterii inginerești sau tehnice, metode, procese și practici uniforme;
- testarea: procesul de verificare a funcționării sistemului conform așteptărilor;

- vot: exprimarea opțiunii de vot;
- alegător: o persoană care are dreptul de a vota într-un anumit proces electoral sau referendum;
- canalul de vot: modalitatea prin care alegătorul își poate exercita dreptul de vot;
- opțiunile de vot: gama de posibilități dintre care se poate face o alegere prin exercitarea votului în cadrul unui proces electoral sau referendum;
- registrul alegătorilor: o listă a persoanelor cu drept de vot (alegători)

---

[1] La adoptarea acestei recomandări, Reprezentantul Permanent al Federației Ruse a indicat că, în conformitate cu articolul 10.2c din Regulamentul de procedură pentru reuniunile reprezentanților miniștrilor, rezervă dreptul guvernului său de a se conforma sau nu Recomandării.

Linii directoare privind implementarea prevederilor Recomandării CM/Rec(2017)5 privind standardele pentru votul electronic

A 289-a ședință, 14 iunie 2017 - Democrația și problemele politice
Comitetul de experți ad-hoc privind standardele juridice, operaționale și tehnice pentru votul electronic (CAHVE)
Punct examinat de GR-DEM în cadrul reuniunilor sale din 20 aprilie și 1 iunie 2017.

Preambul
Comitetul Miniștrilor, în conformitate cu articolul 15.b din Statutul Consiliului Europei, considerând că scopul Consiliului Europei este de a realiza o unitate mai puternică între membrii săi, în scopul protejării și promovării idealurilor și principiilor care sunt patrimoniul lor comun;
Reafirmând convingerea că democrația reprezentativă și directă face parte din acest patrimoniu comun și reprezintă fundamentul participării cetățenilor la viața politică la nivelul Uniunii Europene, precum și la nivel național, regional și local;
Având în vedere obligațiile și angajamentele asumate în cadrul instrumentelor și documentelor internaționale existente, respectiv:

- Declarația universală a drepturilor omului;
- Pactul internațional privind drepturile civile și politice;
- Convenția Organizației Națiunilor Unite privind eliminarea tuturor formelor de discriminare rasială;
- Convenția Organizației Națiunilor Unite privind eliminarea tuturor formelor de discriminare împotriva femeilor;
- Convenția Organizației Națiunilor Unite privind drepturile persoanelor cu handicap;
- Convenția Organizației Națiunilor Unite împotriva corupției;
- Convenția pentru apărarea drepturilor omului și a libertăților fundamentale (ETS nr. 5), în special Protocolul aceasteia (ETS nr. 9);
- Carta europeană a autonomiei locale (ETS nr. 122);
- Convenția privind criminalitatea informatică (ETS nr. 185);
- Convenția pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal (ETS nr.108);
- Protocolul adițional la Convenția pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal, privind autoritățile de supraveghere și fluxurile transfrontaliere de date (ETS nr.181);

- Convenția privind standardele alegerilor democratice, ale drepturilor electorale și ale libertăților în statele membre ale CSI (CDL-EL (2006) 031rev);
- Recomandarea Rec(99)5 a Comitetului Miniștrilor către statele membre privind protecția vieții private pe internet;
- Recomandarea Rec(2004)15 a Comitetului Miniștrilor către statele membre privind guvernanța electronică (e-guvernare);
- Recomandarea CM/Rec(2009)1 a Comitetului Miniștrilor către statele membre privind democrația electronică (e-democrația);
- Documentul reuniunii de la Copenhaga a Conferinței privind dimensiunea umană a OSCE;
- Carta Drepturilor Fundamentale a Uniunii Europene;
- Codul bunelor practici în materie electorală, adoptat de Consiliul pentru Alegeri Democratice al Consiliului Europei și Comisia Europeană pentru Democrație prin Drept (Comisia de la Veneția) și susținut de Comitetul Miniștrilor, Adunarea Parlamentară și Congresul autorităților locale și regionale ale Consiliului Europei;

Având în vedere faptul că dreptul de vot se află la temelia democrației și că, în consecință, toate metodele de vot, inclusiv votul electronic, trebuie să respecte principiile alegerilor democratice și ale referendumurilor;

Recunoscând că utilizarea tehnologiilor informației și comunicațiilor în alegeri de către statele membre a crescut considerabil în ultimii ani;

Luând act de faptul că unele state membre utilizează deja sau intenționează să utilizeze votul electronic pentru mai multe scopuri, printre care:

- crearea posibilității, pentru alegători, de a vota dintr-un alt loc decât la secția de votare din circumscripția electorală de care aparțin;
- facilitarea exercitării votului de către alegători;
- facilitarea participării la alegeri și la referendumuri a cetățenilor cu drept de vot și/sau de ședere în străinătate;
- sporirea accesului la procesul de votare pentru alegătorii cu dizabilități sau cei care întâmpină alte dificultăți de a se prezenta la o secție de votare și de a utiliza dispozitivele disponibile acolo;
- creșterea numărului de participanți la vot prin furnizarea de metode de vot suplimentare;
- alinierea procesului de votare la recentele evoluții ale societății și utilizarea tot mai mare a noilor tehnologii ca mijloc de comunicare și de implicare civică în urmărirea democrației;
- reducerea, în timp, a costului total al organizării alegerilor sau referendumurilor de către autoritățile electorale;
- furnizarea rezultatelor votului în mod fiabil și rapid;

– furnizarea unor servicii mai performante alegătorilor, punându-le la dispoziție o varietate de metode de exprimare a votului;

Evaluând experiența dobândită de către statele membre care au utilizat votul electronic în ultimii ani și lecțiile învățate în urma acestei experiențe;

Conștientizând, de asemenea, experiența rezultată din aplicarea recomandării Rec(2004)11 a Comitetului Miniștrilor către statele membre privind standardele juridice, operaționale și tehnice pentru votul electronic, Ghidul pentru dezvoltarea proceselor care confirmă respectarea cerințelor și standardelor recomandare (Certificarea sistemelor de vot electronic) și liniile directoare privind transparența alegerilor electronice;

Reafirmând convingerea că încrederea publică în autoritățile responsabile cu gestionarea alegerilor este o condiție prealabilă introducerii votului electronic;

Conștientizând preocupările legate de posibilele probleme de securitate, fiabilitate sau transparență ale sistemelor de vot electronic;

Conștientizâmd, prin urmare, că doar acele sisteme de vot electronic care sunt sigure, fiabile, eficiente și robuste din punct de vedere tehnic, deschise spre verificare independentă și ușor accesibile alegătorilor vor consolida încrederea publică, care este o condiție prealabilă pentru desfășurarea alegerilor electronice;

Conștientizând necesitatea ca statele membre să țină seama de mediul în care este implementat votul electronic;

Conștientizând faptul că, în lumina recentelor evoluții tehnice și juridice privind alegerile electronice în statele membre ale Consiliului Europei, este necesară revizuirea și actualizarea amănunțită a dispozițiilor din Recomandarea Rec(2004)11;

Având în vedere activitatea Comitetului ad-hoc de experți privind standardele juridice, operaționale și tehnice pentru votul electronic (CAHVE), înființat de Comitetul Miniștrilor cu sarcina actualizării Recomandării Rec(2004)11;

Adoptă următoarele linii directoare privind standardele de vot electronic, care să servească drept instrument practic pentru guvernele statelor membre în susținerea, adoptarea, punerea în aplicare și monitorizarea implementării votării electronice descrise în acestea și pentru adaptarea sistemelor lor de vot electronic;

Invită guvernele statelor membre să se asigure că liniile directoare sunt difuzate pe scară largă în rândul organismelor de management electoral, al funcționarilor electorali, cetățenilor, partidelor politice, observatorilor naționali și internaționali, organizațiilor neguvernamentale (ONG), mass-mediei, cadrelor universitare, furnizorilor de soluții tehnice în domeniul votului electronic și organismelor de control al votării electronice.

Introducere

1. Prezentele linii directoare sunt versiunea actualizată a Ghidului de elaborare a proceselor care confirmă respectarea cerințelor și a standardelor recomandate (certificarea sistemelor de vot electronic) și a Ghidului privind transparența alegerilor cu

caracter electronic. Cele două linii directoare inițiale au fost aprobate în 2011, pentru a oferi îndrumări cu privire la implementarea dispozițiilor privind certificarea și transparența recomandării Rec(2004)11 a Comitetului de Miniștri către statele membre privind standardele juridice, operaționale și tehnice pentru votarea electronică din 30 septembrie 2004.

2. Recomandarea Rec(2004)11 și liniile directoare inițiale au fost revizuite și actualizate în 2015 și 2016 de Comitetul ad-hoc al experților privind standardele juridice, operaționale și tehnice pentru vot electronic (CAHVE), înființat de Comitetul Miniștrilor la 1 aprilie 2015.

3. Prezentele linii directoare oferă îndrumări privind punerea în aplicare a dispozițiilor din Recomandarea CM/Rec(2017)5. Fiecare dintre liniile directoare este identificată printr-un număr, care se referă la dispoziția corespunzătoare din recomandare.

4. Versiunea actuală a liniilor directoare este o lucrare în desfășurare care va fi finalizată în continuare pentru a aborda toate formele de vot electronic care fac obiectul Recomandării CM/Rec(2017)5. Prin urmare, evoluțiile în curs în domeniul juridic și tehnic vor impune actualizarea regulată a dispozițiilor liniilor directoare.

5. Liniile directoare sunt destinate utilizării în alegeri și referendumuri, la toate nivelurile de guvernare. Acestea nu sunt înțelese ca un set riguros de reguli pentru statele membre, impunând o modalitate specială de punere în aplicare a dispozițiilor recomandării actualizate, dar sunt menite să ofere orientări și să sprijine statele membre în acest domeniu.

6. Liniile directoare, precum recomandarea actualizată, nu constituie un cadru de reglementare exhaustiv pentru votarea electronică. Statele membre trebuie să dezvolte în continuare aceste dispoziții pentru a ține seama de particularitățile naționale în domeniul electoral. Liniile directoare includ, de asemenea, exemple de implementare eficientă a standardelor în contexte specifice, numite bune practici. Exemple de bune practici sunt incluse în scop informativ.

I. Linii directoare pentru implementarea recomandărilor privind sufragiul universal

7. Interfața electorală a unui sistem de vot electronic trebuie să fie ușor de înțeles și de utilizat de către toți alegătorii.

a. Prezentarea opțiunilor de vot pe dispozitivul folosit de către alegător ar trebui optimizată pentru toți alegătorii, inclusiv pentru cei care nu au cunoștințe informatice specializate.

Produsele și serviciile trebuie să fie adaptabile restricțiilor funcționale ale utilizatorilor și circumstanțelor specifice, fără a aduce atingere unor principii precum egalitatea. Acest lucru se poate realiza prin oferirea de versiuni diferite ale aceluiași produs, prin modificări ale parametrilor cheie, design modular, accesorii sau alte metode.

b. Alegătorii ar trebui să fie implicați în proiectarea sistemelor de vot electronic, în special pentru a identifica constrângerile și a ușura testarea utilizării în fiecare etapă principală a procesului de dezvoltare.

Accesibilitatea implică faptul că sistemele sunt concepute astfel încât cât mai mulți alegători să le poată folosi. Produsele și serviciile IT trebuie să fie funcționale și să țină seama de nevoile publicului, fără a fi complicate în mod inutil. Astfel de cerințe ar putea fi realizate printr-o abordare comună, care să implice echipa de dezvoltare și un grup reprezentativ de utilizatori.

c. Ar trebui să se ia în considerare, atunci când se elaborează noi produse IT, compatibilitatea acestora cu cele existente.

8. Sistemul de vot electronic este conceput, în măsura posibilului, pentru a permite persoanelor cu handicap și nevoi speciale să voteze independent.

a. Alegătorii ar trebui să aibă disponibile, ori de câte ori este necesar și posibil, facilități suplimentare, cum ar fi interfețe speciale sau alte resurse echivalente, precum asistența personală.

Votul electronic poate fi o modalitate alternativă de vot, care oferă posibilități suplimentare persoanelor cu handicap și nevoi speciale de a vota în mod independent. Ar trebui găsit un echilibru acceptabil între furnizarea acestor posibilități de acces și respectarea altor cerințe, precum cele referitoare la securitatea votării electronice.

b. Interfețele de vot pe internet ar trebui să respecte cât mai mult posibil orientările stabilite în Inițiativa privind accesibilitatea web (WAI).

Consorțiul World Wide Web (W3C) a fost creat în 1994 pentru a ridica World Wide Web (WWW) la întregul său potential, prin dezvoltarea de protocoale comune. Acesta a inițiat WAI pentru a promova un grad ridicat de accesibilitate pentru persoanele cu handicap. WAI urmărește accesibilitatea web prin intermediul a cinci domenii principale de activitate: tehnologie, linii directoare, instrumente, educație și mobilizare și cercetare și dezvoltare. WAI a elaborat un set de standarde și linii directoare în sprijinul accesibilității (de exemplu, orientările privind accesibilitatea conținutului web, instrumentele de creație, orientările privind accesibilitatea, agentul utilizator, orientările privind accesibilitatea, orientările privind accesibilitatea XML). Mai multe informații sunt disponibile pe site-ul WAI la http://www.w3.org/WAI.

WAI este frecvent utilizat în contextul soluțiilor bazate pe browser pentru votarea pe internet. Chiar dacă votarea pe internet folosește soluții alternative (de exemplu, aplicația de vot este un browser separat unic în sine), principiile generale WAI pot fi respectate.

II. Linii directoare pentru implementarea recomandărilor privind sufragiul egal

9. Toate informațiile oficiale privind votul vor fi prezentate în mod egal, în cadrul şi prin intermediul canalelor de vot.

a. Buletinul de vot electronic nu ar trebui să conțină alte informații despre opțiunile de vot, față de cele prevăzute de lege.

Interfața de vot electronic nu ar trebui să conțină mai multe informații despre alegeri decât buletinele oficiale (tipărite de obicei pe hârtie). Elemente cum ar fi ecrane pop-up care promovează un anumit candidat sau poziție sau elemente audio asociate unui anumit candidat sau punct de vedere și orice alte informații care nu apar pe buletinul de hârtie (egalitatea metodelor de vot) nu ar trebui să apară pe interfața de vot electronic. Acest lucru nu împiedică afișarea informațiilor oficiale privind opțiunile de vot.

b. Dacă informațiile despre opțiunile de vot sunt accesibile de pe site-ul de vot electronic, acesta trebuie prezentat într-un mod echitabil.

Informațiile privind opțiunile de vot trebuie prezentate în mod echitabil pentru toate metodele de vot.

10. Sistemul de vot electronic trebuie să asigure că numai numărul corespunzător de voturi pe alegător este exprimat, stocat în urna electronică şi inclus în rezultatul alegerilor.

a. Dacă unui alegător i se permite să voteze de mai multe ori electronic, trebuie luate măsuri adecvate pentru a se lua în calcul doar un singur vot.

b. Dacă unui alegător i se permite să voteze prin intermediul mai multor canale de vot, trebuie luate măsuri adecvate pentru a se asigura că se va în calcul un singur vot.

Liniile directoare 9a și 9b: Ori de câte ori este permis votul multiplu, acest lucru ar trebui să se reflecte și în procesul de votare electronică. De exemplu, anumite sisteme de votare permit alegătorilor să exercite un vot în avans sau mai multe voturi în avans și să-și schimbe opțiunea mai târziu. Doar ultimul vot este introdus în urna de vot și, prin urmare, este singurul vot valabil exprimat. Acesta este cazul în Andorra, Danemarca și Suedia.

Opțiunea de vot multiplă (mai multe voturi electronice sau mai multe voturi exercitate prin mai multe canale de vot) poate fi introdusă în cazul votului electronic, ca o contramăsură a constrângerii alegătorilor, care rămâne posibilă atunci când votarea are loc în afara unui mediu controlat (votul la distanță). Acesta este cazul în Estonia.

Determinarea votului care trebuie luat în calcul trebuie făcută la nivel național. În contextul votului electronic, o țară poate decide că votul pe hârtie are prioritate. În altă țară, numai ultimul vot va fi luat în calcul. O a treia țară poate decide că primul vot valabil exprimat este cel care contează. Pentru a fi în conformitate cu principiile alegerilor democratice, sistemul de vot electronic (sau utilizarea simultană a metodelor de vot și a votării electronice) trebuie să asigure votul egal. Legislația națională trebuie să stabilească care dintre voturi va fi luat în considerare. Principiul "un om, un vot" trebuie respectat.

Decizia asupra metodei prin care se alege votul care contează depinde de politica națională privind votul la distanță. Țările care au o politică mai strictă în ceea ce privește votul la distanță vor avea tendința de a acorda prioritate buletinului de vot, dacă acesta este votul emis la secția de votare (mediu controlat). Țările care sunt mai deschise față de votul la distanță pot decide că primul vot valabil emis este cel care contează, iar în acest caz un vot electronic dintr-un mediu necontrolat poate înlocui un vot de hârtie emis ulterior. Deciziile privind modul de abordare a coerciției alegătorilor în cazul votului la distanță, trebuie să fie luate, de regulă, de legiuitorul național. Acestea nu ar trebui lăsate doar la latitudinea autorității care reglementează votarea electronică, deoarece sunt o chestiune de politică privind votul la distanță, în general, și nu doar de implementare a votării electronice.

c. În toate celelalte cazuri, ar trebui luate măsuri adecvate pentru a împiedica alegătorul să voteze multiplu.

În țările în care votul multiplu nu este permis, acesta este considerat o încercare de a vota de mai multe ori decât îi este permis unui anumit alegător. Acest risc ar putea apărea, de exemplu, în cazul în care alegătorul încearcă să voteze de mai multe ori sau dacă o altă persoană încearcă să folosească identitatea alegătorului pentru a vota, în numele acestuia, după ce și-a exercitat propriul drept de vot.

În contextul votării cu buletine de vot, acest risc este gestionat prin măsuri organizatorice. De exemplu, în Regatul Unit, în cazul în care o persoană intră într-o secție de votare pentru a vota și descoperă că altcineva a votat deja în numele său, persoana respectivă are dreptul de a vota pe un buletin de vot special. Acest buletin de vot nu este plasat în urnă, ci este închis într-un plic și se examinează numai în cazul unei cereri de verificare și în conformitate cu o hotărâre a unei instanțe. O dispoziție similară se aplică atunci când sunt primite două voturi poștale din partea aceluiași alegător. În contextul votării electronice trebuie luate măsuri adecvate. Identificarea sigură este importantă. Una dintre măsurile care se pot lua constă în menținerea pentru o anumită perioadă a legăturii dintre codurile de identificare ale alegătorului și votul său sigilat.

Introducerea votării electronice la distanță aduce cu sine întrebarea: cum sunt legate perioadele de timp pentru votarea în secție și votul electronic la distanță. La prima vedere, ar părea logic că pentru ambele metode de vot ar trebui să se aplice aceleași perioade de timp, pentru a evita complicațiile și distincțiile. Cu toate acestea, există motive care ar putea determina ca votarea să aibă loc în momente diferite, respectiv:

- atunci când votarea în secție este opțiunea de rezervă pentru alegătorii care se află pe teritoriul național în cazul în care metoda de vot electronic se blochează, timpul de închidere pentru votarea electronică trebuie să fie stabilit înainte de ora de închidere a secției de votare;
- când sistemul este proiectat și operat în așa fel încât alegătorii să poată alege între metodele de vot, dar metodele utilizate nu au acces la un registru comun unde

numele alegătorilor care au votat să poată fi văzut, perioadele de timp în care aceste metode sunt disponibile ar trebui, de regulă, să nu se suprapună.

În toate cazurile, numărarea voturilor ar trebui să înceapă numai după închiderea tuturor canalelor de vot.

d. În toate cazurile, alegătorul ar trebui să fie clar informat cu privire la posibilitățile de vot oferite și la regulile de numărare a voturilor.

Este deosebit de important ca alegătorul să fie informat cu privire la posibilitățile sale de a vota, inclusiv posibilitatea de a emite mai multe voturi prin vot electronic sau de a vota succesiv prin mai multe metode de vot diferite, în cazul în care este permis votul multiplu.

În toate cazurile, alegătorul ar trebui să fie informat cu privire la regulile în vigoare de numărare a voturilor, în special cu privire la votul care va fi luat în considerare în cele din urmă.

III. Linii directoare pentru implementarea recomandărilor privind sufragiul liber

11. Intenția alegătorului nu trebuie să fie afectată de sistemul de vot sau de orice altă influență nejustificată.

a. În cazul votării electronice la distanță, alegătorul trebuie să fie informat cu privire la modalitățile de verificare a faptului că a fost stabilită o conexiune la serverul oficial și că a fost utilizat un buletin de vot autentic.

În contextul votării electronice la distanță, scenariile posibile care trebuie luate în considerare sunt serverele frauduloase, cum ar fi imitarea unui server oficial prin manipularea unui nume de domeniu (DNS), folosind un nume de domeniu similar cu cel al serverului oficial sau coruperea codului serverului (de exemplu, prin programe malware), printre altele. Alegătorii primesc informații despre cum să verifice certificatul site-ului oficial de votare electronică. Semnăturile electronice aplicate buletinului de vot de către autoritatea electorală permit verificarea buletinului de vot. Totuși, nu trebuie să se încalce confidențialitatea votului.

b. Sistemul de vot electronic nu trebuie să permită exercitarea unei influențe manipulative asupra alegătorului în timpul votării. În special buletinul electronic prin care este exprimat votul nu trebuie să conțină informații neoficiale.

Similar cu prevederea 5a, această linie directoare impune ca alegătorul să aibă acces numai la informații oficiale privind votarea, orice influență manipulatoare a părților neautorizate fiind exclusă.

c. Sistemul de vot electronic ar trebui să introducă toate măsurile posibile pentru a evita orice influență manipulativă care ar putea fi exercitată asupra votului odată ce a fost exercitat și va include măsuri care să permită verificarea faptului că nu a fost exercitată nicio astfel de influență.

Conceptul de sufragiu liber protejează de asemenea votul de orice influență manipulativă, după ce a fost exprimat. Orice influență manipulativă asupra intervenției neautorizate în cadrul votului trebuie evitată. Bineînțeles, dacă este permis, votul multiplu nu este afectat de această dispoziție și alegătorului ar trebui să i se permită să voteze de mai multe ori.
Dispoziția vizează prevenirea oricărei modificări neautorizate a votului, odată ce a fost exprimat. De asemenea, protejează împotriva atacurilor care provin din afara sistemului și împotriva amenințărilor interne. Verificarea individuală și universală (a se vedea standardele 15 și 17) sunt controale care vizează detectarea unei astfel de intervenții neautorizate.
d. Atunci când este necesar, sistemul de vot electronic ar trebui să ofere mecanisme (de exemplu, metode de vot multiple) pentru a proteja alegătorii de constrângerea de a vota într-un anumit mod.
Metodele multiple de vot sunt considerate a fi un mecanism care protejează alegătorul de constrângere, permițându-i să voteze din nou.
12. Modul în care alegătorii sunt ghidați prin procesul de votare electronică nu trebuie să-i determine să voteze pripit sau fără confirmare.
a. Alegătorii ar trebui să poată modifica alegerea lor în orice moment al procesului de votare la distanță, înainte să-și exercite votul sau să întrerupă procedura.
Această dispoziție prevede posibilitatea anulării procedurii înainte de votare, adică înainte de a accesa buletinul electronic de vot. Odată ce votul este înregistrat, acest lucru nu va mai fi posibil. Prin urmare, interfața trebuie programată pentru a atrage atenția alegătorilor asupra acestui punct, de exemplu cerându-le să-și confirme intențiile înainte de a emite votul. Ar fi util, de asemenea, să reamintească alegătorilor că această operațiune va valida și finaliza votul în cazurile în care votul multiplu nu este permis.
13. Alegătorul trebuie să fie în măsură să verifice dacă intenția sa este reflectată cu precizie de vot și că votul sigilat a intrat în urna de vot electronică fără a fi modificat. Orice influență nejustificată care a modificat votul trebuie să fie detectabilă.
a. Atunci când se utilizează mașinile de vot în secțiile de votare, statele membre ar trebui să ia în considerare utilizarea buletinelor de vot pe hârtie ca un al doilea mediu pentru stocarea votului, în scopul verificării.
Cunoscută, de asemenea, sub numele de interogare pe hârtie a votului exprimat de către alegător (VVPAT), această metodă vizează asigurarea votului liber în cazul în care votul este exprimat prin intermediul mașinilor de vot electronic, în medii controlate. Dacă soluția electronică aplicată în secțiile de votare este un scaner de vot, nu este necesar un al doilea mediu, deoarece buletinul de vot este în acest caz, prin definiție, din hârtie.
Alte soluții pentru furnizarea unui al doilea mediu includ, de exemplu, părți ale buletinului de vot care poate fi rupt (de exemplu, modelul de scantegritate al lui Chaum) pentru verificarea individuală. Ele pot fi foarte asemănătoare cu VVPAT sau pot lua altă

formă. Acestea ar trebui să fie făcute din hârtie, care este atât nealterabilă, cât și lizibilă/verificabilă de către om.
Valabilitatea acestui al doilea mediu va fi evaluată prin reglementări naționale, care vor decide, de asemenea, ce trebuie făcut în caz de discrepanțe între rezultatele electronice și cele produse de cel de-al doilea mediu.
b. O numărătoare obligatorie a voturilor în cel de-al doilea mediu, dintr-un număr statistic semnificativ de secții de votare selectate aleatoriu ar trebui să se efectueze în special pentru mașinile de vot electronic și pentru scanerele optice.
Criteriile, cum ar fi procentajul voturilor sau numărul de secții de votare unde are loc numărarea, desemnarea lor etc., trebuie stabilite la nivel național. Acestea ar trebui să aibă în vedere ca obiectivul general de asigurare a alegerilor libere să fie atins.

IV. Linii directoare pentru implementarea recomandărilor privind secretul votului

14. Votarea electronică este organizată astfel încât să se asigure că secretul votului este respectat în toate etapele procedurii de votare.
a. Datele din registrul electoral trebuie să fie clar separate de componentele de vot.
Această prevedere se aplică mai specific atunci când tehnicile biometrice de identificare a alegătorului sunt utilizate în secțiile de votare, pe lângă utilizarea mașinilor de vot electronic sau a scanerelor pentru votare. Separarea celor două componente asigură secretul voturilor.
În cazul în care voturile și informațiile anonime ale alegătorilor sunt păstrate împreună, criptarea totală trebuie să protejeze aceste informații.
15. Sistemul de vot electronic și orice parte autorizată trebuie să protejeze datele de autentificare, astfel încât părțile neautorizate să nu poată utiliza, să intercepteze, să modifice sau să obțină altfel cunoștințe despre aceste date.
a. Autentificarea ar trebui să utilizeze mecanisme criptografice.
Această prevedere necesită soluții tehnice de ultimă oră pentru protejarea datelor de autentificare.
16. Un sistem de vot electronic nu oferă alegătorului dovada conținutului votului exprimat, pentru a fi utilizat de către terți.
a. În cazul în care votul electronic este furnizat alegătorului într-un mediu controlat, acestuia nu trebuie să i se permită să îl arate oricărei alte persoane sau să facă dovada în afara secției de votare.
Votarea electronică nu trebuie să facă dovada conținutului votului pentru alegător. Atunci când acest lucru este programat la un moment dat în procedura de votare, cum ar fi cazul votării prin intermediul mașinilor de vot electronic în secțiile de votare, ar trebui să existe măsuri organizatorice pentru a împiedica utilizarea acestei dovezi, pentru evitarea încălcării secretului votului. Scopul este de a proteja secretul voturilor și de a împiedica

practica vânzării voturilor. Bineînțeles, acest lucru nu împiedică alegătorul, în termeni absoluți, să dezvăluie conținutul votului său, de exemplu, prin captarea unei imagini a acestuia. Depinde de legile penale sau administrative naționale, care se aplică și votului electronic, de a sancționa astfel de încălcări ale secretului votului.

b. Nu vor fi afișate informații reziduale legate de decizia alegătorului după exercitarea votului.

Termenul "informație reziduală" se referă la informațiile care rămân accesibile în diverse locații (în memoria calculatorului personal, memoria cache a browserului, memoria video, fișierele swap, fișierele temporare etc.) după votare și care pot dezvălui decizia alegătorului.

Dispoziția îi sfătuiește pe dezvoltatorii de sisteme sau pe furnizorii de servicii să elaboreze sistemul de vot electronic astfel încât informațiile reziduale să fie șterse după votare. Din punct de vedere tehnic, pot exista mijloace limitate pentru a asigura acest lucru într-un mediu de vot la distanță. Cu toate acestea, ar trebui luate toate măsurile posibile pentru a șterge aceste informații reziduale în momentul votării. Cu toate acestea, verificarea individuală poate fi pusă în aplicare, cu condiția să existe garanții adecvate pentru a preveni coerciția sau cumpărarea voturilor.

c. În cazul votării electronice la distanță, alegătorul ar trebui să fie informat despre posibilele riscuri legate de secretul votului și să-i fie recomandate mijloacele de a le reduce înainte de vot.

d. În cazul votării electronice la distanță, alegătorul ar trebui să fie informat cu privire la modul de ștergere, acolo unde este posibil, a urmelor votului din dispozitivul folosit pentru votare.

Orientările 23c și 23d: În cazul votării electronice la distanță, alegătorii ar trebui să fie clar informați cu privire la riscul de încălcare a secretului votului și la măsurile și bunele practici pe care trebuie să le adopte pentru a contracara acest risc, de exemplu prin utilizarea firewall-urilor, etc. Sistemul în sine ar trebui să șteargă automat cât mai multe urme posibile.

Votarea electronică de la distanță, dintr-un mediu necontrolat implică responsabilități comune între alegător și sistemul de vot electronic/organismul electoral. Depinde de responsabilitatea alegătorului de a adopta măsurile recomandate (menționate în această dispoziție). Este datoria autorității electorale să informeze în mod clar alegătorul cu privire la cel puțin trei puncte: principiul responsabilităților comune; diferitele măsuri care trebuie adoptate de către alegător pentru a reduce riscul (executarea unui software antivirus, firewall, ștergerea urmelor votului etc.); precum și riscurile și tehnicile de verificare.

Aceste informații ar trebui să ajungă la alegător cu mult înainte de perioada de vot. Pe baza acestor criterii, alegătorul poate decide dacă utilizează sau nu votul electronic de la distanță.

Mesajele de avertizare pot apărea la începutul procedurii de votare electronică; un mesaj cu privire la pașii recomandați pe care ar trebui să-i urmeze alegătorul după votare (de exemplu, ștergerea traseelor) poate fi necesar să fie transmis alegătorului la sfârșitul procedurii de votare electronică. Cu toate acestea, astfel de mesaje sunt doar mementouri și nu înlocuiesc informațiile complete inițiale pe care alegătorul ar trebui să le primească înainte de începerea perioadei votului electronic.

17. Procesul de vot electronic, în special etapa de numărare, trebuie organizat astfel încât să nu fie posibilă reconstituirea unei legături între votul necriptat și alegător.Voturile trebuie să fie și să rămână anonime.

a. Informațiile despre alegător trebuie să fie separate de decizia acestuia într-o etapă predefinită a procesului de numărare.

b. Orice decodare necesară pentru numărarea voturilor trebuie efectuată cât mai curând posibil după încheierea perioadei de vot.

Termenul "informație despre alegător" se referă la informațiile anonime ale alegătorului, cum ar fi codurile de identificare utilizate în procesul de votare la distanță. Întrucât legătura dintre aceste informații și votul sigilat trebuie menținută pentru o anumită perioadă de timp sub o protecție adecvată, pentru a permite, în special, posibilitatea votării multiple, respectând în același timp principiul "un om, un vot", aceasta ar trebui distrusă înainte ca număratoarea să aibă loc.

În general, criptarea voturilor va fi necesară pentru a asigura anonimatul votului. În multe cazuri, votul este criptat înainte de a începe transmisia prin intermediul rețelelor de calculatoare. Acesta este ținut criptat în urna de vot și este decodificat înainte de numărare. Numărarea este efectuată cu voturi decodificate, care nu pot fi asociate cu niciun alegător.

Cu toate acestea, există metode de criptare care nu necesită decodificare înainte de numărarea voturilor (criptarea homomorfă). Numărarea poate fi efectuată fără a dezvălui conținutul voturilor criptate. În unele cazuri, poate fi chiar necesar ca numărarea să fie efectuată în timp ce voturile sunt în stare criptată, pentru a asigura anonimatul.

c. Statele membre ar trebui să ia măsurile necesare pentru a se asigura că este garantată confidențialitatea oricăror informații obținute de către orice persoană în timpul îndeplinirii funcțiilor de audit.

Pe lângă protecția informațiilor colectate de sistemul de audit împotriva accesului neautorizat, ar trebui luate măsuri juridice și organizatorice pentru a verifica persoanele care au autorizat accesul la sistemul de audit. Astfel de măsuri ar putea fi incluse, de exemplu, în procesul de acreditare.

V. Linii directoare pentru implementarea recomandărilor de reglementare și organizaționale

18. Statele membre care introduc votul electronic trebuie să facă acest lucru într-o manieră treptată și progresivă.

a. Înainte de selectarea și punerea în aplicare a oricărei tehnologii de vot electronic ar trebui să fie realizat și publicat un studiu formal de fezabilitate. Acesta ar trebui să includă motivele pentru adoptarea acestui sistem, analiza riscurilor, evaluarea cadrului juridic, planificarea proiectelor-pilot și evaluarea acestora, precum și o analiză cost-beneficiu.

b. Orice implementare a proiectelor-pilot de vot electronic ar trebui să înceapă cu suficient timp înaintea alegerilor și să includă pregătiri esențiale, precum adoptarea unor reglementări detaliate, dacă este necesar, pentru proiectele-pilot și testarea sistemelor.

c. Versiunea finală a sistemului de vot electronic trebuie testată înainte de a fi folosită la alegerile regulate.

d. Proiectele-pilot ar trebui să se desfășoare pe baza unor criterii clare și cuprinzătoare, pentru a evalua eficacitatea și integritatea sistemului de vot electronic, inclusiv transmiterea rezultatelor.

19. Înainte de a implementa votul electronic, statele membre trebuie să opereze modificările necesare în legislație.

a. Cadrul juridic ar trebui să includă proceduri pentru implementarea votării electronice de la înființare și operare la numărare.

Dispozițiile detaliate vor apărea cel mai probabil în reglementările și instrucțiunile de nivel inferior. Acest lucru ar trebui prevăzut în legile la nivel superior, care ar trebui, de asemenea, să clarifice responsabilitățile pentru adoptarea unor astfel de reglementări detaliate.

b. Cadrul juridic ar trebui să includă reguli pentru stabilirea valabilității votului electronic.

c. Cadrul juridic ar trebui să includă norme privind problemele, eșecurile și discrepanțele rezultate din utilizarea instrumentelor de verificare.

Atunci când statele membre utilizează o modalitate secundară pentru a stoca votul și se efectuează o numărare obligatorie, pot apărea discrepanțe între rezultatele voturilor exprimate. În astfel de cazuri, regulile trebuie să precizeze ce tip de vot (electronic sau varianta alternativă) are prioritate. Un argument pentru votul electronic este că alegătorii și-au exprimat votul în acest mod. Un argument în favoarea modalității secundare de stocare ar fi că acest vot ar fi putut fi verificat chiar de către alegător, mai ales dacă modalitatea în cauză include o variantă de hârtie.

Prin urmare, în caz de neconcordanță, situația ar trebui să fie examinată în detaliu, iar orice decizie privind rezultatul numărării voturilor ar trebui să depindă de rezultatul anchetei. Statelor membre li se solicită să stabilească norme referitoare la votul care se utilizează în numărătoarea oficială, dacă și când este considerată necesară o renumărare,

când și cum are loc numărătoarea obligatorie, în ce circumstanțe sunt luate în considerare toate voturile secundare și când ar trebui repetate alegerile.

d. Cadrul juridic ar trebui să includă proceduri pentru procesul de distrugere a datelor, în special pentru alinierea procesării, stocării și distrugerii datelor (și echipamentelor) tehnologiei votării la legislația privind protecția datelor cu caracter personal.

Mediul de stocare care conține voturile (hard disk, stick-uri de memorie etc.) trebuie distrus.

e. Cadrul juridic ar trebui să includă dispoziții pentru observatorii naționali și internaționali. Statele membre ar trebui să includă rolul observatorilor naționali și internaționali în procesul de votare electronică și ar trebui să îl reglementeze în conformitate cu angajamentele și bunele practici internaționale. Tipul de acces la votarea electronică pe care îl vor avea observatorii va depinde de dispozițiile naționale. Acestea ar trebui să reflecte angajamentele internaționale, precum cele ale Oficiului pentru Instituții Democratice și Drepturile Omului din cadrul Organizației pentru Securitate și Cooperare în Europa (OSCE/ODIHR). Observatorii ar trebui să includă reprezentanți ai partidelor politice și ai publicului larg.

f. Legislația ar trebui să prevadă calendare clare privind toate etapele votului electronic.

Alegerile electronice pot diferi de alte alegeri sau referendumuri în ceea ce privește procedurile care trebuie urmate de către alegători. Exemple de potențiale diferențe sunt perioada de timp în care pot fi exercitate voturile, pașii pe care un alegător trebuie să îi parcurgă pentru a participa la alegerile electronice și modul în care are loc efectiv votarea electronică. Aceste diferențe trebuie comunicate în mod clar alegătorului, pentru a evita orice neînțelegere a procedurilor și pentru a-i oferi toate informațiile necesare pentru a putea lua o decizie bine fundamentată cu privire la metoda de vot pe care o folosește. O atenție deosebită ar trebui acordată timpului necesar alegătorului pentru a lua această decizie.

g. Perioada în care poate fi exercitat votul electronic nu trebuie să înceapă înainte de stabilirea datei alegerilor sau a referendumului.

Comunicarea perioadei de vot este deosebit de importantă atunci când perioada de exercitare a votului electronic diferă de alte metode de vot. Această diferență apare în special în cazul votării electronice la distanță, care poate necesita o perioadă diferită de timp pentru exercitarea votului electronic, datorită naturii specifice a acestei metode.

h. Votarea electronică la distanță poate să înceapă și/sau să se termine la un moment anterior deschiderii oricărei secții de votare.

i. Perioada în care se poate vota electronic nu ar trebui să continue după încheierea perioadei de vot.

Liniile directoare 28h și 28i: Din diferite motive, perioada de vot electronic de la distanță poate fi mai lungă decât perioada în care secțiile de votare sunt deschise. Aceste motive

includ furnizarea unui serviciu mai bun pentru cetățeni și sporirea accesibilității acestora la sistem.

Cu toate acestea, votarea electronică la distanță nu ar trebui să continue după încheierea perioadei de votare în secții. În cazul în care sistemul de vot electronic nu este disponibil (de exemplu, dacă un computer personal al alegătorului nu funcționează din cauza unei căderi de tensiune), un alegător care locuiește sau se află în țara în care au loc alegerile sau referendumul trebuie să fie în continuare capabil să meargă la secția de votare pentru a-și exercita votul. În cazul în care votarea electronică ar continua după închiderea secțiilor de votare, alegătorul nu ar avea această posibilitate.

j. Depunerea voturilor electronice în urna electronică ar trebui să fie permisă pentru o perioadă suficientă de timp după încheierea perioadei de vot electronic, pentru a permite orice întârziere în transmiterea mesajelor pe canalul de vot electronic de la distanță.

k. După încheierea perioadei de vot electronic, niciunui alegător nu ar trebui să i se permită accesul la sistemul de votare electronică.

Liniile directoare 28j și 28k: Aceste dispoziții se referă la sesiunile de vot pe internet, care încep cu puțin timp înainte de încheierea canalului de vot electronic. Buletinul de vot trebuie să rămână accesibil, pentru a putea colecta aceste voturi. Durata va fi echivalentă cu durata normală a unei sesiuni de votare electronică, pentru a permite acelora care au acces la sistem cu câteva secunde înainte de a se închide pentru a finaliza procesul de vot electronic în mod normal.

Un alt caz, din nou în cadrul scenariilor de vot pe internet, se referă la o cerere mai mare privind serviciile care ar putea apărea în perioada scurtă chiar înainte de închiderea urnelor. Acest lucru poate duce la întârzieri înainte ca votul să intre în urna electronică de vot. Voturile care au fost trimise la timp nu ar trebui să fie ignorate ca urmare a unor astfel de întârzieri. Prelucrarea voturilor nu trebuie închisă imediat după închiderea serviciului de votare electronică. Cu toate acestea, începerea unei sesiuni de vot electronic după închiderea sistemului nu ar trebui să fie posibilă.

20. Legislația relevantă reglementează responsabilitățile pentru funcționarea sistemelor de vot electronic și asigură controlul organismului electoral asupra acestora.

a. Procesele de achiziție pentru sistemul de vot electronic ar trebui să se desfășoare în mod transparent.

b. Ar trebui prevăzute dispoziții pentru a exista asigurări împotriva eventualelor conflicte de interese ale părților interesate din sectorul privat, implicate în acest proces.

c. O separare strictă a sarcinilor trebuie menținută și documentată.

d. Statele membre trebuie să ia măsurile adecvate pentru a evita situațiile în care alegerile depind în mod nejustificat de furnizorii de astfel de servicii.

21. Orice observator trebuie să poată observa numărul voturilor. Organismul de management electoral este responsabil pentru procesul de numărare.

a. Ar trebui să se păstreze o evidență a procesului de numărare a voturilor electronice, inclusiv a informațiilor despre începutul și sfârșitul acestui proces, precum și despre persoanele implicate în numărare.
b. Numărarea voturilor trebuie să fie reproductibilă. Ar trebui să existe posibilitatea de a obține dovezi solide potrivit cărora procedura de numărare a fost efectuată în mod satisfăcător, inclusiv printr-o renumărare independentă.
Obiectivul este să existe posibilitatea de a obține dovezi solide că procedura de numărare a fost efectuată corect. O renumărare independentă este o modalitate de a face acest lucru, dacă se face cu un sistem diferit. Cu toate acestea, acest lucru poate fi realizat prin alte mijloace, de exemplu, prin utilizarea unei dovezi criptografice (posibilitate universală de verificare).
c. Alte caracteristici care ar putea influența acuratețea rezultatelor sistemului de vot electronic trebuie să poată fi verificate.
În funcție de sistemul utilizat, pot exista alte elemente pe lângă renumărare care să contribuie la corectitudinea rezultatului. Confirmarea faptului că au fost luate în considerare toate voturile exprimate este un exemplu în acest sens.
Pe lângă instrumentele de verificare, se consideră că procentul de voturi exprimate electronic și compararea rezultatelor votării electronice cu rezultatele votării prin alte metode determină plauzibilitatea rezultatelor votării electronice și validarea preciziei acestora.
d. Sistemul de vot electronic ar trebui să mențină disponibilitatea și integritatea urnelor de vot electronice și rezultatul procesului de numărare atât timp cât este necesar.
Informațiile păstrate în urna electronică trebuie să fie protejate atâta timp cât este necesar pentru a permite eventuale revizuiri sau contestații juridice sau alte cerințe legale în statul membru în cauză.

VI. Linii directoare pentru implementarea recomandărilor privind transparența și observarea

22. Statele membre trebuie să manifeste transparență în toate aspectele legate de votul electronic.
a. Autoritățile electorale competente ar trebui să publice o listă oficială a software-ului utilizat în cadrul unui scrutin electronic. Cel puțin, ar trebui să indice software-ul folosit, versiunea, data instalării și o scurtă descriere a acestuia.
Evoluțiile permanente ale tehnologiilor informației și comunicațiilor impun actualizări frecvente ale hardware-ului și software-ului și adaptări regulate la sistemele centrale și la facilitățile de vot utilizate într-un mediu controlat (de exemplu, mașinile de vot). Pentru ca votarea electronică să rămână transparentă, exactă, completă, ar trebui să fie publicate descrieri actualizate ale componentelor hardware și software, permițând astfel grupurilor interesate să verifice că sistemele în uz corespund celor certificate de către autoritățile

competente. Rezultatele certificării ar trebui să fie puse la dispoziția autorităților, a partidelor politice și, în funcție de prevederile legale în vigoare, la dispoziția cetățenilor.

b. Accesul public la componentele sistemului de vot electronic și la informațiile pe care acesta le furnizează, în special documentația, codul sursă și acordurile de confidențialitate, ar trebui să fie permis părților interesate și publicului larg, cu mult înainte de perioada electorală.

Atunci când un dispozitiv/sistem electronic generează rezultate obligatorii, detaliile tehnice care determină ce și cum se calculează pot deveni cu ușurință la fel de importante ca și o lege electorală care definește regulile de numărare în cadrul secțiilor de votare. Pentru a dobândi încrederea publicului prin asigurarea transparenței sistemului, codul sursă al software-ului de vot, configurația, precum și lista tuturor componentelor hardware și software ale sistemului de vot electronic trebuie să facă parte din traseul de audit. Protocoalele proceselor auditate, cum ar fi procedura de instalare și configurare, verificarea faptului că sursa certificată este cea utilizată în timpul alegerilor și procesul de înregistrare a buletinelor de vot electronice ar trebui, de asemenea, să facă parte din procedura de audit. Acest lucru ar trebui să ajute statele membre să furnizeze documente relevante alegătorilor și terților, inclusiv observatorilor naționali și internaționali și mass-media.

Expresia "cu mult timp înainte" implică stabilirea unor termene clare în reglementările naționale pentru astfel de informări, precum și faptul că termenele limită prevăzute permit părților interesate să-și exercite drepturile, să reacționeze la astfel de informări și să solicite schimbări. Organismul de management electoral ar trebui să aibă timpul și posibilitatea de a reacționa la astfel de observații, inclusiv prin actualizarea sistemului. Publicarea acestor informații, cu douăsprezece luni înainte de vot, poate respecta criteriul "cu suficient timp înainte". Pot fi necesare perioade mai scurte de timp pentru modificări de ultim minut. Cu toate acestea, elementele principale ar trebui să fie dezvăluite cu mult timp înainte de alegeri.

c. Implementarea tehnologiilor de vot electronic ar trebui să includă elaborarea unor linii directoare detaliate, pas cu pas, inclusiv un manual procedural.

23. Opinia publică, în special alegătorii, trebuie să fie informată cu mult timp înainte de începerea votării, într-un limbaj clar și simplu, cu privire la:

- pașii pe care un alegător trebuie să îi urmeze pentru a participa și a vota;
- utilizarea și funcționarea corectă a unui sistem de vot electronic;
- calendarul de vot electronic, incluzând toate etapele.

a. Materialele de sprijin și de orientare privind procedurile de vot ar trebui să fie puse la dispoziția alegătorilor.

Trebuie să existe un material de suport și de orientare privind procedurile de vot, indiferent de metoda specifică utilizată. Pentru fiecare canal de vot electronic folosit, aceste informații ar trebui să fie disponibile cel puțin pe același canal de vot electronic.

Cu alte cuvinte, trebuie să existe cel puțin un site web cu informații de ajutor și facilități de poștă electronică, atunci când internetul este canalul de vot electronic și trebuie să fie disponibilă o linie telefonică atunci când este posibilă votarea prin telefon.

b. În cazul votării electronice la distanță, materialele informative ale alegătorilor ar trebui să fie disponibile și prin intermediul unui alt canal de comunicare, disponibil pe scară largă.

Informațiile privind votarea electronică de la distanță ar trebui să fie disponibile și pe un canal de comunicare diferit, accesibil pe scară largă, pentru situațiile în care canalul de vot electronic de la distanță nu este funcțional. De exemplu, o linie telefonică poate fi un astfel de canal de comunicare alternativ pentru votarea prin internet.

c. Alegătorilor ar trebui să li se ofere o oportunitate de a exersa înainte și separat de momentul votării electronice propriu-zise. Într-un astfel de caz, participanților ar trebui să li se atragă atenția explicit asupra faptului că nu participă la un scrutin sau la un referendum real.

Metodele tradiționale de vot sunt bine utilizate și testate în statele membre, iar alegătorii sunt familiarizați cu regulile generale care le guvernează. Introducerea votării electronice reprezintă o provocare pentru alegători. Astfel de sisteme și modul în care funcționează sunt mai greu de înțeles. Pentru a menține înțelegerea și încrederea alegătorilor, trebuie luate măsuri pentru a le prezenta sistemul. Poate fi necesar ca acest efort să continue de-a lungul timpului.

Pentru a promova înțelegerea și încrederea în orice (nou) sistem de vot electronic, oportunitățile de testare a acestuia trebuie furnizate înainte și separat de momentul votării electronice (de exemplu, prin intermediul sistemelor demo sau al alegerilor de test). O atenție deosebită ar trebui acordată categoriilor de alegători care pot prezenta dificultăți mai mari (de exemplu, persoanele în vârstă) și nevoilor specifice ale acestora.

24. Componentele sistemului de vot electronic se dezvăluie în scopuri de verificare și certificare.

a. Sistemul de vot electronic ar trebui să genereze date de observație fiabile și suficient de detaliate pentru ca observarea alegerilor să poată fi efectuată. Ar trebui să fie posibilă determinarea în mod fiabil a momentului în care un eveniment a generat date de observare. Autenticitatea, disponibilitatea și integritatea datelor ar trebui menținute.

b. Observatorii interni și internaționali trebuie să aibă acces la toate documentele relevante pentru procesele de votare electronică.

Accesul la documentație, inclusiv minutele, rapoartele de certificare, testare și audit, precum și documentația detaliată care explică funcționarea sistemului sunt esențiale pentru observatorii interni și internaționali. Astfel de observatori includ reprezentanți ai partidelor politice și ai publicului larg. Aceștia ar trebui să fie invitați la reuniuni relevante. Atunci când este posibil, statele membre, furnizorul sau organismul de

certificare trebuie să ofere informații tuturor părților interesate, de exemplu prin publicarea unor documente relevante pe internet, cu mult înainte de perioada electorală.
Statele membre ar trebui să elaboreze proceduri pentru a defini cine are acces la ce și când. Astfel de proceduri ar trebui să fie elaborate și pentru observatorii interni și internaționali, precum și pentru mass-media. De asemenea, trebuie stabilite proceduri pentru alte părți interesate, cum ar fi cetățenii, partidele politice și ONG-urile. Accesul liber la informație ar trebui să fie tema centrală a acestor proceduri.
Statele membre ar trebui să facă aceste cerințe clare pentru potențialii furnizori care ar trebui să înțeleagă, de asemenea, că părțile interesate, și în special observatorii interni și internaționali, au nevoie de acces la anumite documente în timpul procedurii de licitație. Acordurile de nedivulgare, care împiedică observatorii să publice evaluări și faptele pe care se bazează evaluările, ar priva toate părțile interesate - în special observatorii - de informații importante.
c. Statele membre ar trebui să pună la dispoziția observatorilor documentația relevantă, în măsura în care acest lucru este posibil, într-o limbă folosită în mod obișnuit în relațiile internaționale.
Informațiile relevante cerute de observatorii interni și internaționali pentru a-și desfășura în mod satisfăcător activitatea ar trebui să fie disponibile în limba sau limbile oficiale ale țării în cauză. Aceste informații ar trebui, de asemenea, să fie puse la dispoziție, în măsura posibilului, într-una dintre limbile oficiale ale Consiliului Europei (engleză și franceză). În special observatorii internaționali au nevoie de acces la documentație într-una din aceste limbi.
d. Statele membre ar trebui să ofere programe de formare pentru grupurile de observatori interni și internaționali.
Sistemul de vot electronic nu este ușor de înțeles pentru persoanele care nu au expertiză în domeniul votului electronic. Pentru a îmbunătăți înțelegerea sistemului în uz de către părțile interesate, este necesară instruirea, în special pentru observatorii interni, dar și pentru cei internaționali. Ar trebui să fie furnizate instrumente de bază și ușor de utilizat în munca de observație, inclusiv modalități de verificare a sigiliilor, citirea unei pagini imprimate de o mașină de vot și citirea unui fișier de audit.
e. Observatorii interni și internaționali și mass-media ar trebui să poată urmări testarea software-ului și a hardware-ului.
Părțile interesate, inclusiv grupurile de observatori acreditate, nu ar trebui să aibă acces doar la documente, ci ar trebui, de asemenea, să poată urmări verificarea dispozitivelor și a sistemului de vot electronic. Observarea acestor teste și/sau proceduri de auditare nu ar trebui să interfereze cu procesul electoral. Prin urmare, o astfel de monitorizare ar trebui să aibă loc numai sub îndrumarea celor responsabili de organizarea alegerilor. După cum s-a menționat deja, astfel de observatori ar trebui să includă reprezentanți ai partidelor politice și ai societății civile. În plus, persoanele care participă la testele și/sau

procedurile de auditare trebuie să participle, de asemenea, la o sesiune de formare în avans. Procesul ar trebui să fie suficient de deschis pentru a le permite observatorilor să aibă o imagine completă asupra funcționării sistemului.

f. Observatorii electorali trebuie să aibă acces la toate etapele procesului de evaluare și certificare.

În ultimii douăzeci de ani, observarea alegerilor s-a dovedit a fi o metodă de succes pentru a asigura transparența și accesul la procesul electoral. Odată cu apariția votului electronic, metodologiile stabilite pentru observarea alegerilor trebuie să fie actualizate. Pentru a permite observatorilor să respecte certificarea sistemelor de vot electronic, durata misiunilor de observare a alegerilor trebuie extinsă. Este esențial ca niciuna dintre procedurile necesare pentru certificarea votării electronice să nu aibă loc în spatele ușilor închise, deoarece acest lucru ar ridica suspiciuni.

Observatorii, inclusiv reprezentanții partidelor politice și ai societății civile, ar trebui să aibă acces la toate informațiile relevante pe întreaga durată a procesului de certificare, pentru a-și îndeplini îndatoririle. Observatorii, la rândul lor, trebuie să dezvăluie metodologia pe care o vor aplica.

VII. Linii directoare pentru implementarea recomandărilor privind responsabilitatea

25. Statele membre elaborează cerințe tehnice, de evaluare și certificare și se asigură că ele reflectă pe deplin principiile juridice și democratice relevante. Statele membre vor actualiza permanent aceste cerințe.

a. Statele membre ar trebui să stabilească obiectivele certificării și metodele de certificare.

Atunci când se analizează certificarea sistemelor de votare la fața locului sau la distanță, primul pas este definirea clară a scopurilor și a cerințelor pentru procedura de certificare. La redactarea acestor cerințe, este important să se verifice dacă acestea respectă legislația internă și standardele internaționale, inclusiv orice contestații sau proceduri de plângere referitoare la desfășurarea alegerilor. Deși o listă detaliată a cerințelor ar putea părea inițial o modalitate bună de a garanta o analiză adecvată a certificării, un cadru legal strict ar putea genera efecte paradoxale. De exemplu, auditorii ar fi supuși unui nivel înalt de supraveghere, dar furnizorii ar putea personaliza produsele lor în scopul limitat de a îndeplini pur și simplu cerințele prescrise de o anumită administrație electorală. În aceste condiții, vânzătorii ar putea să nu optimizeze produsul, iar administrația electorală ar fi obligată prin propriile norme juridice să accepte un produs suboptim. Utilizarea unui contract în care criteriul de atribuire este calitatea și nu prețul ar trebui să contribuie la evitarea acestei capcane.

Definirea scopurilor, a cerințelor în ceea ce privește software-ul, sistemul de operare, procesul hardware și procesul de votare electronică, precum și domeniul de aplicare și

metodele vor contribui la eficacitatea procesului de certificare, la utilitatea regimului de certificare și la transparența generală a sistemelor de vot electronic.
Certificarea sistemelor de vot electronic nu se limitează la certificarea inițială; include, de asemenea, proceduri de decertificare și recertificare a software-ului, a sistemelor de operare, a hardware-ului și a tuturor proceselor.
Factorii sociopolitici pot condiționa încrederea cetățenilor și pot reprezenta o provocare majoră. Deoarece acești factori pot influența, de asemenea, procesele de certificare, statele membre ar trebui să promoveze cercetarea științifică în acest domeniu, inclusiv un schimb internațional de informații relevante.
Trebuie stabilit un cadru care să garanteze că toate părțile sunt conștiente și înțeleg bine sistemul. Activitatea ar trebui făcută în conformitate cu metodologiile stabilite, cum ar fi testarea de confirmare, testarea componentelor, testarea performanțelor și testarea funcțională.
26. Înainte de introducerea unui sistem de vot electronic și la intervale corespunzătoare după aceea, în special după modificarea semnificativă a sistemului, un organism independent și competent evaluează conformitatea sistemului de vot electronic și a oricărei tehnologii a informației și comunicări (TIC) cu cerințele tehnice. Aceasta poate lua forma unei certificări formale sau a unui alt control adecvat.
a. Statele membre ar trebui să stabilească repartizarea costurilor implicate în procesul de certificare. Acestea ar trebui să definească responsabilitatea, inclusiv cea financiară, a organismului de certificare pentru calitatea muncii lor.
Orice persoană autorizată să participe la certificarea unui sistem de vot electronic, incluzând atestatorii, evaluatorii și auditorii, trebuie să fie independentă și calificată. Prin urmare, criteriile, modalitățile și instituțiile competente implicate în selectarea organismelor de certificare ar trebui să fie prevăzute în mod explicit în legislația națională. Statele membre sunt responsabile de elaborarea normelor și orientărilor pentru procesul de selecție.
Aceste proceduri trebuie cunoscute și publicate cu mult înainte de ziua alegerilor. Acest lucru va înlesni sarcina furnizorilor și va încuraja încrederea alegătorilor în proceduri. Numărul organismelor de certificare nu ar trebui limitat; oricine este independent și calificat ar trebui să fie eligibil pentru a efectua certificarea. Ar trebui să se acorde prioritate utilizării unei licitații publice europene sau a unei consultări cu un set de potențiali certificatori pentru stabilirea calificărilor.
Statele membre ar trebui să aibă în vedere efectuarea procedurii de selecție de către auditori profesioniști certificați internațional. De exemplu, CISA (Certified Information System Auditors) este un standard de realizare pentru cei care auditează, controlează, monitorizează și evaluează tehnologiile informației și sistemele de afaceri ale unei organizații. Ar trebui să se acorde atenție costurilor acestor proceduri. Un alt factor

important este acela că utilizarea certificatelor internaționale nu ar trebui să devină un obstacol pentru Statele membre în folosirea unui sistem specific de votare electronică.
Statele membre ar trebui să indice explicit de la bun început ce organisme sunt responsabile pentru costurile procedurii de certificare. Acestea pot decide ca întregul cost, inclusiv certificarea formală, să fie suportat de către furnizori, ceea ce ar putea duce la o mai mare implicare a acestora din urmă. Costurile ar putea fi, de asemenea, responsabilitatea statului membru în cauză, iar o a treia opțiune este împărțirea costurilor. Costurile de certificare nu ar trebui în niciun caz să compromită independența, integritatea și calitatea procesului de certificare. Indiferent de opțiunea aleasă, statul membru ar trebui să dispună de fonduri suficiente și decizia ar trebui făcută publică.
b. Organismele de evaluare și certificare ar trebui să aibă acces deplin la toate informațiile relevante și ar trebui să li se aloce timp suficient pentru desfășurarea procesului de certificare înainte de alegeri.
Organismele de certificare ar trebui să aibă acces la informațiile și datele necesare și suficiente pentru a-și îndeplini sarcinile, și anume să ajungă la o concluzie privind sistemul de vot supus controlului; aceste organisme ar trebui să aibă suficient timp pentru a examina toate informațiile și datele. Cetățenii au dreptul să știe ce informații nu au fost considerate necesare și suficiente pentru a efectua certificarea. În plus, normele privind relația dintre furnizor și certificator, cum ar fi acordurile de nedivulgare (CND) sau alte documente similare, ar trebui să fie făcute publice.
În unele cazuri, cum ar fi alegerile anticipate sau introducerea unui nou sistem de votare, procesele de certificare pot avea loc abia înaintea deschiderii procesului electoral. Acest lucru implică riscul de a nu dispune de suficient timp pentru a întreprinde o procedură de certificare amănunțită, ceea ce, la rândul său, ar putea pune în pericol credibilitatea alegerilor. Prin urmare, procedura de certificare trebuie finalizată înaintea alegerilor, acordând suficient timp examinării concluziilor.
O soluție pentru a economisi timp și bani este certificarea numai a modulelor modificate și a secvenței modulelor pentru viitoarea certificare, odată ce a fost efectuat un proces inițial de certificare și componenta de vot electronic a fost certificată. Acest lucru este posibil numai dacă se face o diferență între modificările majore și modificările minore ale sistemului de vot electronic.
c. Mandatul organismelor de evaluare și certificare ar trebui să fie reconfirmat în mod regulat, la intervale prestabilite.
Statele membre ar trebui să elaboreze proceduri nu numai pentru selecția inițială, ci și pentru procedurile de urmărire, cum ar fi reexaminarea sau confirmarea mandatului și retragerea acestuia. Mandatul acordat oricărui organism pentru certificarea unui sistem de vot electronic trebuie să fie valabil numai pentru o perioadă limitată de timp. Ofertele trebuie să fie făcute la intervale regulate, iar aceste oferte trebuie să fie publice. Trebuie să se clarifice dacă decizia de a încredința certificarea unui sistem unui anumit organism

de certificare selectat poate fi luată de către furnizor sau dacă această decizie revine autorității electorale competente.

d. Concluziile la care s-a ajuns într-un raport de certificare ar trebui să fie suficient de explicite, cu ajutorul informațiilor conținute în acest raport.

Raportul de certificare ar trebui să fie explicit, și anume, concluziile sale ar trebui să se bazeze numai pe informațiile pe care le conține, permițând unei terțe părți să reproducă aceeași cercetare și astfel să confirme că concluziile raportului de certificare sunt valabile.

e. Statele membre ar trebui să stabilească și să publice norme clare cu privire la divulgarea raportului final de certificare și a tuturor documentelor relevante, având în vedere importanța transparenței în cadrul acestui proces.

Statele membre ar trebui să elaboreze și să publice proceduri în care să se definească cine are acces, la ce informații și când. O atenție deosebită trebuie acordată nevoilor observatorilor interni și internaționali și nevoilor mass-media. De asemenea, trebuie stabilite proceduri pentru alte părți interesate, cum ar fi cetățenii, partidele politice, ONG-urile și, nu în ultimul rând, funcționarii electorali. Astfel de reguli procedurale sunt esențiale pentru a consolida încrederea cetățenilor în securitatea și fiabilitatea sistemelor de vot electronic și în rolul de supraveghere al autorităților electorale. Lipsa divulgării în totalitate sau partial a raportului de certificare sau a tuturor documentelor relevante ar trebui luată în considerare numai în circumstanțe excepționale.

O atenție deosebită trebuie acordată componentelor software care sunt relevante pentru securitatea sistemului. Acest lucru se poate face prin includerea testelor de securitate în planurile de testare, pentru ca cititorul să înțeleagă cum a fost testată securitatea. Etichetarea tuturor documentelor de către statele membre și furnizori poate fi, de asemenea, luată în considerare.

Furnizorii și chiar certificatorii înșiși ar putea să nu fie de acord cu publicarea unei părți sau a celor mai multe părți ale documentației sistemului de vot electronic, deoarece aceștia doresc să protejeze drepturile de proprietate intelectuală. Pentru a evita secretizarea excesivă în timpul proceselor de certificare, potențialii furnizori și certificatorii ar trebui, prin urmare, să fie informați, în timpul procesului de licitație, că părțile interesate trebuie să aibă acces la documente specifice. CND, care împiedică observatorii să publice evaluări și faptele pe care se bazează evaluările fac foarte dificilă efectuarea unei observații semnificative.

În cele din urmă, pentru a supraveghea procesul de certificare sau pentru a compensa divulgarea parțială și incompletă a informațiilor către public, statele membre pot înființa comitete specifice alcătuite din experți, academicieni și/sau politicieni. De exemplu, în Belgia, un colegiu de experți este responsabil pentru supravegherea întregului proces electoral pentru constituirea adunării legislative competente.

27. Sistemul de vot electronic este auditabil. Sistemul de audit trebuie să fie deschis și cuprinzător și să raporteze în mod activ posibilele probleme și amenințări.

a. Sistemul de audit ar trebui să înregistreze orele, evenimentele și acțiunile, inclusiv:

- toate informațiile legate de vot, inclusiv numărul alegătorilor eligibili, numărul voturilor exprimate, numărul voturilor valide și nevalabile, numărarea și renumărarea etc.;
- orice atacuri asupra funcționării sistemului de vot electronic și a infrastructurii sale de comunicații;
- cedări ale sistemului, defecțiuni și alte amenințări la adresa acestuia.

Instrumentele automate și procedurile de sistem ar trebui să permită analizarea și raportarea datelor într-un mod rapid și precis, permițând astfel acțiuni corective rapide. Sistemul de audit trebuie să furnizeze rapoarte verificabile privind:

- controale încrucișate ale datelor;
- atacuri de sistem sau de rețea;
- detectarea și raportarea intruziunilor;
- manipularea de date;
- frauda și tentativele de fraudă.

Sistemul de audit ar trebui să țină evidența atacurilor asupra procesului electoral sau a infrastructurii sale de comunicații. Sistemul trebuie să includă o funcție care detectează și raportează tentative de hacking, intruziune sau manipulare. Detectarea atacurilor asupra sistemului de vot va fi înregistrată, raportată și se va acționa imediat.

Sistemul de audit ar trebui să înregistreze toate conturile și sumele, inclusiv toate deciziile luate, acțiunile întreprinse sau excepțiile făcute în timpul procesului de numărare.

b. Sistemul de vot electronic trebuie să mențină surse de timp sincronizate de încredere. Exactitatea sursei de timp ar trebui să fie suficientă pentru a menține momentele de timp pentru trasee de audit și date de observare, precum și pentru menținerea termenelor pentru înregistrare, nominalizare, votare sau numărare.

Pot exista cerințe diferite de acuratețe pentru diferiții utilizatori ai sursei de timp, cum ar fi toleranțe diferite pentru evenimentul de înregistrare și votare. Acest lucru poate duce la mai multe surse de timp sau la o singură sursă de timp care oferă cea mai mare precizie. Termenul "marcă de timp" este utilizat ca indicație pentru marcarea datelor. Există mai multe mijloace disponibile, în funcție de situație: pot fi necesare ștampile de timp securizate pentru evenimentele critice, în timp ce numerele succesive continue sau păstrarea secvenței pot fi suficiente pentru intrările în jurnal. Rețineți că timbrele de vot pot pune în pericol confidențialitatea votului. Ar trebui să se acorde o atenție deosebită modului în care și dacă acestea ar trebui utilizate în legătură cu buletinele de vot sau voturile.

c. Concluziile trase din procesul de audit ar trebui luate în considerare la viitoarele alegeri electronice.

VIII. Linii directoare pentru implementarea recomandărilor privind fiabilitatea și securitatea sistemului

28. Organismul de management electoral este responsabil pentru respectarea tuturor cerințelor, chiar și în cazul eșecurilor și atacurilor. Organismul de management electoral răspunde de disponibilitatea, fiabilitatea, utilitatea și securitatea sistemului de vot electronic.

a. Disponibilitatea serviciilor de vot electronic pentru toți alegătorii în timpul întregului proces de votare electronică trebuie menținută.

Un sistem de vot electronic trebuie să fie protejat împotriva defecțiunilor și cedării acestuia. Cu toate acestea, posibilitatea unei defecțiuni nu poate fi exclusă în întregime. Trebuie prevăzute proceduri și soluții alternative pentru cazurile de urgență.

b. Alegătorii trebuie să fie informați cu promptitudine prin mijloace adecvate în caz de întrerupere, suspendare sau repornire a sistemului de vot electronic.

c. Sistemul de votare nu poate împiedica alegătorii eligibili să își exercite dreptul de vot.

d. Sistemul de vot electronic ar trebui să mențină disponibilitatea și integritatea voturilor.

Din momentul în care dreptul de vot a fost exercitat, nimeni nu ar trebui să poată citi votul, să îl schimbe sau să divulge opțiunea alegătorului care l-a exprimat. Acest lucru se realizează prin procesul de etanșare a urnei, iar în cazul în care urna de vot este la distanță de alegător, prin închiderea votului pe toată durata transmiterii sale de la alegător la urnă. În anumite circumstanțe, sigilarea trebuie făcută prin criptare.

Pentru a sigila urna de vot, sunt necesare măsuri fizice și organizatorice. Acestea pot include blocarea fizică a urnei și asigurarea că mai mult de o persoană o supraveghează. În cazul unui sistem electronic de vot, sunt necesare măsuri suplimentare, cum ar fi controalele de acces, structurile de autorizare și firewall-urile.

Un vot este încheiat atunci când conținutul său a fost supus măsurilor care garantează că acesta nu poate fi citit, schimbat sau asociat de alegătorul care l-a exprimat.

Protocoalele nivelului de servicii (SLA) stabilesc de obicei ratele de disponibilitate și de eșec. Un anumit nivel de degradare a serviciului poate fi acceptabil în perioadele de eșec, de exemplu când un server dintr-un grup se rupe. În procesele de înregistrare, perioadele scurte de întreruperi ale serviciului sau perioade de întreținere pot fi tolerabile.

Dezvoltatorii de sisteme iau totuși în considerare posibilitatea de a refuza serviciile de atac și ar trebui să documenteze rezerva de urgență în performanța sistemului care a fost desemnată. Testele independente de penetrare pot reduce probabilitatea unei întreruperi deliberate a serviciului.

Serviciile care trebuie păstrate în funcție de disponibilitate depind de etapă - înainte de vot, în timpul votării, post-votare. În etapa de pre-votare trebuie să fie disponibile

nominalizările, procesele și serviciile de înregistrare; în etapa de vot, procesele și serviciile de votare; și în etapa post-votare, procesele și serviciile de numărare și renumărare. Procesele de audit trebuie să fie disponibile în toate etapele. Limitele predefinite pentru SLA, ratele tolerabile de eșec sau degradarea serviciilor pot fi diferite pentru diferitele etape sau servicii.

e. Ar trebui adoptate măsuri tehnice și organizatorice pentru a se asigura că nu se pierd definitiv date în cazul unei defecțiuni sau al unei cedări care afectează sistemul de vot electronic.

f. Statele membre ar trebui să ia în considerare posibilitatea de utilizare pe parcursul dezvoltării mecanismelor de securitate.

Liniile directoare 40e și 40f: Acest lucru nu sugerează faptul că trebuie utilizate toate metodele posibile de protecție disponibile. În fiecare caz, trebuie să se aleagă natura și amploarea măsurilor de protecție care trebuie aplicate. Trebuie stabilit un echilibru adecvat între diferiți factori la fel de importanți, de exemplu, între necesitatea foarte importantă de securitate și oportunitatea de a avea sisteme ușor de utilizat de către alegători. Într-un astfel de caz, gradul de utilizare nu trebuie să depășească necesitatea unor niveluri ridicate de securitate, dar poate fi un factor în determinarea măsurilor de securitate care ar trebui adoptate. Considerații asemănătoare s-ar putea aplica dacă un avantaj de securitate suplimentar foarte mic este realizabil numai la un cost de utilizare excesiv de ridicat.

g. Ar trebui efectuate verificări periodice pentru a se asigura că toate componentele sistemului de vot electronic funcționează în conformitate cu specificațiile tehnice ale sistemului și că serviciile sale sunt disponibile.

h. Echipamentele cheie de votare electronică ar trebui să fie amplasate într-o zonă securizată, iar zona respectivă să fie păstrată pe parcursul perioadei electorale împotriva oricărei interferențe sau acces neautorizate.

i. În perioada alegerilor sau a unui referendum, ar trebui să existe un plan de redresare în caz de avarie.

Liniile directoare 40h și 40i: Pentru securitatea lor, sistemele centrale trebuie să fie instalate în locații sigure, controlate. Accesul fizic ar trebui să fie controlat și restricționat. De asemenea, ar trebui planificată o locație alternativă pentru a putea reacționa după un dezastru fizic, cu echipamentul adecvat pre-rezervat (planificarea de recuperare în caz de avarie).

Autoritățile electorale trebuie să definească un anumit nivel de utilizare înainte de a executa sistemul. Pe baza nivelului dorit de servicii, ar trebui să se facă o analiză a riscurilor și să se stabilească scenarii. Acestea vor implica proceduri, aranjamente de rezervă, rezervări de resurse și așa mai departe.

j. Ar trebui să fie posibilă verificarea stării de protecție a echipamentului de vot în orice moment. Cei responsabili cu echipamentul ar trebui să utilizeze proceduri speciale de

monitorizare pentru a se asigura că în timpul perioadei de votare echipamentul de vot și utilizarea acestuia îndeplinesc cerințele.

k. Ar trebui să existe aranjamente de rezervă suficiente și permanent disponibile pentru a asigura buna desfășurare a votului. Orice sistem de backup ar trebui să respecte aceleași standarde și cerințe ca și sistemul original.

l. Personalul în cauză ar trebui să fie gata să intervină rapid, în conformitate cu o procedură elaborată de autoritățile electorale competente.

i. Persoanele responsabile de exploatarea echipamentului ar trebui să elaboreze o procedură de urgență.

ii. Toate operațiunile tehnice ar trebui să facă obiectul unei proceduri oficiale de control. Orice modificare substanțială a echipamentului cheie trebuie notificată.

Liniile directoare 40j, 40k și 40l: Un sistem electronic de votare are nevoie de proceduri formalizate pentru monitorizarea securității și fiabilității acestuia, pentru rezolvarea problemelor și de resurse adecvate pentru depanarea infrastructurii.

Autoritățile electorale ar trebui să fie conștiente de toate modificările critice aduse sistemului, pentru a anticipa eventualele consecințe și a alege politica adecvată de a comunica astfel de schimbări.

m. Orice date stocate după perioada alegerilor sau a referendumului trebuie păstrate în siguranță.

Toate datele electorale sau ale referendumurilor care trebuie stocate se vor păstra într-un mod sigur. Aceasta înseamnă că vor fi necesare mai multe copii ale datelor pentru mai multe tipuri de suport de informație (hard disk, casete, suporturi optice precum DVD sau microfișe, tastă de memorie USB și imprimare) și ar trebui să fie stocate în locații diferite.

29. Numai persoanele autorizate de organismul de management electoral au acces la infrastructura centrală, serverele și datele electorale. Numirile persoanelor autorizate să gestioneze votarea electronică trebuie să fie clar reglementate.

a. Persoanele numite vor avea acces restricționat la serviciile de votare electronică, în funcție de identitatea lor de utilizator sau de rolul utilizatorilor. Autentificarea utilizatorilor ar trebui să fie eficientă înainte de a putea efectua orice acțiune. Separarea taxelor ar trebui să fie clară și să fie aplicată cu strictețe prin măsuri tehnice.

b. În timp ce se deschide o urnă electronică, orice intervenție autorizată care afectează sistemul ar trebui să fie efectuată de echipe formate din cel puțin două persoane, să facă obiectul unui raport, să fie monitorizată de reprezentanții organismului de management electoral și de către toți observatorii electorali.

c. Orice altă activitate tehnică critică ar trebui să fie efectuată de echipe formate din cel puțin două persoane. Componența echipelor ar trebui modificată în mod regulat. Pe cât posibil, astfel de activități ar trebui să se desfășoare în afara perioadelor electorale. Acestea ar trebui să facă obiectul unui raport.

30. Înainte de efectuarea oricărei alegeri electronice, organismul de management electoral se va asigura că sistemul de vot electronic este autentic și funcționează corect.

a. Înainte de fiecare alegeri, echipamentul trebuie verificat și aprobat în conformitate cu un protocol întocmit de către autoritățile electorale competente. Echipamentul trebuie verificat pentru a se asigura că acesta respectă specificațiile tehnice. Constatările trebuie transmise autorităților electorale competente.

Ar trebui să se facă o distincție clară între verificările efectuate în mod regulat după fiecare alegeri sau referendum și verificările efectuate ori de câte ori sistemul este modificat în orice privință. În primul caz, angajații entității care gestionează sistemul electoral sau referendumul, pot efectua verificarea. Cu toate acestea, în cel de-al doilea caz, un organism extern trebuie să facă verificarea, deoarece verificarea este mai aproape de a fi o procedură de certificare.

31. Ar trebui instituită o procedură pentru instalarea regulată a versiunilor actualizate și corectarea tuturor programelor software relevante.

a. Ar trebui elaborate proceduri formale pentru implementarea software-ului și a configurațiilor tehnologiei votării. Trebuie stabilite termene pentru actualizări. Actualizările distribuite ar trebui autentificate (semnate).

32. Organismul de management electoral se va ocupa de toate materialele criptografice într-un mod securizat.

a. Cheile private criptografice ar trebui să fie generate în cadrul unei întâlniri publice și ar trebui împărțite în părți separate și împărtășite de cel puțin două persoane puțin probabil să colaboreze.

33. În cazurile în care apar incidente care ar putea amenința integritatea sistemului, persoanele responsabile cu exploatarea echipamentului informează imediat organismul de management electoral.

a. Tipurile de incidente sunt specificate în prealabil de autoritățile electorale.

b. În cazul unui incident, autoritățile electorale competente ar trebui să ia măsurile necesare pentru a atenua efectele acestuia.

34. Se mențin autenticitatea, disponibilitatea și integritatea registrelor electorale și a listelor de candidați. Sursa datelor trebuie autentificată. Dispozițiile privind protecția datelor trebuie respectate.

a. Imprimarea datelor de identificare a alegătorilor – spre exemplu, cardurile de vot - ar trebui revizuită pentru a asigura securitatea datelor sensibile.

35. Sistemul de vot electronic identifică voturile care sunt afectate de o neregulă.

a. Faptul că s-a votat în termenele stabilite trebuie să fie verificabil.

Într-un context de vot pe internet, expresia "în termenele prescrise" se referă la termenul limită în care se închide canalul de vot pe internet. Acest lucru poate fi implementat prin utilizarea unor note de timp sau prin confirmarea unui sistem de încredere. Cu toate acestea, o notă de timp atașată la vot nu ar trebui utilizată pentru a dezvălui votul.

ANEXĂ

Definiții

În aceaste linii directoare, se utilizează următorii termeni cu următoarele semnificații:

- controlul accesului: prevenirea utilizării neautorizate a unei resurse;
- evaluarea: o evaluare a persoanelor, hardware-ului, software-ului și procedurilor pentru a verifica dacă acestea sunt adecvate pentru îndeplinirea anumitor sarcini;
- audit: o evaluare independentă pre sau post-electorală a unei persoane, organizații, sistem, proces, entitate, proiect sau produs care include analiza cantitativă și calitativă;
- autentificare: asigurarea identității unei persoane sau date;
- disponibilitate: starea de a fi accesibil și utilizabil la cerere;
- buletinul de vot: mijloacele recunoscute legal prin care alegătorul își poate exprima votul;
- candidat: o opțiune de vot constând dintr-o persoană, un grup de persoane și/sau un partid politic;
- exercitarea votului: introducerea votului în urna de vot;
- certificat: un document care este rezultatul unei certificări oficiale, prin care un fapt este certificat sau atestat;
- certificare: un proces de confirmare a faptului că un sistem de vot electronic este în conformitate cu cerințele și standardele prescrise și că include, cel puțin, dispoziții pentru a se asigura funcționarea corectă a sistemului. Acest lucru se poate realiza prin măsuri precum testări și audit și până la certificări formale. Rezultatul final este un raport și/sau un certificat;
- organism de certificare (sau certificator): o organizație autorizată să efectueze un proces de certificare și să emită un certificat la finalizarea procesului;
- raport de certificare: un document care explică ce se certifică prin certificat și modul în care se certifică;
- lanțul de încredere: un proces în domeniul securității calculatorului, care este stabilit prin validarea fiecărei componente hardware și software de jos în sus. Intenția este să se asigure că pot fi utilizate numai software și hardware de încredere, păstrându-se însă flexibiltatea;
- testarea componentelor: o metodă prin care unitățile individuale ale codului sistemului sunt testate pentru a determina dacă sunt adecvate pentru utilizare;
- confidențialitate: starea care caracterizează informațiile care nu ar trebui să fie puse la dispoziție sau dezvăluite persoanelor, entităților sau proceselor neautorizate;

- mediu controlat: spații supravegheate de funcționari electorali, de ex. secții de votare, ambasade sau consulate;
- alegeri electronice: alegeri politice sau referendum în care se utilizează votul electronic;
- organismul de management electoral: instituția responsabilă de gestionarea alegerilor într-o anumită țară la nivel național sau regional;
- urna de vot electronică: mijloacele electronice prin care sunt stocate voturile în așteptarea numărării;
- vot electronic: vot exprimat electronic;
- votare electronică: utilizarea mijloacelor electronice de exprimare și/sau de numărare a voturilor;
- sistemul de vot electronic: hardware-ul, software-ul și procesele care permit alegătorilor să voteze prin mijloace electronice la alegeri sau referendumuri;
- certificare formală: certificare efectuată de autorități, numai înainte de ziua alegerilor și care conduce la emiterea unui certificat;
- linii directoare: orice document care vizează eficientizarea anumitor procese în conformitate cu o rutină stabilită. Prin definiție, liniile directoare nu sunt obligatorii din punct de vedere juridic;
- acordul de nedivulgare: un contract juridic între două sau mai multe părți care prezintă materiale, cunoștințe sau informații confidențiale, pe care părțile doresc să le împărtășească în anumite scopuri, dar doresc să limiteze accesul părților care nu sunt legate de contract;
- acces liber: accesul online la materialele gratuite pentru citire și, eventual, utilizare (sau refolosire) în anumite limite;
- profil de protecție: un set de cerințe de securitate independente de punerea în aplicare pentru o categorie de produse, care satisface nevoile specifice de securitate ale consumatorilor;
- cerința: o necesitate documentată singulară a ceea ce ar trebui să fie sau să îndeplinească un anumit produs sau serviciu;
- vot electronic de la distanță: utilizarea mijloacelor electronice de a vota în afara locurilor unde are loc votul în general;
- sigilare: protejarea informațiilor astfel încât să nu poată fi utilizate sau interpretate fără ajutorul altor informații sau mijloace, disponibile numai persoanelor sau autorităților autorizate, inclusiv prin criptare;
- persoana interesată: o persoană, grup, organizație sau sistem care are un impact asupra sau poate fi afectată de acțiunile unui guvern sau organizație. Acestea includ cetățeni, oficiali electorali, partide politice, guverne, observatori naționali și

internaționali, mass-media, cadre universitare, ONG-uri, organizații anti-votul electronic și organisme specifice de certificare a votării electronice;

- standard (legal): se referă la dispozițiile din anexa I la Recomandarea CM/Rec(2017)5;
- standard (tehnic): o normă stabilită, de obicei, sub forma unui document formal care prevede criterii inginerești sau tehnice, metode, procese și practici uniforme;
- testarea: procesul de verificare a funcționării sistemului conform așteptărilor;
- vot: exprimarea opțiunii de vot;
- alegător: o persoană care are dreptul de a vota într-un anumit proces electoral sau referendum;
- canalul de vot: modalitatea prin care alegătorul își poate exercita dreptul de vot;
- opțiunile de vot: gama de posibilități dintre care se poate face o alegere prin exercitarea votului în cadrul unui proces electoral sau referendum;
- registrul alegătorilor: o listă a persoanelor cu drept de vot (alegători).