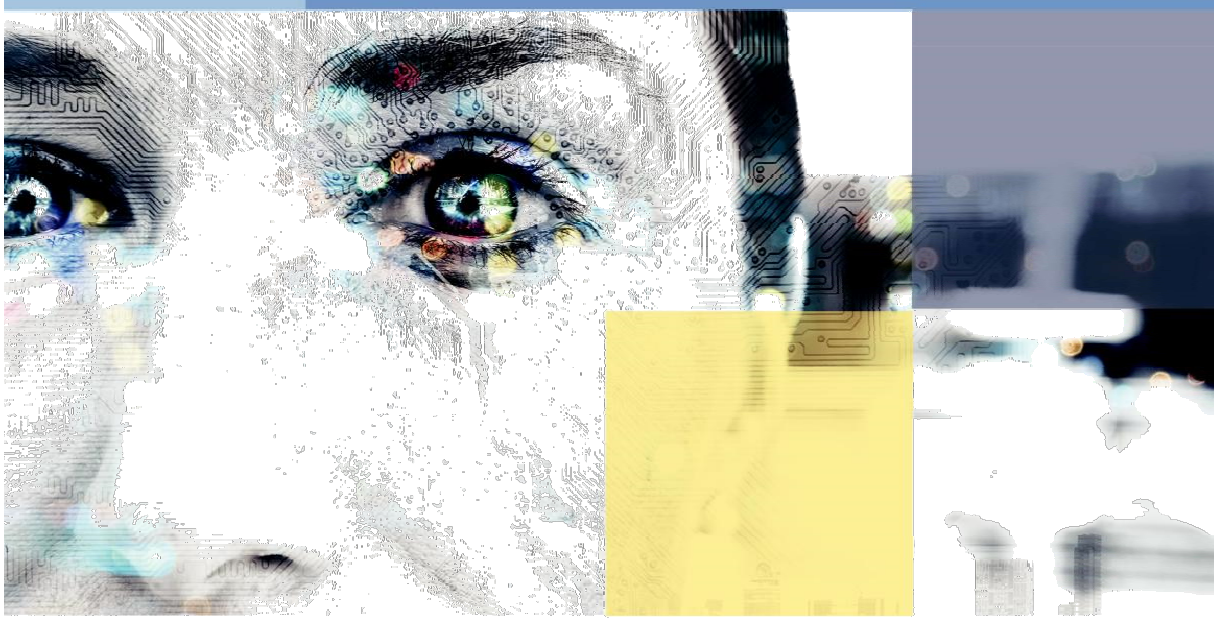
TEHNOLOGIILE DIGITALE ÎN ALEGERI

Întrebări, lecții învățate, perspective



COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

TEHNOLOGIILE DIGITALE ÎN ALEGERI

Întrebări, lecții învățate, perspective

Ardita Driza Maurer

Consiliul Europei

Această publicație este elaborată de Divizia pentru Alegeri și Societate Civilă a Consiliului Europei în cadrul proiectului Consiliului Europei privind „Sprijinirea transparenței, incluziunii și integrității practicii electorale în Ucraina”.

Această publicație conține lucrări originale nepublicate. Opiniile exprimate în prezentul document aparțin autorului şi nu reflectă, în mod necesar, poziția oficială a Consiliului Europei.

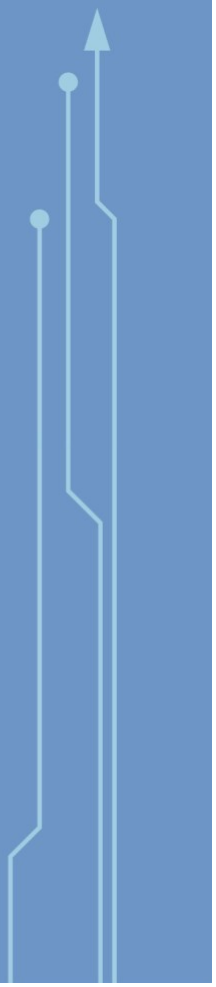
Concept și configurație:
Ganna Vojna

Fotografie de copertă: Shutterstock

Editura Consiliului Europei
F-67075 Strasbourg Cedex
http://book.coe.int

Tipărit la Consiliul Europei

▶ **Dezvoltarea unui cadru de reglementare pentru tehnologiile digitale utilizate în ciclul electoral**	5
▶ **Prezentare generală a tehnologiilor digitale utilizate în ciclul electoral**	39



Dezvoltarea unui cadru de reglementare pentru tehnologiile digitale utilizate în ciclul electoral*

* Prezentul studiu a fost realizat la solicitarea Comisiei Electorale Centrale a Ucrainei cu sprijinul proiectului Consiliului Europei privind „Sprijinirea transparenței, incluziunii și integrității practicii electorale în Ucraina”, implementat în cadrul Planului de acțiuni al Consiliului Europei. pentru Ucraina 2018–2021.

Cuprins

INTRODUCERE	**7**
STANDARDE JURIDICE	**9**
1. Cadrul juridic pentru alegeri	9
a. Instrumente internaționale	9
b. Instrumente naționale	10
2. Cadrul juridic pentru noile tehnologii	12
a. Instrumente internaționale	12
b. Instrumente naționale	14
3. Inspirație din alte domenii	14
ÎNTREBĂRI DE LA ȘI PENTRU AUTORITATEA DE REGLEMENTARE	**15**
1. Identificarea problemei	15
2. Scopuri și obiective	15
3. Beneficii și dezavantaje	16
4. Abordarea „ciclului electoral”	17
5. Abordare multidisciplinară	18
6. O decizie suverană	18
7. Necesitatea, forma și nivelul de reglementare	19
8. Conținutul regulamentului	21
a. Cerințe detaliate	21
b. Centrat pe drepturile omului	21
c. Utilizabilitate	22
d. Protecția datelor	22
e. Transparență	22
f. Securitate cibernetică	23
g. Control, aplicare, răspundere	24
h. Managementul schimbării, resursele și cooperarea cu sectorul privat	25
9. Încredere	25
CONCLUZII	**27**
REFERINȚE SELECTATE	**33**
Texte juridice, ghiduri, evaluări, bune practici internaționale	33
Cercetări relevante privind aspectele juridice și de reglementare	35
Documente relevante din țările selectate	37

INTRODUCERE

Soluțiile digitale sunt deja utilizate în diferite faze ale ciclului electoral de către organele electorale (OE), alegători, partidele politice, justiția electorală, mass-media și altele. Sistemele de informații geografice pentru delimitarea limitelor și stabilirea locației secțiilor de votare, registrele electronice ale alegătorilor, aparatele electronice de votare sau sistemele de vot prin internet, scanerele optice care numără buletinele de vot pe hârtie, soluțiile electronice pentru transmiterea rezultatelor alegerilor de la secțiile de votare către autoritățile centrale, semnarea electronică a cererilor de inițiativă sau referendum, semnarea electronică a listelor de candidați sau a avizului partidelor, sistemele pentru consolidarea și publicarea rezultatelor sau vizualizarea acestora pe zone geografice, metode statistice de evaluare a acurateței rezultatelor și de detectare a potențialelor fraude sunt câteva exemple de soluții digitale utilizate în ciclul electoral. Acestea se bazează pe informații digitizate. Alte tehnologii digitale utilizate sau avute în vedere includ biometria, blockchain, cloud computing *(informatica dematerializată)*, inteligența artificială etc.

Soluțiile digitale pentru alegeri trebuie să respecte principiile aplicabile pentru alegerile democratice. Cu toate acestea, aplicarea practică a principiilor juridice la tehnologiile digitale nu este ușoară. Prima dificultate constă în caracterul general al principiilor juridice care sunt formulate în termeni generali și largi. Aplicarea acestora într-un context specific necesită o interpretare care trebuie să clarifice sensul exact și implicațiile practice care decurg din principii. A doua dificultate majoră constă în natura tehnică a soluțiilor digitale, a căror configurație internă și funcționare pot fi înțelese doar de o mână de specialiști, dar nu și de nespecialiști fără ajutor tehnic. Cu toate acestea, nespecialistul (alegător, administrator electoral, judecător, observatori etc.) este cel care trebuie să utilizeze, să verifice și, în cele din urmă, să aibă încredere în soluția digitală și în rezultatele pe care le produce.

Reglementarea utilizării soluțiilor digitale înseamnă, în mare, două lucruri. În primă instanță, este necesar să se concretizeze principiile pentru alegerile democratice și anume să se clarifice sensul acestora și să se extragă cerințele care se aplică contextului respectiv. Al doilea pas este transpunerea acestor cerințe juridice în prevederi care reglementează configurarea, utilizarea și controlul soluției digitale. Reglementarea trebuie să asigure că utilizarea soluțiilor digitale este reglementată suficient pentru a garanta respectarea principiilor de nivel superior.

Reglementarea este importantă pentru cei care creează soluții digitale, cei care decid să le introducă, cei care le utilizează, le monitorizează și le controlează etc. Aceștia ar putea fi persoana care lucrează la secția de votare, alegătorul, observatorii, administrația centrală a rezultatelor votului etc. Prin urmare, este important să existe un cadru de reglementare bun, astfel încât drepturile, obligațiile, competențele etc. tuturor celor implicați să le fie clare. În cele din urmă, reglementarea este importantă pentru a se asigura că alegerile sunt libere, corecte și democratice.

Consiliul Europei și statele sale membre discută cu privire la utilizarea tehnologiilor digitale în alegeri de douăzeci de ani. Votul electronic și numărarea electronică au fost în centrul acestei preocupări. Consiliul Europei a adoptat prima recomandare privind votul electronic în 2004 și a actualizat-o în 2017,1 extinzând definiția votului electronic pentru a include și numărarea electronică a buletinelor de vot pe hârtie. Cu toate acestea, alte soluții digitale utilizate în timpul ciclului electoral, cum ar fi registrele electronice, soluțiile pentru informarea alegătorilor, tabularea voturilor, transmiterea rezultatelor etc., nu sunt acoperite de Recomandarea Comitetului de Miniștri al Consiliului Europei CM/Rec(2017)5 privind standardele pentru votul electronic.

În alineatele următoare, oferim o prezentare generală a instrumentelor juridice internaționale relevante și câteva întrebări pe care legiuitorul sau autoritatea de reglementare trebuie să le ia în considerare atunci când se confruntă cu introducerea soluțiilor digitale în cadrul alegerilor. Accentul este pus pe principiile directoare, bunele practici și lecțiile învățate.

Două observații preliminare: în primul rând, procesele electorale și politice sunt specifice fiecărei țări și sunt influențate de specificități istorice, geografice, culturale și de altă natură. Aceasta înseamnă că o soluție găsită a fi de succes într-un loc, poate să nu fie pusă în aplicare în același mod și/sau să nu aibă succes în altă parte. Cu toate acestea, soluțiile digitale au, de asemenea, caracteristici tehnice comune, independent de context. Această lucrare se concentrează pe aceste trăsături comune și, ca atare, concluziile generale prezentate aici trebuie să fie valabile în toate locurile.

În al doilea rând, îndrumările existente privind votul electronic se pot aplica altor soluții digitale utilizate în alegeri, votul fiind cel mai complex și mai sensibil pas în cadrul unui scrutin. Într-adevăr, această lucrare se va referi adesea la experiențe de vot electronic. Această lucrare aduce însă câteva noutăți, în comparație cu documentele existente privind votul electronic: ia în considerare toate soluțiile digitale și nu se limitează la votul electronic și, în plus, include și câteva lecții învățate din experiențele recente în domeniul votului electronic, și anume privind transparența și verificarea, care nu au fost încă reflectate în instrumentele de ghidare pentru votul electronic. De remarcat faptul că, Consiliul Europei lucrează, în prezent, la posibile orientări privind utilizarea tehnologiilor digitale în alegeri, în conformitate cu principiile convenționale pentru alegerile democratice.2

---

1. Recomandarea anterioară a Comitetului de Miniștri al Consiliului Europei Rec(2004)11 privind standardele juridice, operaționale și tehnice pentru votul electronic și Ghidurile asociate privind certificarea și transparența. Acestea au fost înlocuite de Recomandarea CM/Rec(2017)5 privind standardele pentru votul electronic și Ghidurile de punere în aplicare asociate.

2. A se vedea lucrările Consiliului Europei/Comitetului European pentru Democrație și Guvernare (CEDG) privind orientările referitoare la utilizarea tehnologiilor digitale pe tot parcursul ciclului electoral, cu excepția fazei de vot, care este deja abordată de Recomandarea Comitetului de Miniștri al Consiliului of Europe CM/Rec(2017)5, campania
electorală (rețele sociale, informare, dezinformare) și problemele de finanțare care sunt abordate de alte inițiative.

Această contribuție se concentrează pe aplicarea principiilor alegerilor democratice libere și corecte. Trebuie luate în considerare, de asemenea, și alte principii relevante pentru alegeri, cum ar fi libertatea de opinie și de exprimare, libertatea de întrunire pașnică, libertatea de asociere, libertatea de mișcare, libertatea de a nu fi discriminat, dreptul la o cale de atac efectivă. Totuși, acestea nu vor fi discutate aici.

Instrumentele internaționale și naționale care reglementează alegerile, precum și tehnologiile digitale sunt relevante atunci când se ia în considerare reglementarea soluțiilor digitale utilizate în alegeri.

1. Cadrul juridic pentru alegeri

a. Instrumente internaționale

Dreptul internațional obligatoriu include articolul 21 din Declarația Universală a Drepturilor Omului (DUDO) a Națiunilor Unite din 1948,3 articolul 25 din Pactul internațional al ONU privind drepturile civile și politice din 1966 (denumit în continuare – PIDCP) și articolul 3 din Protocolul Nr. 1 la Convenția pentru Protecția Drepturilor Omului și a Libertăților Fundamentale (denumit în continuare – Articolul 3 din Protocolul nr. 1 la Convenție), astfel cum este interpretat de Curtea Europeană a Drepturilor Omului. Aceste instrumente sunt obligatorii în țările care le-au ratificat.4 Carta Drepturilor Fundamentale a Uniunii Europene conține drepturi similare și se aplică țărilor UE.

Interpretările autorizate ale instrumentelor menționate mai sus, alte angajamente politice și principii ale așa-numitei moșteniri electorale europene fac, în egală măsură, parte din cadrul juridic internațional pentru alegeri. Aceasta include, în special, Comentariul General 25 al PIDCP, jurisprudența Curții Europene a Drepturilor Omului cu privire la articolul 3 din Protocolul nr. 1 la Convenție, Documentul de la Copenhaga din 1990 al Conferinței pentru Securitate și Cooperare în Europa (CSCE) și alte angajamente privind alegerile, Codul de bune practici în materie electorală din 2002 și Codul de bune practici privind referendumurile din 2007 al Comisiei Europene pentru Democrație prin Drept (Comisia de la Veneția) a Consiliului Europei.

Studiile și evaluările autorizate ale alegerilor și ale cadrelor de reglementare pentru alegeri oferă, de asemenea, îndrumări, cu condiția să se țină seama, în mod corespunzător, de particularitățile cazului care este evaluat și măsura în care recomandările se pot aplica în altă parte. De exemplu, rapoartele de monitorizare a alegerilor ale OSCE/OIDDO (Oficiul pentru Instituții Democratice

3. DUDO nu este un tratat; cu toate acestea, prevederile sale sunt universal acceptate și considerate a fi drept internațional cutumiar.

4. Toate statele membre ale Consiliului Europei au ratificat Pactul internațional al ONU privind drepturile civile și politice; unele au introdus limitări (de exemplu, Elveția cu privire la secretul votului/articolul 25 PIDCP). 45 din 47 de state membre ale Consiliului Europei au ratificat Protocolul nr. 1 la Convenție. Elveția și Monaco l-au semnat, dar nu l-au ratificat până în prezent. Cu toate acestea, cu excepția lipsei caracterului secret, o caracteristică acceptată a votului adunării în Elveția (votul prin ridicarea mâinii), toate celelalte elemente ale dreptului elvețian sunt mai stricte și mai ample în comparație cu articolul 3 din Protocolul nr. 1 la Convenție. Acest lucru este, de obicei, așa și în alte țări. Prevederile internaționale oferă, de obicei, standarde minime care sunt respectate și depășite de legile naționale.

și Drepturile Omului al Organizației pentru Securitate și Cooperare în Europa), APCE (Adunarea Parlamentară a Consiliului Europei) etc., și evaluările comune OSCE/OIDDO – Comisia de la Veneția ale cadrelor de reglementare electorală, în special, cele care abordează utilizarea tehnologiilor digitale în alegeri, sunt de interes. Alte studii, cum ar fi Ghidurile OSCE/OIDDO 2013 pentru revizuirea unui cadru juridic pentru alegeri și îndrumările OSCE/OIDDO privind observarea și evaluarea soluțiilor digitale utilizate în alegeri (inclusiv reglementarea acestora), sunt de interes pentru autoritatea de reglementare. Aceste documente oferă indicii valoroase; cu toate acestea, ele nu oferă îndrumări cuprinzătoare cu privire la modul de reglementare a utilizării tehnologiilor digitale în alegeri.

Consiliul Europei a realizat o activitate de pionierat în ceea ce privește reglementarea tehnologiilor digitale utilizate pentru vot și numărare. Acesta a adoptat prima recomandare în 2004, care a fost apoi înlocuită de Recomandarea Comitetului de Miniștri al Consiliului Europei CM/Rec(2017)5 privind standardele pentru votul electronic. Acesta este singurul instrument internațional care oferă îndrumări cu privire la modul de transpunere a principiilor patrimoniului electoral european în cerințe pentru sistemele de vot electronic. Principiile includ sufragiul universal, egal, liber, secret și direct, organizarea alegerilor la intervale regulate, respectarea drepturilor fundamentale, nivelurile de reglementare și stabilitatea legii electorale și garanțiile procedurale. Recomandarea CM/Rec(2017)5 conține 49 de standarde, și anume cerințe detaliate (Anexa 1) care se aplică tuturor tipurilor de vot electronic și numărare electronică. Acestea sunt explicate în Expunerea de motive a Recomandării. Orientările de punere în aplicare se găsesc în Ghidurile asociate pentru punerea în aplicare a Recomandării CM/Rec(2017)5. Deși recomandarea se referă doar la votul electronic și la numărarea electronică, standardele acesteia pot fi avute în vedere atunci când se iau în considerare alte soluții digitale.

b. Instrumente naționale

Reglementarea alegerilor este o prerogativă națională. Principiile de nivel superior care guvernează alegerile se regăsesc în Constituția națională și/sau în legea electorală națională. Acestea îmbrățișează și dezvoltă principii internaționale. Cerințele detaliate se găsesc de obicei în reglementările de nivel inferior. Alegerile pentru Parlamentul European sunt reglementate suplimentar de Legea europeană privind alegerea membrilor Parlamentului European prin sufragiu universal direct. În unele țări, alegerile locale pot fi reglementate la nivel local. Cu toate acestea, în ceea ce privește alegerile democratice libere și corecte, toate cadrele juridice (supranaționale, naționale și locale) încorporează cel puțin toate principiile de nivel superior ale instrumentelor internaționale menționate mai sus (PIDCP și articolul 3 din Protocolul nr. 1 la Convenție) .

Principiile de nivel superior ale alegerilor democratice au fost introduse treptat în legislațiile și practicile naționale în secolul al XIX-lea, atunci când democrația bazată pe participarea cetățenilor, așa cum o cunoaștem astăzi, a început să se dezvolte în urma revoluțiilor americană și franceză.5 Tehnologia (de nivel redus și înalt) a însoțit aceste evoluții. Introducerea votului australian la mijlocul secolului al XIX-lea a venit ca o reacție la extinderea dreptului de sufragiu la masele de alegători: votul deschis nu mai era tolerabil, deoarece putea și implica o influență nejustificată.6

Aparatele mecanice de vot fuseseră deja introduse în secolul al XIX-lea, urmate de calculatoarele electronice în anii 1960, introducerea aparatelor electronice de vot cu înregistrare directă (DRE) în anii 1990 și votul prin internet în anii de după 2000.7 Mai întâi mecanizarea, apoi tehnologia de calcul au însoțit și susținut mai multe reforme legale: combaterea fraudei8, promovarea egalității alegătorilor, acordarea dreptului de vot, eforturile de a facilita votul și eforturile de creștere a participării.

La nivel național, au existat în principal, două valuri de reglementare privind tehnologiile utilizate în alegeri. Inițial, au fost introduse reglementări privind tehnologia simplă *(low-tech)* (hârtie și soluții mecanice), și anume în anii ’60 și ’70 în Germania, Olanda și Franța. Ulterior, aceste reglementări au fost „actualizate” pentru a guverna soluțiile digitale, în principal, utilizarea dispozitivelor de vot electronic sau de numărare electronică, în anii 1990. Țările care au optat pentru votul prin internet au elaborat noi reglementări dedicate, bazate, totuși, pe analogii cu sistemele existente pe hârtie, și anume votul prin poștă (de exemplu, Elveția sau Estonia, începutul anului 2000).

În ciuda faptului că sunt destul de detaliate în comparație cu reglementarea votului pe hârtie sau mecanic, reglementările privind dispozitivele de vot din Germania, Olanda și Franța s-au dovedit a încălca principiile constituționale. Punctul de referință (cel care constituie reglementarea conformă) este definit de legiuitor, judecătorul constituțional sau autoritate de reglementare și, uneori, nu este clar definit. În plus, definițiile variază. În unele țări, criteriul de referință a fost de așa natură încât reglementările nu au putut fi actualizate și dispozitivele de vot au fost ulterior suspendate (Germania, Olanda). În altă parte, utilizarea dispozitivelor de vot a fost redusă drastic (Franța), deoarece reglementarea existentă este nesatisfăcătoare. În alte țări, actualizările de reglementare au introdus modificări semnificative, permițând dispozitivelor de vot să rămână în uz (Belgia, introducerea VVPAT - pistă de audit pe hârtie verificată de alegător).

Reglementările privind votul pe internet au evoluat chiar mai rapid. În Austria, regulamentul a fost considerat a încălca Constituția, deoarece nu a fost suficient de detaliat pentru a permite comisarilor electorali să își desfășoare sarcinile fără asistență tehnică. Deoarece regulamentul menționat nu a fost și nu a putut fi actualizat pentru a satisface cerința constituțională, astfel încât votul prin internet nu poate fi avut în vedere în Austria. În Elveția, evaluarea fazei îndelungate de experimentare și a regulamentului de primă generație introdus în 2002 a condus

---

5. *Encyclopædia Britannica:* Există o relație directă între dimensiunea unui electorat și formalizarea și standardizarea practicilor de vot ale acestuia.
6. *Encyclopædia Britannica:* Buletinul de vot australian, numit și vot secret, este un sistem de vot în care alegătorii își marchează alegerile în intimitate pe buletinele de vot uniforme tipărite și distribuite de guvern sau își desemnează alegerile prin alte mijloace secrete. Acesta a fost introdus inițial în Australia și s-a răspândit în Europa și Statele Unite pentru a satisface cererea în creștere a publicului și a parlamentului, pentru protecția alegătorilor.
7. Această tendință nu a fost și nu este specifică alegerilor. De la Revoluția Industrială de la sfârșitul secolului al XVIII-lea și începutul secolului al XIX-lea, tehnologia a impulsionat creșterea și a transformat economiile.
8. Frauda a fost destul de extinsă mai ales în secolul al XIX-lea și prima jumătate a secolului al XX-lea. În SUA, de exemplu, unde jurisdicțiile corupte au rezistat introducerii dispozitivelor de vot. A se vedea, de exemplu, *Broken Ballots 2012 - Will Your Vote Count? (Voturi viciate - va conta votul tău)* de Douglas W. Jones și Barbara Simon

la actualizări importante, în 2013, ale cadrului de reglementare. Regulamentul de a doua generație introduce noutăți care reflectă o mai bună înțelegere a tehnologiilor digitale: politica de risc, cerințe de verificabilitate, controale ample din partea organismelor independente și experte, cerințe mai stricte de protecție a datelor și transparență etc. Recomandarea Consiliului Europei privind votul electronic a urmat o cale similară și la fel și reglementarea din Estonia. Experiențele recente cu aplicarea noilor reglementări (Elveția, Estonia) arată că acestea trebuie încă să evolueze pentru a aborda mai bine verificabilitatea sau transparența. O astfel de dinamică este de interes atunci când avem în vedere reglementarea și a altor soluții digitale.

Jurisprudența din cele mai înalte instanțe naționale a jucat un rol important în clarificarea sensului practic al principiilor electorale astfel cum sunt aplicate soluțiilor digitale. Multe discutate au fost deciziile Curții Constituționale a Germaniei (2009) sau a Austriei (2011). Jurisprudența arată importanța interpretării în traducerea principiilor în cerințe detaliate pentru tehnologii și a contribuit la construirea unui consens global asupra necesității unei reglementări detaliate a tehnologiilor digitale. Aceasta arată că aceleași principii pot fi interpretate în moduri foarte diferite și pot duce la rezultate diferite în funcție de specificitățile faptice, istorice și culturale. Acest tip de interpretare nu trebuie lăsată în seama tehnicienilor sau furnizorilor de tehnologie, ci trebuie făcută de legiuitor/autoritatea de reglementare.

În comparație cu votul electronic, alte utilizări ale soluțiilor digitale în alegeri au fost subreglementate până acum. Totuși, există o tot mai mare conștientizare a faptului că acest lucru trebuie să se schimbe, deoarece acestea joacă un rol în integritatea alegerilor. Studiile și rapoartele care evaluează înființarea și utilizarea soluțiilor digitale la nivel național sunt de interes pentru autoritatea de reglementare.

2. Cadrul juridic pentru noile tehnologii

a. Instrumente internaționale

Instrumentele juridice care abordează tehnologiile digitale pot fi foarte relevante, deși acestea nu abordează, în mod specific, alegerile. De exemplu, Convenția privind criminalitatea informatică a Consiliului Europei (Convenția de la Budapesta) servește drept ghid pentru orice țară care dezvoltă o legislație națională cuprinzătoare împotriva criminalității cibernetice și drept cadru pentru cooperarea internațională între statele părți la acest tratat. O notă orientativă privind ingerința electorală explică modul în care Convenția de la Budapesta se poate aplica aspectelor privind imixtiunea în alegerile electorale prin intermediul sistemelor informatice. Convenția privind criminalitatea informatică incriminează mai multe tipuri de conduită, și anume, presupuse infracțiuni îndreptate împotriva alegerilor. Competențele sale procedurale și dispozițiile privind asistența juridică reciprocă sunt relevante atunci când se investighează și se procedează împotriva ingerinței electorale.

Instrumentele de protecție a datelor, și anume, Convenția modernizată a Consiliului Europei pentru protecția persoanelor în ceea ce privește prelucrarea

automatizată a datelor cu caracter personal (Convenția 108+) și instrumentul de referință al UE, Regulamentul (UE) 2016/679, Regulamentul general privind protecția datelor (RGPD)9 sunt relevante. Convenția 108+ a Consiliului Europei și RGPD au fost elaborate în paralel și sunt consecvente una cu cealaltă. Un document de orientare al Comisiei Europene explică aplicarea RGPD în context electoral. Cu toate acestea, majoritatea datelor utilizate în alegeri sunt date calificate a căror prelucrare poate fi permisă numai dacă sunt consacrate prin lege garanții adecvate. Aceasta înseamnă că protecția datelor electorale trebuie să fie acoperită de reglementări specifice alegerilor, care sunt mai stricte decât instrumentele de protecție a datelor.

Legislația supranațională (UE) privind securitatea cibernetică este în curs de elaborare. Adoptată de Parlamentul European în iulie 2016, Directiva privind securitatea rețelelor și a sistemelor informatice (Directiva NIS) este prima parte a legislației la nivelul UE privind securitatea cibernetică. Aceasta oferă măsuri juridice pentru creșterea nivelului general de securitate cibernetică în UE, impunând statelor membre să fie echipate corespunzător și să înființeze un grup de cooperare care să sprijine și să faciliteze cooperarea strategică în ceea ce privește incidentele de securitate cibernetică și să facă schimb de informații referitoare la riscuri și prin promovarea unei culturi a securității în sectoarele vitale pentru economie și societate. În urma directivei, în 2019 a fost adoptată o Lege a UE privind securitatea cibernetică care introduce, pentru prima dată, un cadru de certificare a securității cibernetice la nivelul UE pentru produsele, serviciile și procesele TIC.

Mai recent (mai ales din 2016), s-a pus accent pe securitatea cibernetică a soluțiilor digitale utilizate în alegeri și aplicarea concretă a instrumentelor internaționale privind protecția datelor sau securitatea cibernetică la acestea. Comisia Europeană a elaborat ghiduri privind aplicarea legii Uniunii Europene privind protecția datelor (RGPD) în context electoral.10 Activitatea nivelul UE privind securitatea cibernetică a tehnologiei electorale au dus la un Compendiu privind securitatea cibernetică a tehnologiei electorale, care vizează partajarea de experiențe și oferirea de îndrumări, precum și o prezentare generală a instrumentelor, tehnicilor și protocoalelor pentru a detecta, preveni și atenua amenințările cibernetice. Comitetul Convenției privind criminalitatea informatică a Consiliului Europei (T-CY) a elaborat ghiduri privind aplicarea Convenției de la Budapesta la ingerința electorală prin intermediul sistemelor informatice. Alte documente de interes oferă o imagine de ansamblu asupra modului în care diferite țări abordează astfel de probleme și identifică bunele practici (de exemplu, Institutul Internațional pentru Democrație și Asistență Electorală/IDEA, Securitatea cibernetică în alegeri și modele de colaborare interagenții, 2019).

b. Instrumente naționale

9. Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului (Regulamentul general privind protecția datelor), care a devenit direct aplicabil în întreaga Uniune Europeană la 25 mai 2018. Potrivit Comisiei Europene, aceasta oferă Uniunii Europene instrumentele necesare pentru a aborda cazurile de utilizare ilegală a datelor cu caracter personal în context electoral.

10. Comisia Europeană, Alegeri libere și corecte ─ Document de orientare. Ghiduri ale Comisiei privind aplicarea legislației Uniunii în domeniul protecției datelor în context electoral. O contribuție a Comisiei Europene la reuniunea liderilor de la Salzburg din 19-20 septembrie 2018 (COM(2018) 638 final).

În mod similar, legile naționale privind protecția datelor, transparența, securitatea cibernetică, identitatea electronică, gestionarea registrelor etc. se aplică soluțiilor digitale utilizate în alegeri, chiar dacă aceste legi nu se referă, în mod specific, la alegeri și dacă nu există o regulă specifică în cadrul legislativ electoral privind aceleași probleme (lex specialis) care au prioritate.

Reglementările naționale privind securitatea cibernetică sau protecția împotriva criminalității informatice sunt aliniate la instrumentele internaționale. Sunt identificate bune practici pentru securitatea cibernetică a tehnologiei electorale (de exemplu, Compendiul UE menționat privind securitatea cibernetică a tehnologiei electorale, publicat inițial în martie 2018) și se așteaptă ca acestea să contribuie la armonizarea, în continuare, a practicii naționale în aceste domenii.

3. Inspirație din alte domenii

Digitalizarea afectează toate domeniile vieții. Aceasta perturbă, înlocuind modalitățile anterioare de a face lucrurile și punând la îndoială abilitățile și abordările mai vechi. Dreptul și alte domenii sunt sub presiune. Este interesant de observat modul în care alte sectoare, de exemplu, sistemele critice similare cu alegerile, abordează provocarea.

Se poate observa o abordare fragmentată a aplicabilității legii pe internet, cu accent pe respectarea protecției datelor, sau a securității cibernetice etc.11. Totuși, în domeniul alegerilor, se admite că, pentru toate aceste aspecte trebuie să se aplice standarde mai stricte, iar astfel de standarde trebuie stabilite în regulamentul electoral dedicat. Așadar, la alegeri, există șansa ca abordarea să fie mai puțin fragmentată.

Protecția drepturilor fundamentale în context digital este o preocupare comună. Desigur, aplicarea drepturilor fundamentale la tehnologiile digitale trebuie consolidată pentru a contracara tendințele de eroziune. Nu sunt necesare noi dispoziții constituționale care să abordeze tehnologiile digitale, dar există o necesitate ridicată privind aplicarea eficientă a dispozițiilor constituționale existente la tehnologiile digitale. Marea provocare este cum trebuie realizat acest lucru. Aceasta este într-adevăr provocarea pentru legiuitor în cazul reglementării soluțiilor digitale în alegeri.

Ca exemplu, ne putem referi la sistemul de sănătate, care a preluat și utilizează multe soluții digitale. Acesta este un sistem critic pentru societate. În multe țări, experiența poate fi rezumată după cum urmează: „Am văzut o serie de soluții DHT [tehnologie digitală de sănătate] ieșite pe piață în ultimii ani. Unele au fost bune și altele nu atât de bune, dar aspectul cu care ne-am luptat cu adevărat este definirea unui standard comun cu privire la cum arată binele”.12 Această observație poate fi făcută și în domeniul electoral. Răspunsul trebuie găsit în cadrul de reglementare pentru soluțiile digitale în alegeri.

---

11. În loc de multe, a se vedea Udo di Fabio, *Grundrechtsgeltung in digitalen Systemen, 2016*

12. Sistemul Național de Sănătate din Regatul Unit, Cum evaluăm aplicațiile de sănătate și instrumentele digitale, https://digital.nhs.uk/services/nhs-apps-library/guidance-for-health-app-developers-commissioners-and-assessors/how-we-assess-health-apps-and-dig-ital-tools#top

ÎNTREBĂRI DE LA ȘI PENTRU AUTORITATEA DE REGLEMENTARE

Atunci când are în vedere soluțiile digitale care să înlocuiască, să completeze sau să amplifice soluțiile low-tech *(tehnologia simplă)* existente utilizate în alegeri, legiuitorul13 se confruntă cu întrebări care se regăsesc la răscrucea dintre legislația electorală și tehnologiile digitale. Următoarele se bazează pe documentele revizuite (a se vedea Referințele de mai jos).

1. Identificarea problemei

Inovațiile digitale pot fi introduse cel mai bine ca o soluție la problemele existente, nu ca un scop în sine. Identificarea clară a problemei care trebuie rezolvată este primul pas către găsirea unei soluții adecvate. „Problema" este diferența dintre situația existentă și cea dorită. Poate fi o problemă identificată care trebuie corectată, un potențial câștig în eficiență sau îmbunătățirea realizării unor principii de nivel superior.

Identificarea problemei „originale" este utilă pentru a o distinge de problemele ulterioare care pot apărea din utilizarea tehnologiei digitale și pentru a cântări drepturile concurente. O parte a identificării „problemei" este identificarea celor afectați de aceasta sau interesați să o rezolve și așteptările acestora. Aceștia pot fi alegătorii (de exemplu, expatriați, cu deficiențe de vedere etc.), administrația electorală, concurenții politici etc. Orice inovație în ciclul electoral trebuie să țină cont de interesele prezente. Propunerile de soluții digitale trebuie să se bazeze pe cercetarea problemei și așteptările utilizatorilor.

După identificarea problemei și înainte de a se alege o soluție, este necesar să se evalueze eficiența soluțiilor existente și a celor potențiale pentru a realiza alegeri libere, corecte și democratice. Este important ca astfel de evaluări să fie distribuite pe scară largă.

2. Scopuri și obiective

Următorul pas este identificarea situației dorite și stabilirea obiectivelor în vederea obținerii scopului respectiv. Obiectivele (cele cantitative și calitative) vor fi criteriile de evaluare a soluției. Scopul și obiectivele trebuie să fie „neutre din punct de vedere al soluțiilor". Experiența sugerează că trebuie evitat să se pornească de la o idee clară a soluției atunci când sunt definite scopurile și obiectivele. În plus, scopurile și obiectivele trebuie să fie consensuale.

Pe baza acestui lucru, următorul pas este identificarea potențialelor soluții. Trebuie avute în vedere toate soluțiile posibile în scopul găsirii celor care contribuie mai bine la întărirea principiilor constituționale. Experiența arată că este posibil ca soluțiile digitale să nu fie cea mai bună opțiune în toate cazurile. Analiza beneficiilor și riscurilor acestora este

13. În prezenta lucrare, Folosim termenul „legiuitor" (de obicei Parlamentul) sau „autoritatea de reglementare" (de obicei, Guvernul sau unitățile sale) ca sinonime

următorul pas important. De exemplu, un grup de lucru al Ministerului Justiției din Finlanda a concluzionat că votul online nu trebuie introdus în alegerile generale, deoarece riscurile acestuia sunt mai mari decât beneficiile sale. Deși fezabilă din punct de vedere tehnic, tehnologia a fost considerată „a nu fi încă la un nivel suficient de înalt pentru a îndeplini toate cerințele", referindu-se la reconcilierea dintre verificabilitate și confidențialitate.

3. Beneficii și dezavantaje

Pentru a evalua oportunitatea de a introduce o soluție avută în vedere, legiuitorul trebuie să ia în considerare atât avantajele, cât și dezavantajele acesteia. De regulă, legiuitorul primește informații cu privire la aceste aspecte din partea inițiatorului regulamentului și poate consulta, de asemenea, și alți experți.

Unele beneficii privesc administrația electorală, altele pot viza alegătorii sau, mai general, întregul sistem. Din perspectiva administrării alegerilor, soluțiile digitale pot oferi rezultate mai rapide, implica un risc redus de greșeli, facilita interacțiunile și schimbul de informații în timp real sau îmbunătăți controalele registrelor prin furnizarea de mecanisme eficiente de identificare a intrărilor duplicate. Pot fi subliniate eficiența și rentabilitatea. Beneficiile nu sunt percepute în același mod în diferite țări. De exemplu, tehnologia mobilă care permite anunțarea mai devreme a rezultatelor alegerilor poate fi considerată foarte benefică în țările în care ajută la dispersarea tensiunii în alegerile strâns contestate, în timp ce este considerată mai puțin crucială în alte locuri cu o cultură politică mai puțin conflictuală.

Din perspectiva alegătorului sau una democratică, soluțiile digitale pot oferi avantaje în ceea ce privește disponibilitatea (înregistrare online, vot la distanță), independență (de exemplu, unele voturi electronice pot oferi persoanelor cu dizabilități o oportunitate pe care altfel nu ar fi avut-o în cazul în care ar fi trebuit să voteze confidențial), prin prevenirea greșelilor involuntare la completarea buletinelor de vot etc. Introducerea tehnologiilor de dragul de a părea moderni în fața electoratului nu este recomandat.

Legiuitorul trebuie să poată obține o opinie informată cu privire la beneficiile reale. Unele dintre acestea pot fi măsurate deja înainte de introducere (de exemplu, eficiența, viteza, lipsa erorilor, transparența etc.). Altele sunt mai ipotetice și imposibil de măsurat până când soluția este pusă în uz, în mod efectiv (de exemplu, creșterea participării, creșterea încrederii alegătorilor). Având în vedere acest lucru, legiuitorul poate avea în vedere mecanisme de evaluare periodică a beneficiilor și dezavantajelor după introducerea soluției și reevaluarea periodică a acestor soluții.

Trebuie să aibă loc o dezbatere semnificativă înainte de a se lua decizia de a introduce tehnologia digitală în alegeri. Principalele provocări trebuie să fie discutate]n mod deschis. Provocările includ utilizarea durabilă și rentabilă a tehnologiei. Costurile relativ mari de întreținere ale mașinilor și actualizarea software-ului reprezintă o problemă care a fost raportată de mai multe țări.

În plus, securitatea cibernetică devine o provocare importantă. Este esențială monitorizarea rezistenței acestor sisteme digitale la amenințările cibernetice pentru a preveni

ingerință nejustificată sau frauda în alegeri. Soluțiile digitale trebuie actualizate]n mod periodic. Personalul instruit și calificat trebuie să fie disponibil și la îndemână. Sunt posibile situații în care sunt necesare resurse financiare și umane din ce în ce mai mari pentru a menține un mediu electoral acceptabil din punct de vedere constituțional, în special pentru soluții digitale accesibile prin internet, cum ar fi votul la distanță. Costurile de testare periodică a sistemelor sau cele aferente depozitării și reînnoirii echipamentelor sau nevoii de personal calificat sunt elemente importante care trebuie luate în considerare.

Tehnologia poate ajuta la îmbunătățirea proceselor electorale; cu toate acestea, primii care adoptă această tehnologie raportează, de asemenea, o complexitate mai ridicată ca urmare a introducerii TIC. De exemplu, planificarea ciclurilor electorale devine mai complexă. Pe măsură ce costurile de organizare a alegerilor cresc, la fel crește și acordarea de contracte semnificative firmelor din sectorul privat, adesea internaționale. Posibila dependență de soluțiile din sectorul privat este un dezavantaj major care trebuie dezbătut de legiuitor.

Impactul potențialelor eșecuri ale soluțiilor digitale asupra integrității alegerilor este încă o problemă de îngrijorare. Un impact negativ major asupra ciclului electoral poate fi obținut, în principiu, cu un efort relativ mic prin compromiterea soluțiilor digitale. În același timp, pot fi avute în vedere soluții inovatoare care să contribuie la contracararea acestor riscuri. Legiuitorul trebuie să înțeleagă bine respectivele beneficii, dezavantaje și soluții pentru a putea face evaluări semnificative și a lua decizii bune.

Ca regulă generală, pentru a contracara deficiențele, este important să aveți răbdare cu introducerea soluțiilor digitale. Obiectivele clare, studiile de fezabilitate și proiectele pilot trebuie să preceadă și să ghideze introducerea soluțiilor digitale în procesul electoral. Sugerăm că este necesară evaluarea periodică a beneficiilor și dezavantajelor după introducerea soluției și reevaluarea periodică a acestor soluții.

4. Abordarea „ciclului electoral”

Legiuitorul trebuie să gândească cât mai larg posibil, în ceea ce privește utilizarea soluțiilor digitale pe tot parcursul ciclului electoral. O întrebare inițială, conform experienței, este studierea gradului de automatizare în întregul ciclu. Ambiția este de a înțelege și reglementa utilizarea tehnologiei digitale pe tot parcursul ciclului, nu doar soluțiile specifice. Soluțiile pot evolua rapid, în timp ce principalele caracteristici ale tehnicii subiacente vor persista foarte probabil pe termen lung și trebuie reglementate pentru întregul ciclu.

Trebuie examinată integrarea soluțiilor digitale și potențiala sinergie a acestora cu alte soluții low-tech utilizate în ciclul electoral. Durata de viață a tehnologiilor digitale constituie o problemă. Aceasta poate fi relativ scurtă și este necesară corelarea duratei de viață a diferitelor tehnologii utilizate pe parcursul ciclului electoral.

Un alt aspect important este ca legiuitorul sau autoritatea de reglementare să revizuiască cu un ochi critic toate procesele a căror digitizare este luată în considerare. Este bine

cunoscut faptul că tehnologia nu va îmbunătăți procesul subiacent dacă procesul are probleme; tehnologia digitală le poate amplifica și poate fi mai dăunătoare decât tehnologia low-tech.

5. Abordare multidisciplinară

Legiuitorul trebuie să abordeze reglementarea soluțiilor digitale nu numai cu argumente și raționamente juridice, ci și cu o bună înțelegere a problemelor tehnice. Acest lucru necesită o muncă multidisciplinară. Aspecte foarte importante sunt definițiile și interpretările. Definițiile sunt importante pentru înțelegerea reciprocă și, în ultimii ani, au fost elaborate mai multe glosare, care explică termenii juridici și tehnici specialiștilor din ambele domenii (exemplele includ Anexa II la Recomandarea CM/Rec(2017)5, glosarul Comisiei de la Veneția de termeni electorali și tehnici etc.). Astfel de definiții sunt necesare și importante, dar nu suficiente.

Soluțiile digitale se bazează pe matematică. Programatorii au nevoie de definiții formale/rigide ale conceptelor juridice relevante (de exemplu, principiile alegerilor democratice libere și corecte) pe baza cărora aceștia creează modele sau soluții. Dacă definițiile de bază se schimbă, soluția trebuie, de asemenea, să evolueze și ea. În practică, principiile juridice sunt definite în linii mari. Aplicarea acestora la situații concrete necesită interpretare. Interpretarea va dezvălui care trebuie să fie sensul unui concept în fiecare context. Interpretarea este, de asemenea, necesară pentru a evalua concepte și valori conflictuale. Când vine vorba de soluții digitale, este important ca aceste interpretări să fie făcute de autoritatea competentă și să nu fie lăsate în seama furnizorilor de soluții sau a tehnicienilor.

Este necesară o abordare multidisciplinară. Acest lucru va necesita schimburi iterative între experții în materie juridică și tehnică. Legiuitorul trebuie să prevadă un cadru adecvat, resurse și timp pentru ca acest dialog important să aibă loc.

6. O decizie suverană

Acceptabilitatea utilizării soluțiilor digitale în alegeri depinde de conformitatea acestora cu principiile de nivel superior, inclusiv cele privind alegerile democratice libere și corecte. Această conformitate trebuie asigurată mai întâi în regulament.

Niciun document orientativ internațional nu impune țărilor, respectiv legiuitorilor, să introducă tehnologii digitale în alegeri. După cum s-a explicat anterior, această decizie depinde de mulți factori, unii dintre aceștia, specifici țării. În plus, tehnologia digitală nu este întotdeauna cea mai bună soluție. Abordarea instrumentelor internaționale este de a încuraja țările să înțeleagă că trebuie asigurată conformitatea constituțională a soluțiilor digitale și de a propune îndrumări în acest sens. Chiar și atunci când introducerea instrumentelor digitale este încurajată, conformitatea necesară cu principiile alegerilor libere și corecte este o condiție prealabilă puternică (de exemplu, Legea electorală modificată a UE (neintrată în vigoare), care oferă statelor membre libertatea de a oferi... vot electronic sau prin internet, dacă sunt sigure că vor respecta normele UE relevante privind protecția

datelor cu caracter personal, secretul votului și credibilitatea rezultatelor).14

La un moment dat, deciziile internaționale pot impune, ca efect secundar, digitizarea proceselor electorale asupra țărilor. Legea electorală modificată a UE (neintrată încă în vigoare) inserează un nou articol, care impune fiecărui stat membru obligația de a desemna o autoritate de contact responsabilă cu schimbul de date privind alegătorii și candidații cu omologii săi din alte state membre, în scopul evitării înregistrărilor multiple în registre și votul multiplu. Astfel de schimburi impun digitizarea de facto a registrelor, deoarece pare imposibil de realizat, în mod semnificativ, obiectivul de a compara datele și de a identifica înregistrările duble, în cazul în care o astfel de muncă este efectuată manual. Acest tip de „digitizare forțată" trebuie să fie discutat în detaliu înainte de a deveni obligatoriu.

În cele din urmă, decizia de a introduce soluții digitale este o prerogativă națională care trebuie luată de legiuitorul național pe baza unor considerente specifice situației naționale. După cum atestă decizia Curții Constituționale a Germaniei din 2009, fiecare societate trebuie să își găsească propria soluție și să ia în considerare implicațiile mai largi ale fiecărei modernizări, inclusiv prețul acesteia. Fiecare societate, și anume, legiuitorul, trebuie să decidă dacă este dispusă și capabilă să plătească respectivul preț, care poate fi unul financiar sau implica alte valori mai importante. De asemenea, legiuitorul trebuie să decidă dacă țara este pregătită și capabilă să introducă o modernizare durabilă și benefică. O bună abordare este efectuarea de teste care să ofere informații importante privind luarea deciziilor.

7. Necesitatea, forma și nivelul de reglementare

Reglementarea este fundamentul unei soluții digitale conforme din punct de vedere constituțional. Experiența arată că reglementarea este adesea luată în considerare la sfârșitul procesului de introducere, după ce soluția este aproape finalizată. Acest lucru este greșit, așa cum a arătat și discuția anterioară privind identificarea problemelor, evaluarea scopurilor și obiectivelor etc. Se așteaptă ca regulamentul să ofere îndrumări privind dezvoltarea soluțiilor. Aceasta înseamnă că legiuitorul trebuie să reglementeze, în mod proactiv, principalele aspecte ale utilizării tehnologiilor digitale în alegeri, într-un mod neutru din punct de vedere al soluțiilor.

După cum demonstrează experiența multor țări (SUA, Germania, Olanda, Franța etc.), reglementările moștenite, moștenite din soluții mecanice sau alte soluții low-tech, nu sunt adecvate pentru reglementarea soluțiilor digitale, chiar dacă au fost actualizate. În general, analogiile cu procesele tradiționale nu sunt suficiente. După cum arată exemplul german, nu este suficient ca legea să prevadă

14. Articolul 223 din Tratatul privind funcționarea Uniunii Europene, care prevede modificarea Legii electorale, face acest lucru cu scopul de a obține *„o procedură uniformă în toate statele membre sau în conformitate cu principii comune tuturor statelor membre"*. Pe lângă armonizarea regulilor de fond (de exemplu, vârste minime diferite pentru a candida la alegeri sau praguri minime comune), legea urmărește, de asemenea, *„să încurajeze participarea alegătorilor la alegerile pentru Parlamentul European și să profite pe deplin de posibilitățile oferit de evoluțiile tehnologice."* Articolul 4a stipulează că *„Statele membre pot prevedea posibilități de vot în avans, vot prin corespondență și vot electronic și prin internet, în cadrul alegerilor pentru Parlamentul European. Când fac acest lucru, acestea adoptă măsuri suficiente pentru a asigura, în special, credibilitatea rezultatului, secretul votului și protecția datelor cu caracter personal în conformitate cu legislația aplicabilă a Uniunii"*. Cu toate acestea, nu este clar ce dovezi au utilizat autorii legii pentru a concluziona că votul electronic va crește participarea.

că „dispozitivele pot fi utilizate cu condiția ca secretul votului să fie garantat” (articolul 35 din Legea electorală federală). Un regulament detaliat trebuie să indice, în mod clar, ce implică aceasta și să permită controale independente, pentru a asigura că aceste cerințe sunt respectate.

Cine reglementează ce constituie o altă întrebare. În unele țări, instanțele au fost cele care au definit cum trebuie să arate regulamentul pentru ca acesta să fie conform. Curtea Constituțională din Germania a afirmat că reglementarea trebuie să fie detaliată până la punctul în care cetățeanul să poată controla modul în care votul său este gestionat fără cunoștințe sau asistență tehnică. Aceasta este o definiție importantă a transparenței în alegeri. Desigur, Curtea Constituțională din Germania a „descoperit” această definiție (pe baza interpretării sale a dispozițiilor constituționale relevante) și nu a inventat-o. În alte țări, precum SUA sau Elveția, instanțele au invitat legiuitorul să elaboreze aceste definiții. În India, cea mai înaltă instanță a decis că este necesară o pistă de audit pe hârtie verificată de alegători, pentru ca dispozitivele de vot să respecte principiile, dar decizia acesteia fusese deja anticipată de autoritatea electorală. Elementul comun în toate cazurile este că definirea sensului concret al principiilor superioare într-un context în care sunt utilizate soluții digitale afectează însuși sensul principiilor. Așadar, decizia trebuie luată de autoritatea competentă, de obicei, legiuitorul.

Delegarea competențelor de reglementare către guvern sau comisia electorală centrală etc. trebuie să fie încadrată, în mod clar. De exemplu, Comisia de la Veneția și OSCE/OIDDO au subliniat că utilizarea soluțiilor digitale, care sunt probleme esențiale în procedurile electorale (de exemplu, votul prin internet), trebuie să fie clar definită în lege.

Aspectele privind reglementare sunt mai complexe în statele federale. Implementarea noii tehnologii în acest caz trebuie să facă față, de asemenea, și unui sistem descentralizat de administrare a alegerilor. În Argentina, provinciile și-au extins prerogativele de reglementare, iar discrepanțele dintre reglementările provinciale în domeniul votului electronic au fost dăunătoare. În mod similar, în Canada, lipsa standardelor federale sau provinciale a lăsat multe municipalități să ia decizii în mare măsură izolate. În ambele cazuri, încrederea în furnizori pentru a stabili standardul pentru securitatea cibernetică și responsabilitatea publică a fost problematică. Elveția, o altă țară federală, poate oferi un bun exemplu în acest sens: spre deosebire de alte aspecte ale alegerilor, votul prin internet este reglementat în primul rând și în principal la nivel federal, asigurând aceleași standarde în întreaga țară. Acesta nu este (deocamdată) cazul în ceea ce privește alte soluții digitale utilizate în alegeri, cum ar fi votul electronic pur: cantoanele au rezistat până acum încercărilor de a avea reglementări armonizate/centralizate la nivel federal.

8. Conținutul regulamentului

A. Cerințe detaliate

Reglementarea detaliată este importantă pentru punerea în funcțiune a soluțiilor digitale pentru alegeri, pentru procedurile de control și certificare, pentru clarificarea drepturilor și obligațiilor părților interesate și pentru informarea inovatorilor și furnizorilor de soluții digitale cu privire la cerințe.

Comisia de la Veneția sau OSCE/OIDDO au subliniat că prevederile privind utilizarea tehnologiei trebuie să fie însoțite de elaborări detaliate în legea privind soluțiile tehnice utilizate și procedurile care trebuie urmate. Acestea trebuie să acopere, printre altele, aspecte privind achizițiile, testarea, auditul și accesul public la tehnologii. Comisia subliniază faptul că declararea principiilor generale nu este suficientă atunci când reglementăm soluțiile digitale pentru alegeri dacă nu există nicio garanție că aceste principii generale vor fi puse în aplicare cu reguli specifice care sunt fundamentale pentru alegerile cu adevărat democratice. Prin urmare, este necesar ca reglementările să fie elaborate într-o manieră detaliată și responsabilă.

La introducerea noilor tehnologii în unele părți ale ciclului electoral, și anume la vot și numărare, apare un conflict între cerințele sufragiului secret și exactitate. De exemplu, alegătorul trebuie să poată verifica dacă votul său a fost înregistrat și numărat conform voinței sale (acuratețe), dar, în același timp, nu trebuie să primească dovada care îi permite să își vândă votul sau să dovedească cuiva care exercită constrângere, cum a votat (secret). Publicul trebuie să poată verifica corectitudinea rezultatului (acuratețe), fără a afla cum au votat alegătorii individuali (secret). Criptografia oferă soluții care permit astfel de cerințe conflictuale până la un anumit punct. Cu toate acestea, nu este posibil să se satisfacă complet și simultan toate cerințele conflictuale. Soluțiile criptografice se bazează pe ipoteze precum că unii participanți la proces sunt sinceri, de exemplu. Astfel de ipoteze influențează, în mod direct, punerea în aplicare a principiilor generale de nivel superior și trebuie reglementate în detaliu de către autoritatea competentă.

b. Centrat pe drepturile omului

În prezent, este admis la nivel global că instrumentele TIC de participare trebuie să fie conforme cu drepturile omului din punct de vedere al concepției. Acest lucru indică necesitatea, în cazul nostru, de a avea o reglementare detaliată care să clarifice implicațiile drepturilor omului (în acest caz dreptul la alegeri libere, corecte și democratice) asupra utilizării soluțiilor digitale în alegeri. O astfel de reglementare trebuie să preceadă dezvoltarea și introducerea unei soluții specifice. Dezvoltatorii de soluții trebuie să își orienteze munca astfel încât să țină cont de cerințele de reglementare. Aceștia trebuie să cunoască, în prealabil, principalele implicații ale principiilor alegerilor libere, corecte și democratice asupra tehnologiei avute în vedere.

Din nou, acest lucru arată că legiuitorul trebuie să fie proactiv și să ia în considerare utilizarea pe scară largă a soluțiilor digitale, în ciclul electoral. Mai jos sunt câteva elemente (lista este departe de a fi exhaustivă) ale unui astfel de regulament.

c. Utilizabilitate

Utilizabilitatea este un aspect important și nu numai pentru a obține soluții ușor de utilizat. Este important și din punct de vedere al securității. Pentru a le implementa efectul și a minimiza utilizarea greșită/abuzul, soluțiile digitale trebuie să fie înțelese și utilizate în mod corespunzător. Utilizatorii trebuie să fie pregătiți să observe și să gestioneze eventualele erori care pot apărea. Este important ca astfel de aspecte să fie abordate în regulament, astfel încât competențele și obligațiile utilizatorilor să fie clarificate. Acest lucru indică, de asemenea, importanța educației utilizatorilor preconizați și a altor părți interesate, precum și dispozițiile de reglementare necesare privind informarea și educația.

d. Protecția datelor

În cazul reglementării votului electronic trebuie avute în vedere instrumentele de protecție a datelor. Dar, după cum s-a menționat mai sus, datele electorale sunt date sensibile și, ca atare, sunt supuse unor cerințe mai stricte, care trebuie prevăzute în legislația electorală.

De menționat că protecția datelor în cazul alegerilor înseamnă protecția anumitor date de la operatorul de date (de exemplu, autoritatea electorală). Secretul votului presupune ca nici autoritatea electorală, nici alți actori să nu știe cum a votat un alegător. Aceeași autoritate trebuie, în același timp, să controleze accesul la soluție, deoarece acest acces este limitat doar la deținătorii de drepturi. Acest lucru face uz de soluții digitale pentru unele aspecte ale alegerilor, cum ar fi votul, deosebit de delicat.

Legiuitorului i se cere să ia decizii importante în acest sens. De exemplu, acestuia i se va cere să cântărească valori precum securitatea și transparența sau libertatea de a vota. Aceste decizii sunt premisele pentru implementarea tehnicilor digitale.

Reglementările existente, în principal pentru votul electronic, au evoluat și încă trebuie să facă acest lucru. Este important un control adecvat al implementărilor de protecție a datelor. În vederea alegerilor pentru Parlamentul European din 2019, Comisia Europeană a pregătit un document de orientare privind aplicarea legislației Uniunii Europene privind protecția datelor în context electoral.

e. Transparență

Rolul transparenței este de a garanta că întregul sistem și soluția digitală specifică funcționează în mod corect. Acestea fiind spuse, autoritatea de reglementare trebuie să precizeze care părți ale sistemului trebuie să fie transparente; care sunt implicațiile concrete; cine participă la exercițiul de transparență; cum se asigură și controlează transparența necesară; cum se sancționează nerespectarea; și cum se tratează informațiile care sunt dezvăluite prin transparență etc. În plus, participanții trebuie să fie informați și trebuie să fie capabili să participe la exercițiu, mai ales dacă transparența face parte din securitatea sistemului.

Transparența are, de asemenea, și o altă dimensiune: se preconizează ca, în unele cazuri, soluțiile digitale să facă politica mai transparentă, să combată corupția, să îmbunătățească serviciile

publice, să implice semnificativ cetățenii în elaborarea politicilor locale etc. Dacă sunt reglementate și implementate în mod corespunzător, acestea pot chiar reuși să facă acest lucru.

Reglementarea transparenței soluțiilor digitale a evoluat considerabil în ultimii ani trecând de la securitate prin abordări de obscuritate și sisteme de tip black-box, la transparență parțială (implicarea partidelor politice și a observatorilor acreditați în exerciții de transparență), la o abordare mai deschisă care implică publicarea de coduri sursă și alte documente relevante, controlul de către specialiști independenți și piratarea etică a soluțiilor etc. O astfel de transparență este considerată parte a măsurilor de securitate.

f. Securitate cibernetică

Securitatea cibernetică în alegeri a fost o problemă extrem de actuală în ultimii ani. Țările au devenit conștiente de faptul că utilizarea soluțiilor digitale, în special a celor conectate la internet, ar putea permite unui singur actor (inclusiv unei puteri străine) să controleze alegerile; lipsa unei dovezi durabile, cu sigiliu a rezultatului/datelor corecte. Cadrele de reglementare trebuie să abordeze strategiile de risc, măsurile de protecție, posibilitățile de verificare și planificarea pentru situații de urgență, printre altele.

În ceea ce privește strategiile de risc, măsurile de protecție și planificarea pentru situații de urgență, la nivel regional există ghiduri bazate pe instrumente juridice internaționale care abordează securitatea cibernetică. Comitetul Convenției de la Budapesta privind criminalitatea informatică a Consiliului Europei a emis, de exemplu, o notă orientativă privind alegerile. Nota abordează utilizarea prerogativelor procedurale ale Convenției de la Budapesta și a prevederilor privind asistența judiciară reciprocă într-o anchetă sau o procedură penală specifică privind ingerința electorală. Convenția de la Budapesta incriminează mai multe tipuri de conduită (accesul ilegal, interceptarea ilegală, ingerința în materie de date, ingerința în sistem, utilizarea abuzivă a dispozitivelor, falsificarea computerizată). Dacă este făcută fără a avea dreptul de către persoane, precum și companii sau alte grupuri, în contextul alegerilor, o astfel de conduită încalcă alegerile libere, corecte și democratice. Întrucât ingerința electorală are adesea o dimensiune internațională, Convenția de la Budapesta oferă îndrumări privind cooperarea internațională pentru a contracara astfel de infracțiuni. De asemenea, la nivelul UE, Grupul de Cooperare NIS a emis ghiduri specifice care se concentrează pe securitatea cibernetică a tehnologiei utilizate în alegeri. Compendiul acestuia, din 2018, privind securitatea cibernetică a tehnologiei electorale este menit să împărtășească experiențe și să ofere îndrumări, precum și o privire de ansamblu asupra instrumentelor, tehnicilor și protocoalelor pentru a detecta, preveni și atenua astfel de amenințări.

În ceea ce privește opțiunile de verificare, cea mai mare parte a efortului se face în domeniul votului electronic. Experiențele recente arată că controlul instalării și implementării soluțiilor de verificabilitate este crucial pentru ca acestea să își îndeplinească rolul. Cu toate acestea, utilizarea unor astfel de metode este încă la început; înțelegerea lor de către nespecialiști este destul de limitată. Este necesară o mai bună înțelegere interdisciplinară dacă urmează să fie impuse astfel de metode pentru a asigura securitatea soluțiilor digitale utilizate în alegeri.

g. Control, aplicare, răspundere

Experiența votului electronic arată că reglementarea trebuie să includă cerințe minime, inclusiv pentru controlul soluției și pentru verificarea independentă atât a soluției, cât și a rezultatelor furnizate de aceasta (a se vedea Recomandarea CM/Rec(2017)5 privind standardele pentru votul electronic).

Astfel de cerințe se pot aplica dincolo de votul electronic. Acestea trebuie să reflecte pe deplin principiile alegerilor democratice libere și corecte și alte principii juridice relevante. Soluțiile digitale trebuie să facă obiectul evaluărilor de către organisme independente și competente, la intervale adecvate și după modificări importante. Acestea trebuie să fie deschise auditurilor și să raporteze, în mod activ, asupra potențialelor probleme și amenințări.

Responsabilitatea finală pentru respectarea cerințelor, chiar și în cazul defecțiunilor și atacurilor, revine autorității responsabile cu îndeplinirea sarcinii încredințate soluției digitale. Autoritatea trebuie să efectueze controale pentru a se asigura că soluția și toate materialele și procedurile aferente sunt autentice, funcționează corect, sunt actualizate, sunt protejate și sunt operate într-o manieră sigură. Soluția trebuie să reflecte tehnologia de ultimă generație, ceea ce înseamnă că cooperarea cu mediul academic (experți independenți și competenți) este importantă. Experiența cu votul electronic arată că acesta este o provocare și că poate fi dificilă menținerea soluțiilor de ultimă generație în timp.

După cum s-a menționat mai sus, pentru soluțiile critice și expuse internetului, controalele (certificare, audituri etc.) pot să nu fie suficiente. Este necesară verificarea independentă a rezultatelor. Verificarea poate lua diferite forme în funcție de soluție. Poate fi ea însăși digitală sau pe hârtie sau o combinație a celor două. Pentru instrumentele de verificare digitală, experiența arată că este necesar controlul controlerelor, și anume, controlul sistemului de verificare. În plus, pentru a-și juca corect rolul, soluțiile de verificabilitate trebuie să fie înțelese și utilizate de utilizatori, care pot fi alegători, administrația electorală, observatori etc. Prin urmare, este necesar să existe utilizatori cunoscători care să utilizeze corect soluția. De exemplu, anumite atacuri pot fi detectate numai dacă destui utilizatori finali efectuează verificarea, înțeleg problema dezvăluită de verificare și se plâng.

În urmă cu mai bine de zece ani, Curtea Constituțională a Germaniei a declarat că certificarea nu este suficientă și este necesară verificarea de către alegător. Curtea nu a acceptat argumentul potrivit căruia ar putea fi de așteptat ca sistemele implementate să fie viabile, având în vedere că acestea au fost examinate și certificate într-o procedură desemnată înainte de punerea în aplicare. Recomandarea Comitetului de Miniștri al Consiliului Europei CM/Rec(2017)5 privind standardele pentru votul electronic prescrie verificarea individuală și universală a votului și a rezultatelor generale (a se vedea, în special, standardele 15-18) – două rezultate esențiale ale sistemelor de vot electronic. Acest lucru ajută la asigurarea sufragiului liber.

Modelul de verificare german sau austriac impune ca verificarea să fie înțeleasă și efectuată de nespecialiști (alegătorul sau comisarul electoral) fără cunoștințe tehnice. Acest lucru necesită coexistența, în paralel cu soluția digitală, a unei soluții pe hârtie, care să poată fi înțeleasă de nespecialist. Celălalt model de verificare este cel estonian sau elvețian. Metoda de verificare poate fi controlată și validată de experți,

care se referă la metode aprobate de comunitatea științifică respectivă. Cu toate acestea, pare dificilă aplicarea unor astfel de metode alegerilor politice de la unu-la-unu.

h. Managementul schimbării, resursele și cooperarea cu sectorul privat

O altă diferență între soluțiile tradiționale și cele digitale este caracterul evolutiv al tehnicii digitale. Reglementarea trebuie să integreze și să reflecte acest lucru. Strâns legat de natura evolutivă a tehnologiei, este faptul că soluțiile digitale necesită resurse umane calificate și financiare. În timp, nevoia de resurse poate varia în funcție de eforturile necesare pentru a asigura conformitatea constituțională a soluției. Nevoia de resurse și perspectiva posibilității ca o astfel de nevoie să evolueze în timp trebuie abordate în regulament, în mod corespunzător. OE-urile care au introdus soluții digitale se confruntă cu provocarea de a menține și înlocui partea de software și hardware. Există îngrijorări cu privire la sustenabilitatea unor tehnologii electorale. Poate este înțelept să se aibă în vedere astfel de probleme în faza de reglementare și poate să fie evitate cele mai complexe tehnologii.

Un aspect important este cooperarea necesară cu sectorul privat. Sectorul privat poate juca mai multe roluri, inclusiv furnizor de soluții, controlor, certificator, operator etc. Având în vedere acest fapt, legiuitorul trebuie să analizeze cu atenție relația dintre sectorul public și cel privat. Cerințele detaliate care asigură respectarea principiilor de nivel superior trebuie să fie deja prevăzute în documentele de achiziție. Responsabilitatea finală pentru desfășurarea alegerilor revine autorității de stat însărcinate cu desfășurarea alegerilor. Regulamentul trebuie să abordeze cerințele de răspundere și control și, după cum arată experiența, să reglementeze consecințele posibilelor deficiențe. Legiuitorul trebuie să ia în considerare cu atenție și, în mod ideal, să evite dependența de furnizorii privați pentru soluțiile sensibile care au un impact critic asupra întregului proces electoral. În plus, autoritatea trebuie să aibă suficient personal calificat și trebuie să investească în formarea sa pentru a garanta întreținerea sistemului, pentru a facilita introducerea de noi funcții și alte modificări și pentru a permite funcționarea corectă a acestuia.

9. Încredere

Încrederea este adesea menționată atunci când se discută despre utilizarea soluțiilor digitale în alegeri.
Aceasta are diferite fațete.

Încrederea este considerată o condiție prealabilă pentru introducerea soluțiilor digitale în alegeri. Acest lucru este clar pentru votul electronic, dar se aplică și altor soluții digitale; de exemplu, la tehnologia biometrică. Introducerea tehnologiei nu poate rezolva lipsa de încredere în sistemul electoral. Au existat și alte abordări în trecut. Unii dintre cei mai timpurii și cei mai pasionați adoptatori ai tehnologiilor digitale pentru alegeri s-au numărat dintre cele mai sărace țări, adesea fără un lung istoric de alegeri democratice. În aceste contexte, adoptarea de noi tehnologii și uneori costisitoare a fost concepută pentru a combate abuzurile și a crea încredere

între părțile electorale interesate și electorat. Inițial, unele țări au reușit să facă acest lucru. Cu toate acestea, a devenit clar că doar soluțiile digitale în sine nu pot crea încredere. Încrederea existentă, în special în autoritățile însărcinate cu desfășurarea alegerilor, este o condiție prealabilă pentru introducerea soluțiilor digitale. Acolo unde publicul sau părțile interesate politice nu au încredere unul în celălalt sau în soluțiile digitale, acestea nu sunt acceptate, în ciuda meritelor tehnice obiective și a avantajelor pe care le-ar putea avea. Încrederea existentă, precum și consultarea publică și sprijinul sunt necesare pentru o introducere cu succes a soluțiilor digitale. Experiența arată că consultările, testarea, pilotarea etc. pot contribui la insuflarea încrederii. Cu toate acestea, soluția trebuie să fie mai întâi de încredere.

Cercetările au acordat o mare importanță credibilității tehnologiilor digitale în alegeri. Aceasta se referă la cerințe de ultimă generație, controale, implementări, soluții validate de colegi etc. Cu toate acestea, în multe cazuri, tehnologia a fost introdusă fără o cercetare, planificare, testare, formare sau educare a alegătorilor corespunzătoare, iar acest lucru a erodat, în schimb, încrederea în proces și a crescut costurile. În alte părți, au fost introduse tehnologii care nu sunt de încredere și amenință integritatea electorală, iar acest lucru poate duce la o erodare a încrederii publicului în procesele electorale.

Încrederea se bazează pe transparență. Nu este suficient ca soluțiile să fie demne de încredere și ca alegerile să fie libere, corecte și democratice - oamenii trebuie să aibă, de asemenea, convingerea că lucrurile s-au și întâmplat astfel, potrivit Curții Constituționale a Germaniei. Respectarea principiilor constituționale ale sufragiului liber, corect și secret etc. înseamnă că alegerile trebuie să fie însoțite de încrederea oamenilor în ceea ce privește conformitatea. Pentru Curtea Constituțională germană, singura modalitate de a realiza acest lucru este de a permite tuturor să verifice conformitatea.

CONCLUZII

Mai jos, rezumăm principalele constatări.

Soluțiile digitale sunt deja utilizate în ciclul electoral. Acestea trebuie să se conformeze tuturor **principiilor constituționale** relevante, mai precis, principiilor alegerilor libere, corecte și democratice.

- Spre deosebire de reglementarea soluțiilor low-tech, nu este suficient ca reglementările soluțiilor digitale să reafirme doar principiile. Acestea trebuie să includă dispoziții detaliate care traduc principiile în cerințe legale detaliate, care guvernează tehnologia digitală.

- Provocarea pentru legiuitor este să se asigure, deja la nivel de reglementare, că drepturile constituționale sunt respectate.

Instrumentele internaționale care reglementează alegerile sunt relevante atunci când se are în vedere reglementarea soluțiilor digitale utilizate în alegeri. Acestea includ convenții universale (Declarația Universală a Drepturilor Omului, Pactul Internațional cu privire la Drepturile Civile și Politice) și regionale (Convenția Europeană a Drepturilor Omului, Carta Drepturilor Fundamentale a UE), interpretări autorizate ale unor astfel de convenții, jurisprudență din instanțele internaționale, angajamente politice, documente fără caracter obligatoriu *(soft-law)*, studii și evaluări ale reglementărilor existente și utilizările soluțiilor digitale.

Instrumentele internaționale care reglementează protecția datelor, criminalitatea informatică sau securitatea cibernetică sunt, de asemenea, relevante.

- Convenția modernizată a Consiliului Europei pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal (Convenția 108+) și Regulamentul general al UE privind protecția datelor (RGPD) sunt extrem de relevante, cu toate acestea, unele date referitoare la alegeri sunt date calificate: necesită o protecție mai strictă, care trebuie definite în regulamentele specifice alegerilor.

- În cadrul Regulamentului general al UE privind protecția datelor (RGPD), Convenția de la Budapesta privind criminalitatea informatică a Consiliului Europei și instrumentele juridice ale UE privind securitatea cibernetică, au fost elaborate ghiduri și culegeri specifice de bune practici care vizează alegerile.

Reglementările naționale pentru soluțiile digitale utilizate în alegeri sunt încă la început și evoluează.

- Reglementările specifice se referă, în principal, la votul electronic. Au existat, în principal, două tipuri de reglementări. În unele țări, instrumentele mai vechi care reglementau utilizarea soluțiilor low-tech au evoluat pentru a reglementa dispozitivele de vot electronic. Cu toate acestea, majoritatea dintre ele s-au dovedit a fi neconforme din punct de vedere constituțional, fapt ce a condus la suprimarea sau reducerea drastică a utilizării dispozitivelor de vot electronic. Reglementările de primă generație privind

votul pe internet au fost, de asemenea, considerate insuficiente. În unele locuri, acestea au fost actualizate pentru a reflecta o mai bună înțelegere a tehnologiilor digitale (politica de risc, verificabilitate, controale independente, obligații privind transparența). Cu toate acestea, experiența recentă arată că ele trebuie să continue să evolueze pentru a aborda mai bine probleme precum verificabilitatea sau transparența.

- Alte soluții digitale sunt subreglementate.

Identificarea clară a **problemei** care trebuie rezolvată este primul pas către găsirea unei soluții adecvate.

- Propunerile de soluții digitale trebuie să se bazeze pe cercetarea problemei și așteptările utilizatorilor.
- Astfel de evaluări trebuie să fie distribuite pe scară largă.

Următorul pas este identificarea situației dorite (**scopul**) și stabilirea **obiectivelor** către scopul respectiv.

- Scopurile și obiectivele trebuie să fie „neutre din punct de vedere al soluțiilor”.
- După identificarea acestora, legiuitorul trebuie să ia în considerare toate soluțiile posibile, în scopul găsirii celor care contribuie mai bine la întărirea principiilor constituționale.

Pentru a evalua oportunitatea de a introduce o soluție avută în vedere, legiuitorul trebuie să ia în considerare atât **avantajele, cât și dezavantajele** acesteia.

- Legiuitorul trebuie să înțeleagă bine beneficiile, dezavantajele și respectivele soluții pentru a putea face evaluări semnificative și a lua decizii bune.
- Ca regulă generală, pentru a contracara deficiențele, este important să aveți răbdare cu introducerea soluțiilor digitale. Obiectivele clare, studiile de fezabilitate și proiectele pilot trebuie să preceadă și să ghideze introducerea soluțiilor digitale în procesul electoral.
- Sugerăm că este necesară introducerea evaluării periodice a beneficiilor și dezavantajelor după soluție și că este necesară reevaluarea periodică a acestor soluții.

Legiuitorul trebuie să gândească cât mai larg posibil, în ceea ce privește utilizarea soluțiilor digitale pe tot parcursul **ciclului electoral**.

- Soluțiile pot evolua rapid, în timp ce principalele caracteristici ale tehnicii subiacente vor persista, foarte probabil, pe termen lung. Sugerăm că astfel de caracteristici trebuie reglementate pentru întregul ciclu. Ambiția trebuie să fie înțelegerea și reglementarea utilizării tehnologiei digitale pe tot parcursul ciclului, nu doar pentru soluții specifice.
- Sunt importante gradul de automatizare a ciclului electoral, durata de viață a diferitelor tehnologii utilizate și revizuirea critică a proceselor a căror digitizare este avută în vedere.

Reglementarea soluțiilor digitale necesită o **abordare multidisciplinară**.

- Ca un pas inițial, în ultimii ani au fost elaborate mai multe glosare care explică termenii juridici și tehnici în atenția specialiștilor din ambele domenii. Acest lucru este necesar și important, dar nu suficient.
- Deoarece soluțiile digitale se bazează pe matematică, programatorii utilizează definiții formale/rigide ale conceptelor juridice relevante pentru a construi soluții digitale. Totuși, în practică, principiile juridice sunt definite în linii mari și interpretarea este necesară. Nu există o definiție atât de strictă a unui concept juridic. În ceea ce privește soluțiile digitale, este important ca interpretările principiilor pentru tehnologia respectivă să fie, în cele din urmă, hotărâte de către autoritatea competentă (legislator sau autoritatea de reglementare) și să nu fie lăsate numai în seama furnizorilor de soluții sau tehnicienilor.
- Sugerăm că munca multidisciplinară necesită schimburi iterative între experții din domeniul juridic și tehnic. Legiuitorul trebuie să prevadă cadre, resurse și timp adecvate pentru ca acest dialog important să aibă loc și aceasta trebuie să devină norma atunci când se reglementează soluțiile digitale pentru alegeri.

Niciun document orientativ internațional nu impune țărilor, respectiv legiuitorilor, să introducă tehnologii digitale în alegeri. Aceasta este **o decizie suverană**. Fiecare societate, și anume, legiuitorul, trebuie să decidă dacă este pregătită și capabilă să introducă o astfel de modernizare. O bună abordare este efectuarea de teste care să ofere informații importante privind luarea deciziilor.

11 Necesitatea, forma și nivelul de reglementare

- Reglementarea este fundamentul unei soluții digitale conforme din punct de vedere constituțional. Se preconizează ca aceasta să ofere îndrumări cu privire la dezvoltarea de soluții. Legiuitorul trebuie să reglementeze proactiv principalele aspecte ale utilizării tehnologiilor digitale în alegeri, într-un mod neutru din punct de vedere al soluțiilor.
- Reglementarea nu poate doar reafirma principiile sau proceda prin analogie cu soluțiile pe hârtie. Aceasta trebuie să indic, în mod clar, implicațiile practice ale principiilor și să permită controale independente pentru a se asigura că cerințele detaliate sunt respectate.
- Definirea sensului concret al principiilor superioare într-un context în care sunt utilizate soluții digitale afectează însuși sensul principiilor. Deci, în cele din urmă, decizia trebuie luată de autoritatea competentă, de obicei, legiuitorul.
- Delegarea competențelor de reglementare către guvern sau comisia electorală centrală etc. trebuie să fie încadrată în mod clar.
- Aspectele de reglementare sunt mai complexe în statele federale cu un sistem descentralizat de administrare a alegerilor. Este important să vă asigurați că aceleași standarde juridice se aplică în toată țara și în soluții.

Cerințele detaliate sunt importante. Declararea principiilor generale nu este suficientă atunci când sunt reglementate soluțiile digitale pentru alegeri dacă nu există nicio garanție că aceste principii generale vor fi puse în aplicare cu reguli specifice care sunt fundamentale pentru alegerile cu adevărat democratice. Prin urmare, este necesar ca reglementările să fie elaborate într-o manieră detaliată și responsabilă. Cerințele detaliate sunt deosebit de importante atunci când se introduc soluții criptografice.

Instrumentele de participare trebuie să fie **conforme cu drepturile omului prin concept**. Dezvoltatorii de soluții trebuie să își orienteze activitatea pentru a ține cont de cerințele detaliate de reglementare pentru soluțiile digitale. Aceștia trebuie să cunoască în avans principalele implicații ale principiilor alegerilor libere, corecte și democratice asupra tehnologiei avute în vedere.

14 **Utilizabilitatea** este importantă din perspectiva ușurinței de utilizare și, de asemenea, deoarece contribuie la securitatea soluției digitale.

15 Unele date electorale sunt date sensibile.

- **Protecția datelor**, în acest caz, înseamnă protecția anumitor date de la operatorul de date (de exemplu, autoritatea electorală). Aceeași autoritate trebuie, în același timp, să controleze accesul la soluție, deoarece acest acces este limitat doar la deținătorii de drepturi. Acest lucru face uz de soluții digitale pentru unele aspecte ale alegerilor, cum ar fi votul, deosebit de delicat.

- Legiuitorul va trebui să cântărească valori opuse precum securitatea și transparența sau libertatea de a vota. Astfel de decizii sunt premisele pentru implementarea tehnicii digitale.

16 Reglementarea **transparenței** soluțiilor digitale a evoluat către o abordare mai deschisă.

- Aceasta implică publicarea codurilor sursă și a altor documente relevante, controlul de către specialiști independenți, piratarea etică a soluțiilor etc. O astfel de transparență este considerată parte a măsurilor de securitate.

- Autoritatea de reglementare trebuie să precizeze care părți ale sistemului trebuie să fie transparente, care sunt implicațiile concrete, cine participă la exercițiul de transparență, cum se asigură transparența necesară și să o controleze, cum se sancționează neconformitatea, cum se tratează informațiile care sunt dezvăluite prin transparență etc.

Securitatea cibernetică pentru alegeri este o problemă extrem de actuală în ultimii ani. Cadrele de reglementare trebuie să abordeze strategiile de risc, măsurile de protecție, posibilitățile de verificare și planificarea pentru situații de urgență, printre altele.

- În ceea ce privește strategiile de risc, măsurile de protecție și planificarea pentru situații de urgență, la nivel regional există ghiduri bazate pe instrumente juridice internaționale care abordează securitatea cibernetică.

- În ceea ce privește posibilitățile de verificare, cea mai mare parte a eforturilor se face în domeniul votului electronic. Controlul instalării și implementării soluțiilor de verificabilitate este crucial pentru ca acestea să își îndeplinească rolul. Este necesară o mai bună înțelegere interdisciplinară dacă urmează să fie impuse astfel de metode pentru a asigura securitatea soluțiilor digitale utilizate în alegeri.

18 Control, aplicare, răspundere

- Reglementarea trebuie să includă cerințe minime pentru controlul soluției și pentru verificarea independentă atât a soluției, cât și a rezultatelor furnizate de aceasta.
- Responsabilitatea finală pentru respectarea cerințelor, chiar și în cazul defecțiunilor și atacurilor, revine autorității responsabile cu îndeplinirea sarcinii încredințate soluției digitale.
- Soluția trebuie să reflecte tehnologia de ultimă generație, ceea ce înseamnă că cooperarea cu mediul academic (experți independenți și competenți) este importantă. Acest lucru poate fi dificil de asigurat în timp.
- Pentru soluțiile digitale critice și expuse internetului, controalele (certificare, audituri etc.) pot să nu fie suficiente. Este necesară verificarea independentă a rezultatelor. Verificarea poate lua diferite forme.
- Pentru instrumentele de verificare digitală, experiența arată că este necesar controlul controlerelor, și anume controlul sistemului de verificare.
- Soluțiile de verificabilitate trebuie să fie înțelese și utilizate efectiv de către utilizatorii finali, care pot fi alegători, administrația electorală, observatori etc. De exemplu, anumite atacuri, pot fi detectate numai dacă destui utilizatori finali efectuează verificarea, înțeleg problema dezvăluită prin verificare și apoi reclamă.

19 Managementul schimbării

- Caracterul evolutiv al tehnicii digitale trebuie integrat în reglementarea acesteia.
- Strâns legat de natura evolutivă a tehnologiei, este faptul că soluțiile digitale necesită resurse umane calificate și financiare. Nevoia de resurse și perspectiva posibilității ca o astfel de nevoie să evolueze în timp trebuie abordate în regulament, în mod corespunzător.
- Legiuitorul trebuie să analizeze cu atenție relația dintre sectorul public și cel privat. Cerințele detaliate care asigură respectarea principiilor de nivel superior trebuie prevăzute, în avans, în documentele de achiziție.
- Responsabilitatea finală pentru desfășurarea alegerilor revine autorității de stat însărcinate cu desfășurarea alegerilor. Regulamentul trebuie

să abordeze cerințele de răspundere și control și, după cum arată experiența, să reglementeze consecințele posibilelor deficiențe.

- Autoritatea trebuie să aibă suficient personal calificat și trebuie să investească în formarea acestuia.

20 Încredere

- Încrederea este considerată o condiție prealabilă pentru introducerea soluțiilor digitale în alegeri.
- Soluțiile trebuie să fie, în primul rând, de încredere. Aceasta se referă la cerințe de ultimă generație, controale, implementări, soluții validate de omologi etc.
- Încrederea se bazează pe transparență și posibilități de verificare.

REFERINȚE SELECTATE

Texte juridice, ghiduri, evaluări, bune practici internaționale

- Consiliul Europei, *Convenția pentru apărarea Drepturilor Omului și a Libertăților fundamentale, (Convenția Europeană a Drepturilor Omului, CEDO) (în vigoare, 1953).*

- Consiliul Europei, *Convenția modernizată pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal (Convenția 108+), CETS Nr. 223 (Protocol adoptat în iunie 2018).*

- Consiliul Europei, Comitetul consultativ al Convenției 108+, *Raport privind inteligența artificială. Inteligența artificială și protecția datelor: provocări și posibile remedii (ianuarie 2019).*

- Consiliul Europei, *Convenția privind criminalitatea informatică (Convenția de la Budapesta), CETS Nr. 185 (în vigoare, 2004).*

- Consiliul Europei, Comitetul Convenției privind criminalitatea informatică (T-CY), *Nota orientativă Nr. 9, Aspecte ale ingerinței electorale prin intermediul sistemelor informatice acoperite de Convenția de la Budapesta. Adoptată de T-CY la 8 iulie 2019.*

- Consiliul Europei, Curtea Europeană a Drepturilor Omului, *Ghid privind articolul 3 din Protocolul 1 la Convenția Europeană a Drepturilor Omului - Dreptul la alegeri libere (aprilie 2019).*

- Consiliul Europei, Comitetul de Miniștri, *Recomandarea CM/Rec(2017)5 a Comitetului de Miniștri către statele membre privind standardele pentru votul electronic (Adoptată de Comitetul de Miniștri la 14 iunie 2017 la cea de-a 1289-a reuniune a adjuncților miniștrilor).*

- Uniunea Europeană, *Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică).*

- Uniunea Europeană, *Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (Directiva NIS).*

- Uniunea Europeană, Grupul de Cooperare NIS, *Compendiu privind securitatea cibernetică a tehnologiilor electorale, Publicația CG 03/2018.*

- Uniunea Europeană, *Regulamentul (UE) 2016/679 Regulamentul general privind protecția datelor, (RGPD).*

- Comisia Europeană, *Alegeri libere și corecte. Document de orientare. Ghidul Comisiei privind aplicarea legislației Uniunii privind protecția datelor în context electoral (septembrie 2018).*

- Uniunea Europeană (Consiliul), *Directiva Consiliului 94/80/CE din 19 decembrie 1994 de stabilire a modalităților detaliate pentru exercitarea dreptului de vot și de a candida*

la alegerile municipale de către cetățenii Uniunii cu reședința într-un stat membru a cărui cetățenie nu o au.

Uniunea Europeană, *Legea privind alegerea reprezentanților Adunării prin sufragiu universal direct, JO L 278, 8.10.1976, p. 5, astfel cum a fost modificată ultima oară prin Decizia Consiliului 2002/772/CE, Euratom, din 25 iunie și 23 septembrie 2002.*

Uniunea Europeană (Consiliul), *Decizia Consiliului 2018/994* [nu este în vigoare] *de modificare a legii privind alegerea membrilor Parlamentului European prin sufragiu universal direct, anexată la Decizia 76/787/ECSC, CEE, Euratom a Consiliului din 20 septembrie 1976.*

Uniunea Europeană, Președinția estonă a Consiliului UE, *Declarația de la Tallinn privind guvernarea electronică (oct. 2017).*

Uniunea Europeană, *Regulamentul nr. 211/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 privind inițiativa cetățenească.*

Comisia Europeană pentru Democrație prin Drept (Comisia de la Veneția) și colab., *Raport comun privind tehnologiile digitale și alegerile (iunie 2019).*

Comisia Europeană pentru Democrație prin Drept (Comisia de la Veneția), *Compilarea avizelor și rapoartelor Comisiei de la Veneția privind tehnologiile digitale în procesul electoral, CDL-PI(2018)011 (2018).*

Comisia Europeană pentru Democrație prin Drept (Comisia de la Veneția), Grabenwarter, Cap. *Raport privind compatibilitatea votului la distanță și votului electronic cu standardele Consiliului Europei, 2004.*

Comisia Europeană pentru Democrație prin Drept (Comisia de la Veneția), *Cod de bune practici în chestiuni electorale - Ghid și raport explicativ* (2002).

IDEA, *Securitatea cibernetică în alegeri. Modele de colaborare interagenții, 2019.*

IDEA, RECEF, *Utilizarea noilor tehnologii în procesele electorale - Raport al atelierului de lucru:*
Praia, Cabo Verde, 22–23 noiembrie 2017.

IDEA, *Certificarea TIC în cadrul alegerilor, 2015.*

IDEA, *Proiect de management electoral, Ediție revizuită, 2014.*

IDEA, *Obligații internaționale pentru alegeri, Ghid privind cadrele juridice, 2014.*

IFES, Goldsmith, B./Ruthrauff, H., *Implementarea și supravegherea tehnologiilor electronice de vot și numărare, 2013.*

OSCE/OIDDO, *Manual pentru observarea noilor tehnologii de vot, 2013.*

OSCE/OIDDO, *Ghid privind revizuirea unui cadru juridic pentru alegeri, 2013.*

OSCE/OIDDO, A se vedea Rapoartele „Misiunii de evaluare a nevoilor" și „Misiunii de evaluare a alegerilor" privind alegerile desfășurate în țările din regiunea Consiliului Europei. A se vedea, în mod special, secțiunile „Cadrul juridic", „Noile tehnologii de vot" și „Recomandări" din rapoartele respective, disponibile la www.osce.org/elections.

Comisia la nivel înalt a Secretarului General al ONU, *Era interdependenței digitale, iunie 2019.*

Adunarea Generală a ONU, Consiliul pentru Drepturile Omului, Raportul Oficiului Înaltului Comisar al Națiunilor Unite pentru Drepturile Omului – Proiect de ghid pentru state privind implementarea efectivă a dreptului de a participa la afacerile publice (septembrie 2018).

Cercetări relevante privind aspectele juridice și de reglementare

Barrat J. *(2016),* (Coord.) *El voto electronic y sus dimensiones jurídicas: entre la ingenua complacencia y el rechazo precipitado, Iustel.*

Barrat J. și Goldsmith B. (2012), *Conformitatea cu standardele internaționale*, *proiect norvegian privind votul electronic.*

Benaloh J., Rivest R., Ryan P. și colab. *(2014), Verificabilitatea întregului proces.*

Cardillo și colab., *Votul online în alegerile municipale din Ontario: Un conflict între principiile juridice și tehnologie?, în Krimmer R. și colab. (Ed.), E-Vote-ID 2019.*

Driza Maurer A., *Exercițiul de transparență Swiss Post/Scytl și posibilul impact al acestuia asupra reglementării votului pe internet, în Krimmer R. și colab. (Ed.): E-Vote-ID 2019.*

Driza Maurer A., Barrat J. (Ed.), *Jurisprudența votului electronic: O analiză comparativă, Routledge 2017.* Publicația include capitole referitoare la cadrul juridic al tehnologiilor digitale utilizate în alegerile din Germania, Austria, Brazilia, India, Estonia, Franța, Argentina, Finlanda, Mexic, Elveția, SUA, Australia și Venezuela.

Driza Maurer A., *Standarde europene actualizate pentru votul electronic. Recomandarea Consiliului Europei Rec(2017)5 privind standardele pentru votul electronic, în R. Krimmer și colab. (Ed.): E-Vote-ID 2017.*

Driza Maurer A. *(2016), Actualizare a Recomandării Consiliului Europei privind standardele juridice, operaționale și tehnice pentru votul electronic – o perspectivă juridică. În: Tagungsband IRIS (Internationales Rechtsinformatik Symposion).*

Driza Maurer A., *Zece ani Rec (2004)11 a Consiliului Europei. Lecții învățate și perspective. În: Krimmer, R., Volkamer, M. (ed.) (2016), Procedura de vot electronic 2014.*

Driza Maurer A., *Votul pe internet și federalismul: Cauza elvețiană, în Barrat J. (Coord.) El voto electronic y sus dimensiones jurídicas : entre la ingenua complacencia y el rechazo precipitado, Iustel.*

Gibson P., Krimmer R. și colab. (2016), *O revizuire a votului electronic: trecut, prezent și viitor.*

Hill R., *Votul electronic și legea. Probleme, soluții și o întrebare provocatoare. În Krimmer, R. și colab. (ed.), Procedurile E-VOTE-ID 2016.*

Krimmer și colab. (Ed.), A se vedea lucrările conferințelor E-Vote-ID, 2019, 2018, 2017, 2016.

Loeber L., *Legiferarea pentru alegerile activate electronic: dileme și preocupări pentru legiuitor. În Krimmer R. și colab. (ed.) Procedurile E-VOTE-ID 2016.*

Loeber L. „*Votul electronic în Olanda; de la acceptarea generală la îndoiala generală în doi ani*" *în Krimmer, R. și Grimm R. (Ed.) (2008), Votul electronic 2008 (EVOTE08).*

Madise Ü. și Vinkel P. (2011), „*Constituționalitatea votului prin internet la distanță: Perspectiva estoniană*", *Juridica International.*

Mohanty și colab. (2019), *Auditarea alegerilor din India.*

Neumann S., Volkamer M., *Un cadru holistic pentru evaluarea sistemelor de vot pe internet. În: Zissis D., Lekkas D. (ed.) (2014), Proiectarea, dezvoltarea și utilizarea sistemelor de vot electronic securizate, seria de cărți IGI Global*

Neumann S. (2016), *Evaluarea și îmbunătățirea schemelor de vot pe internet pe baza cerințelor de securitate fundamentate juridic.*

Puiggali J., Rodriguez-Peréz A.*, Proiectarea unui cadru național pentru votul online și îndeplinirea cerințelor acestuia: experiența elvețiană. În Krimmer și colab. (ed.) E-Vote-ID 2018 Proceduri.*

Saltman Roy (2008), *Istoria și politica tehnologiei de vot. În căutarea integrității și a încrederii publice.*

Schwartz B. și Grice D. (2013), *Stabilirea unui cadru juridic pentru votul electronic în Canada.*

Solvak M., Vassil K., *Votul electronic în Estonia: Difuzia tehnologică și alte evoluții pe parcursul a zece ani (2005-2015).*

Spycher O., Volkamer M. și Koenig R. (2011), *Transparență și măsuri tehnice pentru a stabili încrederea în votul prin internet norvegian.*

Taylor G. (2010), *Restricții constituționale privind calculatoarele de vot cu ecran tactil din Germania, în Election Law Journal, volumul 9, numărul 4.*

Comisia de la Veneția/Autoritatea Electorală Permanentă a României, *Expert electoral, Procedurile primelor dezbateri ale experților științifici electorali „Legea electorală și noile tehnologii: Provocări juridice", București, 12 - 13 aprilie 2016* (contribuții ale mai multor experți).

Vinkel P. *(2015), Votul electronic la distanță în Estonia: Legalitate, impact și încredere, TUT Press.*

Volkamer M., Spycher O. și Dubuis E. *(2011), Măsuri pentru a stabili încrederea în votul prin internet.*

Volkamer M. (2009), Evaluarea votului electronic, cerințele și procedurile de evaluare pentru sprijinirea autorităților electorale responsabile, Springer-Verlag Berlin Heidelberg.

Documente relevante din țările selectate

- Austria, *Legea privind Sindicatul Studenților (Bundesgesetz über die Vertretung der Studierenden [Hochschülerinnen- und Hochschülerschaftsgesetz 1998 – HSG 1998]), Monitorul Oficial Federal I 1999/22, ultima modificare Monitorul Oficial Federal I 2013/79. În 2014, Legea privind Sindicatul Studenților din 1998 a fost înlocuită de Legea privind Sindicatul Studenților din 2014, Monitorul Oficial Federal I 45/2014.*

- Austria, Curtea Constituțională (*Verfassungsgerichtshof*) *Decizia V 85-96/11-15, 13 decembrie 2011. Pentru o discuție detaliată, a se vedea capitolul privind Austria de Melina Oswald, „Votul electronic în Austria: Probleme de determinare juridică" în Driza Maurer/Barrat (Ed.), Jurisprudența votului electronic: o analiză comparativă, 2017.*

- Belgia, (Legea privind votul electronic cu pistă de audit pe hârtie) *Loi du 7 fevrier 2014 organisant le vote électronique avec preuve papier (Moniteur belge du 14 février 2014).*

- Finlanda, Ministerul Justiției, *Raportul grupului de lucru „Votul online în Finlanda – Studiu de fezabilitate" 19.12.2017.*

- Franța, Commission Nationale de l'Informatique et des Libertés (CNIL), *Délibération n° 2019-053 du 25 avril 2019 important adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.*

- Franța*, Rapport d'information n° 73 (2018-2019) de Mme Jacky Deromedi et M. Yves Détraigne, fait au nom de la commission des lois, déposé le 24 octobre 2018 "Réconcilier le vote et les nouvelles technologies".*

- Franța, Sénat, Commission des lois, *Rapport d'information de MM. Alain Anziani et Antoine Lefevre, "Vote électronique: Préserver la confiance des électeurs" 2014.*

- Germania, *Ordonanța privind utilizarea dispozitivelor de numărare a voturilor în alegerile pentru Bundestag-ul german (Verordnung über die Verwendung von Stimmenzählgeräten bei Wahlen zum Deutschen Bundestag) (BGBl. 1961 I 1618).*

- Germania, Curtea Constituțională *(Bundesverfassungsgericht), Decizia 2 BvC 3/07, 2 BvC 4/07, of 3 martie 2009. Pentru o discuție detaliată, a se vedea capitolul referitor la Germania de Sebastian Seedorf, „Germania: Caracterul public al alegerilor și consecințele acestuia pentru votul electronic" în Driza Maurer/Barrat (ed.), Jurisprudența votului electronic: o analiză comparativă, 2017.*

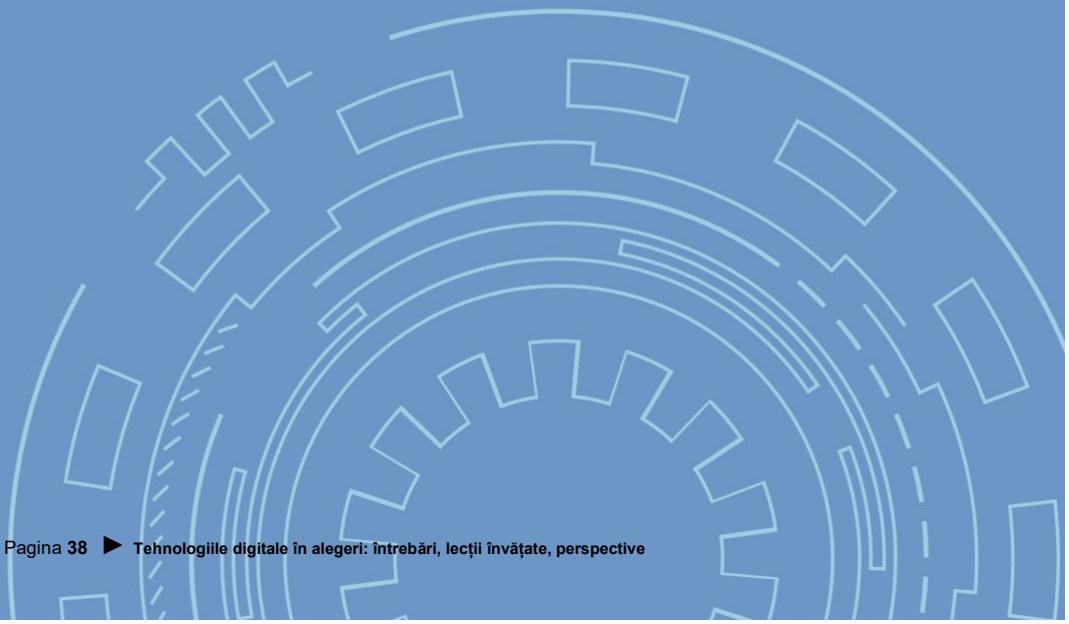
- Olanda, Comisia consultativă privind procesul electoral, *Raport: Votând cu încredere. Rezumat, concluzii și recomandări (2007).*

- *Ordonanța Cancelariei Federale* Elveține *privind votul electronic (VEleS), RS 161.116.*

- *Consiliul Federal* Elvețian, (Primul raport guvernamental privind fezabilitatea votului electronic) *„Rapport sur le vote électronique. Chances, risques et faisabilité" din 9 ianuarie 2002, FF 2002 612 (2002).*

- *Consiliul Federal* Elvețian, (Al doilea raport guvernamental privind evaluarea programelor pilot) "*Rapport sur les projets pilotes en matière de vote électronique" of 31 May 2006, FF 2006 5205 (2006).*

- *Consiliul Federal* Elvețian, (Al treilea raport guvernamental privind evaluarea experiențelor și bazele pentru dezvoltarea viitoare a votului electronic) „Rapport du Conseil fédéral sur le vote électronique. *Evaluation de la mise en place du vote électronique (2006–2012) et bases de développement" of 14 iunie 2013, FF 2013 4519 (2013).*



Prezentare generală a tehnologiilor digitale utilizate în ciclul electoral**

Cuprins

1. ABORDARE ȘI DEFINIȚII	**40**
a. Introducere	41
b. Ciclul electoral	43
c. Noile tehnologii	43
2. CONTESTAREA CONFORMITĂȚII NOILOR TEHNOLOGII CU ARTICOLUL 3 AL PROTOCOLULUI Nr. 1 LA CONVENȚIA EUROPEANĂ A DREPTURILOR OMULUI	**44**
a. Perspectiva tehnologică	44
b. Perspectiva ciclului electoral	53
3. PROBLEME DE SINTEZĂ ȘI TRANSVERSALE	**57**
4. REFERINȚE SELECTATE	**59**

** Aceasta este o versiune prescurtată a lucrării „Noile tehnologii în ciclul electoral. Ghid al Consiliului Europei" prezentat de autor grupului de lucru pentru democrație și tehnologie al Comitetului European pentru Democrație și Guvernare (CEDG) al Consiliului Europei, la 28 ianuarie 2020. Comitetul European pentru Democrație și Guvernare (CEDG) a primit sarcina specifică de a elabora standarde privind utilizarea noilor tehnologii în diferitele etape ale procesului electoral. Această sarcină a fost atribuită de grupul de lucru pentru democrație și tehnologie.

1. ABORDARE ȘI DEFINIȚII

a. Introducere

Lucrarea de față oferă o imagine de ansamblu asupra principalelor tehnologii digitale utilizate sau avute în vedere în timpul unui ciclu electoral și identifică problemele de conformitate cu principiile alegerilor democratice. Aceasta este o versiune prescurtată a lucrării „Noile tehnologii în ciclul electoral. Ghid al Consiliului Europei" prezentat în cadrul grupului de lucru pentru democrație și tehnologie al Comitetului European pentru Democrație și Guvernare (CEDG) al Consiliului Europei, la 28 ianuarie 2020.1

În calitate de gardian al valorilor consacrate în Convenția Europeană pentru Protecția Drepturilor Omului și a Libertăților Fundamentale (Convenția Europeană a Drepturilor Omului sau Convenția) și protocoalele la aceasta, Consiliul Europei are misiunea de bază de a supraveghea punerea în aplicare a Convenției în țările din regiune, inclusiv în activitățile aferente alegerilor. În conformitate cu articolul 3 din Protocolul nr. 1 la Convenție și jurisprudența Curții Europene a Drepturilor Omului, Organul Electoral (și anume Statul) are obligația pozitivă de a se asigura că toate activitățile conduse de acesta în cadrul unui ciclu electoral respectă dreptul la alegeri libere, inclusiv cele susținute de noile tehnologii. Acest raport se concentrează pe respectarea și implementarea articolului 3 din Protocolul Nr. 1 la Convenție2 de noile tehnologii utilizate în ciclul electoral. Mai precis, accentul este pus pe principiile sufragiului universal, egal, liber și secret și pe unele condiții pentru implementarea acestor principii (de exemplu, garanții procedurale de imparțialitate, transparență și observare etc.).3 Alte principii relevante pentru alegeri, cum ar fi libertatea de opinie și de exprimare, libertatea de întrunire pașnică, libertatea de asociere, libertatea de mișcare, libertatea de a nu fi discriminat, dreptul la o cale de atac efectivă, trebuie, de asemenea, luate în considerare. Totuși, acestea nu vor fi discutate aici.

Soluțiile digitale îmbunătățesc și facilitează procesele electorale, dar aduc și provocări și riscuri. Acestea pot crește eficiența și viteza, pot ajuta la evitarea erorilor de lucru manual etc., dar pot, de asemenea, să creeze noi vulnerabilități, să expună sistemul electoral la noi amenințări și să permită noi atacuri asupra acestuia. Autoritatea de reglementare trebuie să ia decizii în cunoștință de cauză, pentru ca noile tehnologii să fie introduse și puse în funcțiune

---

1. Pentru a afla despre activitatea Consiliului Europei în alegeri și pentru a obține îndrumări cu privire la utilizarea tehnologiilor digitale în domeniul electoral, consultați www.coe.int, în special, lucrările actuale ale Comitetului European pentru Democrație și Guvernare (CEDG), cea a Diviziei de Asistență Electorală și a Comisiei Europene pentru Democrație prin Drept (Comisia de la Veneția), printre altele.
2. 45 din 47 de state membre au ratificat acest protocol. Elveția și Monaco l-au semnat, dar nu l-au ratificat încă. Cu toate acestea, cu excepția lipsei acceptate a secretului în (doar) unele alegeri locale, în care este utilizat votul prin ridicarea mâinii, principiile electorale ale dreptului elvețian sunt, de obicei, considerate a fi mai stricte în comparație cu P1-3 CEDO.
3. Comisia de la Veneția, Codul de bune practici în materie electorală, Avizul Nr. 190/2002, adoptat de Comisia de la Veneția la a 52-a sesiune (Veneția, 18-19 octombrie 2002); CDL-AD (2002) 23 rev. Aplicarea principiilor sufragiului direct și frecvența alegerilor nu pare să fie afectată de tehnologia utilizată în ciclul electoral.

în condiții de siguranță. Utilizarea în siguranță implică faptul că soluțiile digitale (la fel ca orice aspect al unei alegeri) respectă principiile alegerilor democratice și, astfel, asigură, printre altele, sufragiul universal, egal, liber și secret.

Toate țările din regiune au subscris la standardele internaționale minime pentru alegeri democratice. Acestea se regăsesc în articolul 25 din Pactul internațional cu privire la drepturile civile și politice (PIDCP) din 1966 și articolul 3 din Protocolul nr. 1 la Convenția Europeană a Drepturilor Omului4 privind dreptul la alegeri libere.5 Acestea sunt elaborate în continuare în angajamentele politice (Documentul CSCE de la Copenhaga din 1990 obligă statele participante să garanteze drepturile omului și libertățile fundamentale, inclusiv cele referitoare la alegeri), jurisprudența Curții Europene a Drepturilor Omului și instrumentele juridice fără caracter obligatoriu *(soft law)* (Comentariul general UNHRC nr. 25 din 1996 și Codul de bune practici al Comisiei de la Veneția din 2002 privind chestiuni electorale și Codul de bune practici privind referendumurile din 2007).

Lucrarea oferă o privire de ansamblu asupra unor tehnologii noi care au fost introduse sau luate în considerare pentru a fi utilizate în ciclul electoral, principalele caracteristici ale acestora și problemele de conformitate. Apoi, aceasta analizează diferitele faze ale ciclului electoral și soluțiile digitale utilizate sau luate în considerare și conformitatea acestora. Lucrarea se încheie cu un rezumat și câteva întrebări transversale relevante pentru toate noile tehnologii și toate fazele ciclului electoral.

Lucrarea se bazează pe lucrările anterioare de la Consiliul Europei în domeniul votului electronic (a se vedea Recomandarea CM/Rec(2017)5 privind standardele pentru votul electronic, denumită în continuare Recomandarea CM/Rec(2017)5). De asemenea, sunt luate în considerație lucrări ale Comisiei de la Veneția, Divizia Consiliului Europei pentru asistență electorală și societatea civilă, Convenția Consiliului Europei privind criminalitatea informatică (Convenția de la Budapesta) și Convenția modernizată pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal (Convenția 108+), precum și lucrările altor organizații precum OSCE/OIDDO, International IDEA, UE etc.

b. Ciclul electoral

Un ciclu electoral cuprinde toți pașii și procesele care sunt necesare pentru ca o alegere sau un vot să aibă loc.6 Organul Electoral (OE), autoritatea responsabilă cu organizarea alegerilor, desfășoară și/sau controlează activitățile unui ciclu electoral. Noțiunea de „ciclu” implică și faptul că acești pași se repetă la intervale regulate,

4. 45 din cele 47 de state membre ale Consiliului Europei au ratificat acest protocol. Elveția și Monaco l-au semnat, dar nu l-au ratificat încă. Cu toate acestea, în Elveția, de exemplu, principiile electorale federale și cantonale sunt de facto mai stricte în comparație cu articolul 3 din Protocolul Nr. 1 la Convenție. Singura excepție este lipsa secretului în unele alegeri locale, în care este utilizat votul prin ridicarea mâinii, ceea ce este acceptat de Curtea Supremă din motive istorice și practice, în ciuda criticilor din partea doctrinei juridice.

5. Articolul 3 din Protocolul nr. 1 la Convenție prevede: „Înaltele părți contractante se angajează să organizeze alegeri libere la intervale rezonabile prin vot secret, în condiții care să asigure libera exprimare a opiniei poporului în alegerea legislativului”.

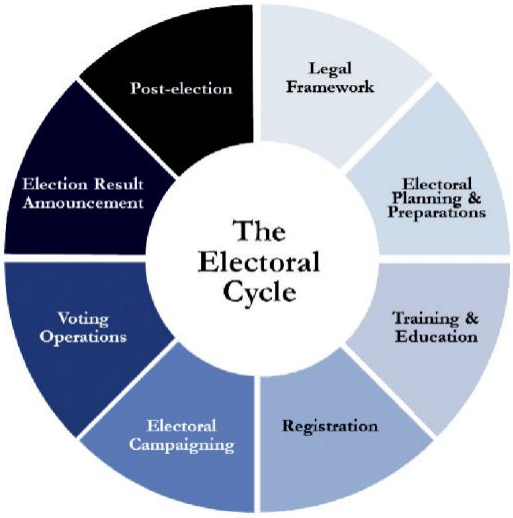
6. Ne referim la ciclul electoral așa cum este definit de IDEA în *Conceptul de management electoral*, 2014: *12; 16; 75-77*, cu mici modificări și completări.

pentru fiecare alegere.7 Principalele faze ale unui ciclu electoral sunt următoarele:

Cadrul juridic. Acesta include proiectarea și elaborarea legislației.

Planificarea și pregătirea pentru punerea în aplicare a activităților electorale. Aceasta include recrutarea și formarea personalului electoral, precum și planificarea electorală.

Formarea și educarea alegătorilor, reglementarea conduitei observatorilor.



Sursă: IDEA

Înregistrarea alegătorilor, a partidelor politice și a observatorilor electorali; nominalizarea partidelor și candidaților. Înregistrarea și tratarea problemelor/întrebărilor care pot duce la un referendum (vot popular).

Campanie electorală, inclusiv informații oficiale adresate alegătorilor.

Operațiuni de votare, inclusiv sondaje, numărare și tabelare a rezultatelor.

Anunțarea **rezultatelor alegerilor**, inclusiv transmiterea și publicarea rezultatelor, soluționarea disputelor electorale, raportare, auditare.

Atribuții postelectorale inclusiv distrugerea și/sau arhivarea materialelor.8

Desfășurarea voturilor democrației directe presupune pași similari și suplimentari, precum aprobarea formală și/sau materială a propunerii (inițiativă sau referendum), controlul formularului de strângere a semnăturilor susținătorilor, primirea și controlul valabilității semnăturilor, numărarea, validarea și publicarea rezultatelor și, în cele din urmă, organizarea votului dacă s-a colectat cu succes numărul necesar de semnături valabile. Includem toți acești pași în faza de înregistrare (Nr. 4 de mai sus). După

7. Ciclul electoral a fost conceptualizat de International IDEA și Comisia Europeană în 2005. Scopul a fost acela de a ilustra faptul că alegerile nu sunt evenimente, ci procese și de a integra aceste cunoștințe pe parcursul fazelor de planificare și implementare a tuturor proiectelor de asistență electorală — vizând angajamentele pe termen lung de fonduri și alte resurse, un accent pe sustenabilitate în cadrul instituțiilor electorale și un angajament general față de dezvoltarea democratică a unei țări, care depășește cu mult în viitor evenimentul imediat care urmează să fie susținut, https://www.idea.int/data-tools/tools/online-electoral-cycle

8. Secvența cronologică reală a fazelor poate fi diferită de cea prezentată mai sus.

aceea, OE informează alegătorii, planifică și efectuează votul etc. În această lucrare, termenul alegeri/ciclu electoral se referă atât la alegeri, cât și la voturile democrației directe.

Lucrarea are în vedere utilizarea noilor tehnologii în diferitele faze ale ciclului electoral, cu excepția problemelor privind formarea opiniei și finanțarea alegerilor, care sunt tratate în alte fluxuri de lucru la nivelul Consiliului Europei.

c. Noile tehnologii

În prezenta lucrare, termenii „nou” și „digital” sunt utilizați ca sinonime. Tehnologiile și soluțiile digitale utilizate, testate sau avute în vedere în ciclul electoral sunt digitizarea documentelor și a procedurilor, biometria, blockchain-ul, informatica dematerializată *(cloud computing)*. Se discută despre inteligența artificială, cu excepția utilizării acesteia în domeniul formării de opinie (campanii electorale).

Soluțiile digitale stochează și manipulează informațiile digital și nu pot fi observate sau înțelese de neprofesioniști. Tehnologiile mai complexe, cum ar fi inteligența artificială, pot evolua astfel încât funcționarea lor detaliată să nu fie înțeleasă nici măcar de inginerii care le-au construit. Așadar, principala caracteristică a unor astfel de tehnologii este complexitatea acestora. În plus, ele evoluează rapid. Acest lucru le face diferite din punct de vedere calitativ de tehnologiile și soluțiile „vechi” pe hârtie sau mecanice.

2. CONTESTAREA CONFORMITĂȚII NOILOR TEHNOLOGII CU ARTICOLUL 3 DIN PROTOCOLUL Nr. 1 LA CONVENȚIA EUROPEANĂ A DREPTURILOR OMULUI

a. Perspectiva tehnologică

Digitalizare

Existența tehnologiei digitale și aplicarea acesteia la aproape toate aspectele vieții, inclusiv în alegeri, este un fapt care nu poate fi pus sub semnul întrebării.9 Digitalizarea este primul nivel, care permite tratarea informatică a informațiilor. Aceasta este conversia textului, imaginilor și sunetului într-o formă digitală care poate fi procesată de un calculator.

Datele digitizate includ registrele alegătorilor, registrele candidaților, rezultatele introduse în format electronic etc. Procesele digitalizate includ înregistrarea electronică, identificarea electronică a alegătorilor, votul electronic la dispozitivele de vot din secțiile de votare sau prin internet, numărarea electronică (care implică un program software utilizat pentru înregistrarea și calcularea rezultatelor și poate și alocarea de locuri), program software utilizat în scopuri statistice, transmiterea electronică a rezultatelor preliminare și/sau finale, de exemplu, de la secțiile de votare la o unitate centrală etc. Digitizarea proceselor este mai problematică atunci când tranzitează pe internet, din cauza aspectelor de securitate cibernetică. Datele și procesele digitizate pot fi grupate în sisteme de informare și management electoral.

În alineatele următoare, includem informații dintr-un chestionar pregătit și distribuit de CEDG și la care mai multe țări au răspuns până la sfârșitul anului 2019. Chestionarul a fost scurt și s-a concentrat pe punerea în aplicare a Recomandării CM/Rec(2017)5. Răspunsurile au fost oferite de diferite birouri, nu în mod sistematic de OE-uri. În ciuda acestor limitări, răspunsurile oferă o imagine de ansamblu actuală, deși nu exhaustivă, a tehnologiilor digitale utilizate în procesele electorale.

Votul electronic reprezintă cea mai supravegheată utilizare a noilor tehnologii în ciclul electoral, deoarece acoperă cel mai sensibil proces al unui ciclu electoral, și anume, votul efectiv și rezultatul alegerilor. Acesta este, de asemenea, cel mai avansat exemplu de utilizare a noilor tehnologii, deoarece, de obicei, nu este vorba doar de digitizarea proceselor de vot și numărare, ci implică, în mod ideal, ca toate documentele și procesele implicate să fie digitizate, astfel încât tranzacțiile să poată avea loc fără discontinuitate media.

Potrivit Recomandării CM/Rec(2017)5, votul electronic cuprinde exprimarea electronică a votului și numărarea electronică a buletinelor de vot pe hârtie. Exprimarea electronică a votului include atât votul la aparatele electronice de vot (denumite în continuare AEV) în secțiile de votare, cât și votul prin internet dintr-un mediu necontrolat (denumit în continuare

9. Comisia Europeană pentru Democrație prin Drept (Comisia de la Veneția) și colab., 2019, „Raport comun privind tehnologiile digitale și alegerile”

votul prin internet). exprimarea electronică a votului implică numărarea electronică. Există, de asemenea, numărarea electronică pură a buletinelor de vot de hârtie prin utilizarea de scanere optice, care digitizează buletinul de vot pe hârtie și apoi procedează la numărătoare.

Votul electronic este practicat în câteva țări, așa cum se arată în răspunsurile la chestionar, inclusiv în *Belgia* (AEV pentru toate tipurile de alegeri și referendumuri); *Bulgaria* (AEV numai pentru alegerile naționale și UE, precum și pentru alegerea președintelui și vicepreședintelui Republicii Bulgaria, dar nu și pentru referendumuri); *Estonia* (votul prin internet pentru toate alegerile naționale, dar nu pentru referendumurile locale, care utilizează diferite soluții tehnice); regiunea autonomă *Åland* din *Finlanda* (votul prin internet, recent suspendat); *Franța* (AEV în 66 de comune și votul prin internet pentru francezii expatriați, în timpul alegerilor parlamentare și consulare; la nivel local, consiliile municipale pot utiliza votul prin internet pentru a vota); *Islanda* și *Norvegia* (votul prin internet doar pentru referendumurile locale); *Federația Rusă* (AEV pentru alegerile naționale și regionale); *Elveția* (votul prin internet pentru voturile și alegerile federale, cantonale și comunale; în prezent, suspendat).

Răspunsurile la chestionarul CEDG arată că numărarea electronică pură (tehnologia de recunoaștere optică a caracterelor) este practicată în *Ungaria* (numai pentru rezultatele preliminare), *Letonia, Malta* (din mai 2019, alegerile pentru Parlamentul European și pentru consiliile locale), *Norvegia, Elveția* (unele cantoane scanează și numără buletinele de vot pe hârtie la voturile referendumului), *Federația Rusă*, precum și *Regatul Unit* (*Anglia* l-a utilizat din 2000 la alegerile locale și naționale; *Scoția* l-a utilizat la alegerile locale și naționale din 2007). Cu această ocazie, s-au constatat erori semnificative în proiectarea buletinului de vot. Numărarea electronică a fost utilizată din nou la alegerile locale din 2012 și 2017, cu succes. Numărarea buletinelor de vot [sistemul de vot unic transferabil] a fost redusă de la trei/patru zile la câteva ore).

Votul electronic este avut în vedere în *Azerbaidjan, Franța*10 *România*,11 *Serbia*,12 *Ucraina*,13 *Regatul Unit*.14 Acesta a fost suspendat sau desființat parțial sau total în

10. Un raport din 2018 al Senatului francez (Deromedi, Detraigne) a recomandat utilizarea votului electronic la alegerile consulare din 2020 și la alegerile parlamentare din 2022. Guvernul francez a aprobat recent soluția votului prin internet pentru alegerile din 2020.

11. Autoritatea Electorală Permanentă a României ia în considerare votul electronic, cu toate acestea, potrivit răspunsului, este posibil ca punerea în aplicare să nu înceapă înainte de sfârșitul anului 2020, deoarece unii actori politici și instituții administrative nu au încredere în această tehnologie.

12. O posibilă lege viitoare privind referendumurile și inițiativele populare consideră inițiativa electronică ca o încercare inițială a votului electronic în Serbia.

13. Potrivit răspunsului, se pregătește o lege privind referendumurile naționale și locale care ia în considerare opțiunea votului electronic.

14. Un test fără caracter obligatoriu a avut loc în mai 2019 în cadrul alegerilor locale. Se presupune că acesta prezenta un sistem verificabil integral, cuprinzând calculatoare cu ecran tactil la cabina de votare, coduri de acces emise alegătorilor, chitanțe pe hârtie verificabile ale alegătorului, publicarea voturilor criptate pe site-ul electoral, sistemul semnalând dacă vreun vot electronic a fost modificat în mod ilegitim. Procesul a avut loc într-un context în care guvernele din Țara Galilor și Scoția au propus proiecte pilot de vot electronic în alegerile locale.

Bulgaria,15 *Finlanda*,16 *Franța*,17 *Germania*,18 *Irlanda*, *Olanda*,19 *Norvegia*,20 *Elveția* 21 și *Regatul Unit*.22

Votul electronic a fost luat în considerație pentru alegerile politice, dar nu a fost lansat în *Austria*,23 *Republica Cehă, Danemarca, Finlanda*24 *Letonia25 Spania*.26 Principalele argumente împotriva introducerii votului electronic se referă la securitate, complexitate și cost.

Digitizarea documentelor și proceselor ciclului electoral este totuși larg răspândită. Iată o prezentare generală bazată pe răspunsurile la chestionarul CEDG care au fost transmise la sfârșitul anului 2019.

Datele și procesele de bază sunt digitizate în *Finlanda, Ungaria, Letonia* (de exemplu, districte electorale, municipalități, circumscripții electorale, autorități electorale, pregătirea și publicarea listelor de candidați, pregătirea schemelor de vot).

Serviciile sau procesele digitizate, care sunt utilizate înainte de ziua votării, includ servicii electronice pentru ca alegătorii să își găsească sau schimbe secția de votare (*Ungaria*); să solicite votul prin corespondență (*Letonia*); sau să își verifice și modifice detaliile electorale (*Irlanda*) sau să se înregistreze pentru vot în străinătate (*Spania*); colectarea de semnături pentru noile partide care doresc să candideze la alegeri (*Danemarca*); 27 colectare de semnături pentru referendumuri naționale sau locale (*Franța*).

15. În 2019, Parlamentul bulgar a abolit votul electronic pentru alegerile locale din cauza complexității acestor alegeri și a costului financiar al votului electronic.

16. Acesta a fost desființat după ce un test pentru alegerile municipale din 2008 a identificat mai multe probleme.

17. Din 2008, un moratoriu a suspendat orice extindere a AEV-urilor către noi comune. La ultimele alegeri naționale, votul prin internet a fost anulat. Cu toate acestea, se preconizează ca acesta să fie utilizat în 2020 și 2022, astfel cum se recomandă în raportul Senatului din 2018.

18. Decizia Curții Constituționale Federale din 3 martie 2009, BVerfGE 123, 39. Decizia a declarat Ordonanța federală privind dispozitivele de vot (*Bundeswahlgeräteverordnung of 3 septembrie 1975, BGBl. 1975 I 2459, modificat ultima dată prin articolul 1 din Ordonanța din 20 aprilie 1999, BGBl. 1999 I 749*) ca fiind incompatibilă cu principiul caracterului public al alegerilor conform căruia specialiștii trebuie să poată urma și înțelege principalele etape ale procesului electoral fără cunoștințe tehnice speciale.

19. În 2006, după decenii de vot electronic, AEV a fost supus unor critici dure în Olanda pentru lipsa de securitate și posibilitate de audit. Din 2008, votul se desfășoară numai cu buletine de vot pe hârtie.

20. După ce a organizat procese în 2011 și 2013, în 10 și, respectiv, 12 municipalități, guvernul norvegian a întrerupt votul electronic din cauza lipsei de voință politică de a-l consacra drept un canal obișnuit. Acesta rămâne o opțiune doar pentru referendumurile locale.

21. De la jumătatea anului 2019, votul prin internet a fost suspendat în Elveția, de facto, deoarece niciun sistem de vot prin internet nu îndeplinește cerințele legale.

22. După procesele de la alegerile locale din Anglia între 2002 și 2007, votul electronic a fost întrerupt, în principal, din cauza problemelor de complexitate și transparență; s-a considerat că riscurile depășesc avantajele și lipseau o viziune, o strategie clare, o planificare eficientă, rentabilitatea și certificarea sistemului.

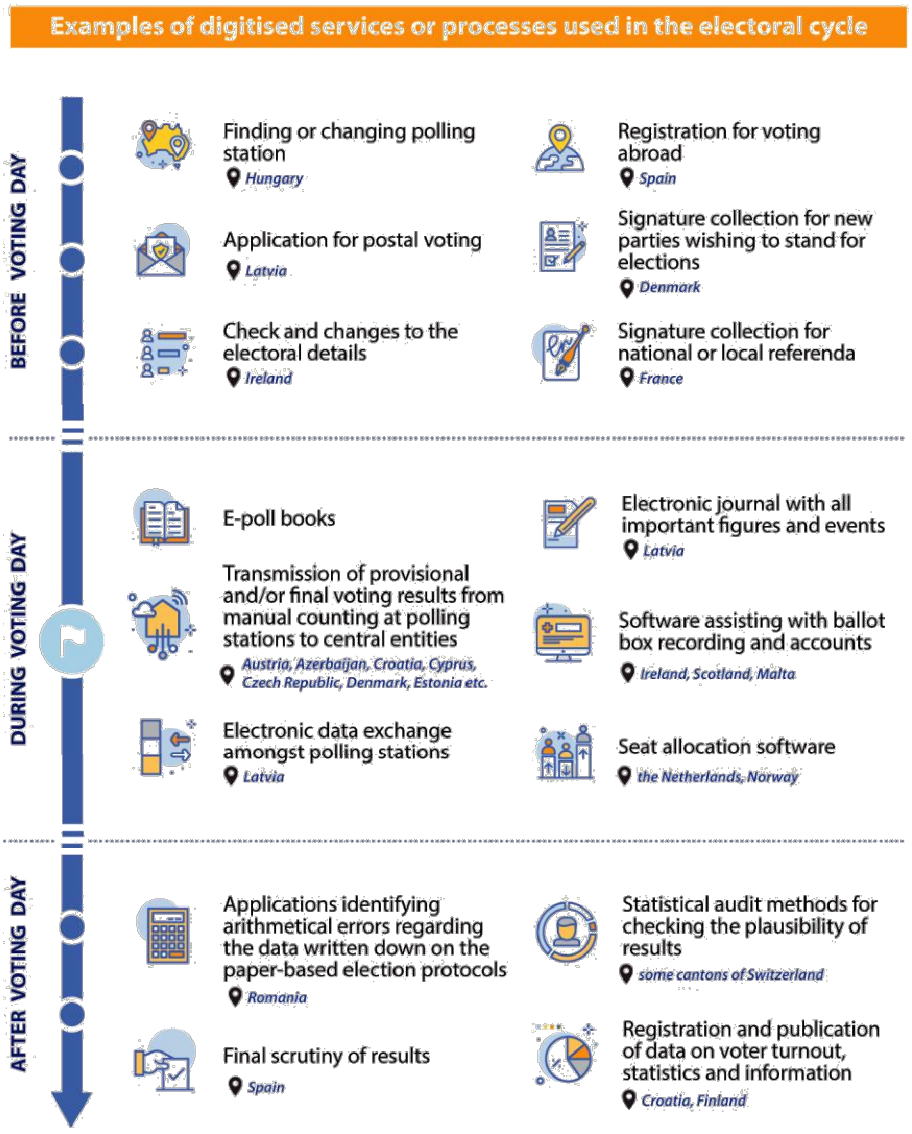
23. O decizie a Curții Constituționale din 2011 a stabilit că comisia electorală trebuie să înțeleagă toți pașii și procedurile votului prin internet fără asistență din partea experților tehnici, un lucru imposibil de realizat.

24. Un raport a concluzionat, la sfârșitul anului 2017, că riscurile votului prin internet depășesc, în prezent, beneficiile.

25. Potrivit răspunsului la chestionar, unele discuții din parlament arată că introducerea votului electronic este din nou avută în vedere, deși nu este un concept popular.

26. Votul prin internet a fost discutat doar pentru spaniolii care locuiesc în străinătate.

27. După experiențele inițiale și problemele identificate, Parlamentul danez a decis în 2019 să procure un sistem reproiectat.



Serviciile sau procesele digitizate disponibile în timpul și după ziua votării (în afara oricărui vot electronic) includ *jurnalul* electronic cu toate cifrele și evenimentele importante (*Letonia*);28 cărți electronice de votare; schimbul electronic de date între secțiile de votare, asigurând posibilitatea alegătorilor de a vota la orice secție de votare în timpul zilelor de vot anticipat (*Letonia*); transmiterea rezultatelor votului provizoriu și/sau definitiv din numărarea manuală la secțiile de votare către entitățile centrale unde sunt consolidate, numărate și publicate, după caz (în *Austria*, *Azerbaidjan*, *Croația*,

28. Un proiect pilot a avut loc la alegerile pentru Parlamentul European din 2019 din Letonia.

Cipru, Cehia, Danemarca, Estonia, Finlanda, Grecia, Germania, Ungaria, Letonia, Norvegia, România, Slovacia, Slovenia, Spania, Olanda); program software care asistă responsabilii electorali cu înregistrarea urnelor și conturile în conformitate cu sistemul de reprezentare proporțională-vot unic transferabil (RP-VUT) (*Irlanda, Scoția, Malta*); program software de alocare a locurilor (*Olanda, Norvegia* etc.).

Un tip important de document digitizat, care poate fi utilizat aproape peste tot în regiune sunt registrele: registrele alegătorilor și candidaților, registre care țin evidența celor care au votat deja în timpul unei alegeri (utilizarea dreptului de vot). Pe lângă țările care utilizează *exprimarea electronică a votului*, acestea sunt utilizate și în *Finlanda, Ungaria, Letonia, Norvegia, Serbia* și *Slovenia*.

Serviciile sau procesele digitizate disponibile după ziua votării includ soluții de *verificare* a rezultatelor, inclusiv aplicații de identificare a erorilor aritmetice privind datele înscrise pe protocoalele electorale pe hârtie (*România*);29 sau metode de audit statistic pentru verificarea plauzibilității rezultatelor; scrutinul final al rezultatelor (*Spania*);30 înregistrarea și publicarea datelor privind prezența la vot, statistici și informații (de exemplu, în *Croația* sau *Finlanda*, printre altele).

În mai multe țări sunt raportate planuri de extindere a utilizării soluțiilor digitale, și anume, în *Danemarca*, unde se preconizează să fie implementat, în 2020, un Sistem de management electoral; în *Franța*, unde se are în vedere colectarea de semnături electronice pentru referendumuri; în *Finlanda*, unde este planificată introducerea unui Sistem de Informații Electorale (SIE); în *Irlanda*, unde modernizarea registrului electoral este în curs de desfășurare și se examinează lansarea națională a înregistrării online; în *Letonia*, unde se intenționează introducerea unei liste electronice a alegătorilor pentru secțiile de votare la următoarele alegeri municipale și parlamentare, pentru a oferi posibilitatea de a vota la oricare dintre acestea, în ziua alegerilor. În aceste cazuri sunt necesare modificări juridice.

Conformitatea soluțiilor de vot electronic cu principiile naționale pentru alegeri democratice (normele naționale includ standardele internaționale ale articolului 25 PIDCP și articolului 3 din Protocolul nr. 1 la Convenția Europeană a Drepturilor Omului) a fost examinată de instanțele supreme din *Germania*, *Austria*, *Estonia*, *Elveția* și *Franța*, printre altele.31 Preocupările cu privire la ingerința străină în alegeri au condus, mai recent, la o examinare mai atentă a securității (și, prin urmare, a conformității) soluțiilor digitale, altele decât votul electronic, utilizate în procesele electorale, și anume registrele de alegători și sistemele de înregistrare sau transmitere și calcul al rezultatelor, astfel cum a fost cazul în *Germania* și *Olanda* în 2017.

29. Orice neconcordanță între cifre este semnalată de aplicație; ca măsură de precauție, programul software poate fi conceput astfel încât să nu permită transmiterea imediată a datelor în cazurile în care cifrele nu sunt în concordanță, așa cum este cazul în România.

30. La trei zile de la alegeri, se efectuează o verificare finală a voturilor pe hârtie transmise de fiecare secție de votare, în care Comisiile Electorale sunt asistate de o aplicație informatică care le facilitează activitatea.

31. Pentru o viziune comparativă internațională, a se vedea Driza Maurer, Barrat (ed.), Jurisprudența votului electronic – o analiză comparativă, Routledge 2015, 2017. Pe lângă țările europene menționate, se discută, de asemenea, și jurisprudența din India, Brazilia, Mexic, SUA, Australia, Argentina și Venezuela.

La digitizarea proceselor, o întrebare inițială care apare este cum trebuie să arate procesul digitizat: trebuie să imite procesul tradițional, pe hârtie sau poate introduce noi caracteristici perturbatoare necesare conformității și care sunt posibile prin noua tehnologie? Până acum, a predominat imitarea. De exemplu, din perspectiva sufragiului egalității votului, un canal de vot electronic nu are voie să ofere alegătorilor mai multe posibilități sau posibilități diferite decât un canal tradițional (a se vedea standardul 5 din Recomandarea CM/Rec(2). Cu toate acestea, o altă logică, centrată pe atingerea obiectivelor, spre deosebire de realizarea egalității formale între soluții bazate pe tehnologii diferite a fost utilizată și pare mai adecvată. Aceasta se concentrează pe principii care trebuie respectate/aplicate și ia în considerare particularitățile tehnologiei utilizate. De exemplu, vulnerabilitățile și amenințările specifice legate de votul electronic recomandă introducerea verificabilității individuale și a verificabilității universale pentru a asigura respectarea principiului sufragiului liber (a se vedea standardele 15 ff din Recomandarea CM/Rec(2017)5). Acum, verificabilitatea individuală în votul electronic permite alegătorului să își verifice propriul vot, care este o caracteristică complet nouă ce nu există în cazul votului pe hârtie. De asemenea, votul multiplu este permis special pentru alegătorii pe internet (în unele țări), pentru a contracara riscul votului în familie, care este prezent în toate votările la distanță, inclusiv în cea pe internet. Un alt exemplu este proiectarea specifică a unui sistem de vot electronic pentru a permite, în măsura în care este posibil, persoanelor cu dizabilități și nevoi speciale să voteze în mod independent. Un altul este cerința ca un sistem de vot electronic să informeze alegătorul dacă acesta transmite un vot nevalabil (standardul 14 din Recomandarea CM/Rec(2017)5). Din nou, acest lucru nu este posibil în cazul votului pe hârtie: în acest caz, votul electronic oferă un avantaj care ajută la o mai bună asigurare a dreptului la sufragiu liber.

În concluzie, digitizarea documentelor și proceselor joacă un rol semnificativ în susținerea alegerilor în multe țări ale Consiliului Europei, permițând prelucrarea accelerată și uniformă a datelor. Fiecare fază a ciclului electoral este susținută de instrumente digitale. Introducerea și extinderea acestora sunt continue și pot pune bazele pentru introducerea ulterioară a altor tehnologii noi.

Biometrie

Biometria introduce posibilitatea de a surprinde și salva în format electronic unele caracteristici fizice (iris, amprentă, recunoaștere facială etc.) care trebuie să permită identificarea unică a unei persoane. În mod tradițional, identificarea unică este asigurată de reguli procedurale și se bazează pe registrele alegătorilor. Prin mărirea listelor electorale cu date biometrice, scopul este de a asigura identificarea unică a alegătorilor și de a preveni votul multiplu. În ziua alegerilor, caracteristicile biometrice ale alegătorilor sunt capturate și comparate cu informațiile biometrice stocate în bazele de date. Biometria în alegeri a fost utilizată în principal în țările din America de Sud sau Africa. Cu foarte puține excepții, statele membre ale Consiliului Europei nu iau în considerare biometria în alegeri. Protecția datelor, secretul votului, precum și privarea de drepturi a alegătorilor din cauza erorilor de identificare biometrică (acceptare falsă și respingere falsă) sunt printre principalele motive pentru care nu a fost utilizată biometria în alegerile din Europa până în prezent. Un raport din 2018 al Senatului francez sugerează luarea în considerare a identificării unice a alegătorilor prin introducerea biometriei.

Utilizarea biometriei în alegeri ridică probleme de conformitate cu articolul 3 din Protocolul Nr. 1 la Convenția Europeană a Drepturilor Omului. Cât de unice și de permanente sunt caracteristicile biometrice pentru a asigura dreptul de vot în timp? Este ușoară și rapidă colectarea de informații biometrice și autentificarea alegătorului în timpul votului? Sunt culegerea și utilizarea unor astfel de caracteristici acceptate de alegători? Trebuie asigurate stocarea securizată a datelor (protecția secretului datelor) și securitatea sistemului.

Blockchain

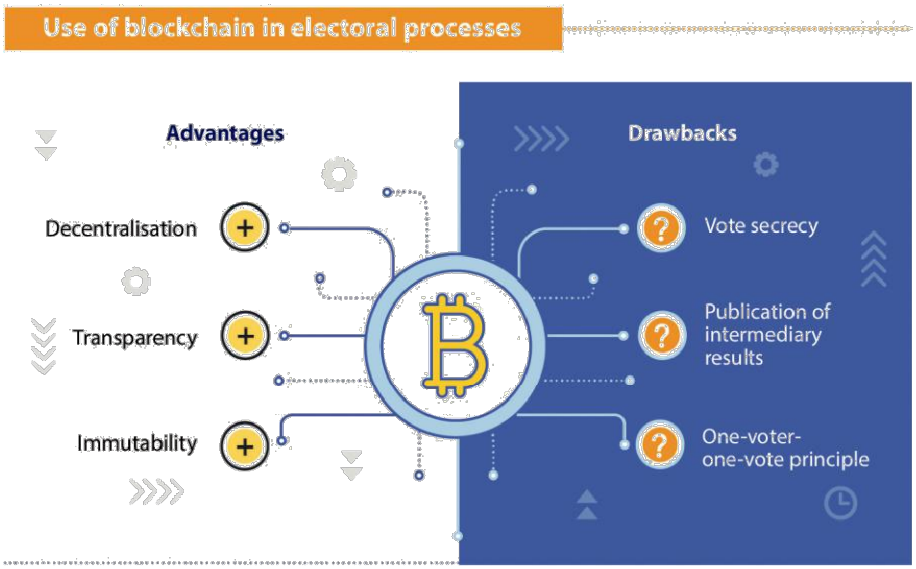
Blockchain-ul este o serie de date imuabile cu marcaj de timp, care este distribuit și gestionat de un grup de calculatoare. Principalele sale caracteristici sunt descentralizarea, transparența și imuabilitatea.32 Tranzacțiile înregistrate pe mai multe calculatoare asigură că nicio înregistrare nu poate fi modificată retroactiv, fără modificarea tuturor blocurilor ulterioare.

Câteva încercări cu votul blockchain au avut loc la nivel local.33 Votul blockchain pretinde multe avantaje față de sistemele de vot tradiționale, centralizate, pe hârtie. Cu toate acestea, majoritatea proprietăților sale (de exemplu, identificarea electronică, semnăturile digitale pentru a garanta integritatea datelor, criptografie puternică, verificabilitatea alegătorilor și posibilitățile multiple de vot) nu sunt exclusive blockchain-ului și sunt, de asemenea, prezente în votul electronic „tradițional" verificabil. Votul prin blockchain introduce cel puțin o caracteristică specifică: orice informație procesată, prin calcul sau stocare de date, este partajată între mai multe noduri (descentralizare). Într-un sistem de vot descentralizat, un set de entități trebuie să convină asupra modului în care a fost exprimat un vot înainte de a-l înregistra. Aceasta înseamnă că nu există o singură entitate care preia controlul: nu este doar organizatorul scrutinului, OE, care validează un vot, ar putea fi, de asemenea, și diverse instituții acreditate (de exemplu, Consiliul Europei, partidele politice sau consiliile locale). Acest lucru oferă avantajul protecției împotriva amenințărilor interne: se presupune că nici măcar un guvern corupt nu poate falsifica voturile. Odată ce un vot a fost înregistrat, acesta nu poate fi eliminat sau modificat, deoarece blockchain-ul pretinde a fi imuabil. Dacă există suficiente noduri (în grup), se susține că sistemul nu poate fi spart de hackeri. Identitățile alegătorilor sunt anonimizate, iar voturile ar fi secrete. Acest lucru este discutabil, deoarece identitatea unei persoane poate fi urmărită utilizând informații privind adresa publică și IP-urile. Alte probleme se referă la interoperabilitate, costuri etc.

Blockchain-ul este din ce în ce mai utilizat pentru procesele în care sunt necesare înregistrări sau tranzacții, contracte și documente oficiale inalterabile, persistente și cu opțiune de căutare. Administrațiile îl utilizează pentru cărțile funciare oficiale sau tranzacțiile oficiale etc. Se poate imagina că administrațiile care îmbrățișează blockchain-ul pot fi tentate să îl utilizeze, de asemenea, și în ciclul electoral; de exemplu, pentru a ține registre ale alegătorilor, partidelor etc. Așadar, dacă Registrul Civil se bazează pe blockchain, atunci registrul electoral extras va fi probabil păstrat în același mod. Introducerea blockchain-ului pentru a gestiona un element al ciclului electoral poate afecta întregul ciclu.

32. Sursa Wikipedia, https://en.wikipedia.org/wiki/Blockchain

33. De exemplu, orașul Zug din Elveția a desfășurat o simulare de vot blockchain prin internet, în perioada 25 iunie-1 iulie 2018. A se vedea evaluarea http://www.stadtzug.ch/dl.php/de/5c00ff8dbd830/eVoting_Final_Report_ENG.pdf



Blockchain ridică mai multe probleme de conformitate cu articolul 3 din Protocolul Nr. 1 la Convenția Europeană a Drepturilor Omului, printre altele cu privire la secretul votului (deoarece datele publicate pe blockchain rămân acolo), la nepublicarea rezultatelor intermediare (deoarece numărul de voturi pentru fiecare candidat sunt cunoscute înainte de încheierea votării); la securitate; ușurință în utilizare (deoarece este necesară o perioadă de așteptare substanțială până la încheierea unei tranzacții sau a unui vot); respectarea principiului un alegător-un vot (deoarece puterea de calcul este importantă pentru luarea deciziilor în blockchain), etc.

Cloud computing *(informatica dematerializată)*

Cloud computing este disponibilitatea la cerere a resurselor sistemului informatic, în special stocarea datelor și puterea de calcul, fără gestionarea activă directă de către utilizator. Termenul este utilizat, în general, pentru a descrie centrele de date disponibile pentru mulți utilizatori prin Internet.34 Există cloud-uri publice și private.

Organizațiile, precum afacerile, sunt înclinate sau și-au transferat deja IT-ul în cloud, deoarece se presupune că este mai ieftin și mai sigur decât menținerea capacităților interne. Acest lucru constituie o provocare atunci când vine vorba de sisteme critice, cum ar fi alegerile, în care autoritățile trebuie să dețină puterea și, de preferință - așa cum ar spune înțelepciunea convențională astăzi - expertiza și soluțiile IT interne.

Cloud-ul poate introduce noi vulnerabilități în sistemul electoral; de exemplu, securitatea documentelor și proceselor sensibile, secretul și confidențialitatea, răspunderea sau interoperabilitatea (și anume, posibilitatea de a prelua datele sau de a le transfera într-un alt cloud) și multe amenințări de atacuri, în timp ce investigarea

34. Wikipedia, https://en.wikipedia.org/wiki/Cloud_computing

neregulilor și criminalistica devine mai complexă. Utilizarea informaticii dematerializate pentru documentele și procesele ciclului electoral nu a fost prea tematizată. Utilizarea sa efectivă și întrebările de conformitate care decurg din aceasta (secret, securitate, interoperabilitate etc.) necesită investigații suplimentare.

Inteligență artificială

Inteligența artificială (IA) se referă la o gamă largă de metode, atât actuale, cât și speculative.35 Aceasta se referă la sistemele care manifestă un comportament inteligent analizându-le mediul și luând măsuri – cu un anumit grad de autonomie – pentru a atinge obiective specifice.36 Domeniul IA recurge la multe domenii. Obiectivele tradiționale ale cercetării IA includ raționamentul și luarea deciziilor (reprezentarea cunoștințelor, planificarea, programarea, căutarea, optimizarea), învățarea (învățare automată, rețele neuronale, învățare profundă, arbori de decizie etc.) și robotica (IA încorporată; capacitatea de a mișca și interacționa cu lumea fizică). Până acum, soluțiile IA sunt specifice domeniului.

IA poate avea impact asupra noilor soluții tehnologice utilizate în alegeri. De exemplu, aceasta poate fi utilizată pentru a conduce atacuri cibernetice într-un mod care este chiar mai sofisticat și mai dificil de prezis decât acum „inclusiv mai capabil să urmărească obiective foarte personalizate și să se adapteze în timp real”.37 Acest lucru trebuie luat în serios de către OE-uri. În același timp, este de așteptat ca IA să fie antrenată și utilizată pentru apărarea cibernetică. IA poate fi avută în vedere, de asemenea, și în formare și educație sau în probleme de soluționare a litigiilor. Aceasta poate fi interesantă în scopuri de recuperare a informațiilor.

Principalele probleme privind IA includ problemele privind datele și explicabilitatea. Sistemele IA trebuie să prelucreze o mulțime de date pentru a funcționa bine și sunt la fel de bune pe cât sunt datele care le sunt furnizate. Dacă datele de antrenament sunt părtinitoare (de exemplu, nu sunt suficient de incluzive), la fel va fi și IA antrenată pe acestea și, în consecință, deciziile sale vor fi inechitabile. Există totuși un avertisment important: principiul datelor deschise nu se aplică tuturor tipurilor de date colectate în alegeri, ceea ce face mai dificilă dezvoltarea soluțiilor IA pentru alegeri. Într-adevăr, contrariul este adevărat, deoarece, de exemplu, informațiile detaliate privind participarea și conținutul votului sunt acoperite de cerința sufragiului secret. Explicabilitatea se referă la natura opacă a unor IA: este imposibil, chiar și pentru inginerii lor, să înțeleagă cum iau acestea decizii. Există un consens din ce în ce mai mare la nivel național și internațional că sistemele IA trebuie proiectate astfel încât deciziile acestora să poată fi explicate, iar oamenii să fie răspunzători.38

35. Serviciul de Cercetare al Parlamentului European (2019) „Cum funcționează inteligența artificială”, „De ce contează inteligența artificială”. A se vedea și Wikipedia, https://en.wikipedia.org/wiki/Artificial_intelligence

36. Comisia Europeană, indep. Grupul de experți la nivel înalt privind inteligența artificială, „O definiție a IA: Principalele capacități și discipline”, 8 aprilie 2019

37. Raportul panelului ONU la nivel înalt, *Era interdependenței digitale*, iunie 2019

38. Recomandarea 3C a Raportului panelului ONU la nivel înalt, *Era interdependenței digitale,* iunie 2019; *Legea de responsabilitate algoritmică din SUA din 2019*; *Strategie Künstliche Intelligenz der Bundesregierung* a Guvernului german, noiembrie 2018; Cedric Villani (Franța) Raport *Pentru o inteligență artificială relevantă. Spre o strategie franceză și europeană,* din martie 2018

b. Perspectiva ciclului electoral

I. Cadrul juridic

Această parte a ciclului electoral include proiectarea și elaborarea întregii legislații și a reglementărilor privind alegerile la toate nivelurile guvernamentale și de toate tipurile, inclusiv dreptul formal și material și chiar codurile de conduită și alte instrumente, care pot avea un impact direct sau indirect asupra alegerilor. Nu toate aceste elemente sunt inițiate sau elaborate de OE, de aceea este, de asemenea, important ca OE să aibă o bună imagine de ansamblu și înțelegere a tuturor elementelor de reglementare care trebuie luate în considerare în ciclul electoral. Acesta este momentul în care noile tehnologii pot ajuta, de exemplu, la pregătirea, organizarea și recuperarea informațiilor.

Un alt aspect al acestei probleme este că legislația trebuie să reglementeze utilizarea noilor tehnologii în ciclul electoral. Până acum, s-a dovedit dificilă redactarea de reglementări care să respecte principiile de nivel superior, astfel cum se arată în deciziile curților constituționale din Germania și Austria privind conformitatea reglementărilor referitoare la votul electronic. Nu este clar cum se aplică principiile juridice noilor tehnologii și care trebuie să fie conținutul unei reglementări conforme. Principii precum legalitatea sau certitudinea juridică a legii electorale sunt contestate de complexitatea noilor tehnologii și de evoluția rapidă a acestora.

Una dintre dificultăți se referă la concepte al căror conținut și domeniu de aplicare pot fi diferite în lumea digitală față de cea analogică. Într-o lume analogică, securitatea și controalele electorale, de exemplu, sunt considerate într-un mod destul de static, ca produse și procese bine definite, în timp ce într-un context digital, acestea trebuie să avanseze zilnic pentru a răspunde la vulnerabilități și amenințări în evoluție și pentru a face față noilor riscuri. Unii compară acest lucru cu o cursă a înarmărilor. Acest aspect trebuie reflectat în reglementare, dar cum? De exemplu, în lumea analogică, OE-urile sunt responsabile pentru securitate, cu excepția cazurilor excepționale, cum ar fi *forța majoră*. Cum le definim responsabilitatea într-un context digital? Este ușoară acceptarea *forței majore* în contexte low tech. Este pericolul din programul software (cu referire la IA) acceptabil? Pe măsură ce noile tehnologii evoluează prin încercare și eroare, ce trebuie să asigure un OE, și anume, ce obligații pozitive decurg din sarcina sa de a asigura conformitatea cu articolul 3 din Protocolul Nr. 1 la Convenție pe tot parcursul ciclului electoral?

Răspunsurile sunt departe de a fi banale. Curțile constituționale (de exemplu, din Germania și Austria), parlamentul, guvernul și organizațiile de supraveghere (de exemplu, din Olanda, Norvegia sau Franța) au recunoscut deficiențele reglementărilor existente, de exemplu, pentru votul electronic. Moștenite din anii ’70, ’80 și ’90, astfel de reglementări trebuie să evolueze pentru a ține cont de cele mai noi tehnologii. În câteva cazuri (Belgia, Estonia, Elveția), autoritatea de reglementare le-a actualizat sau a introdus altele noi. Conformitatea acestora este testată în practică și se pare că astfel de reglementări trebuie să continue să evolueze (un exemplu este exercițiul de transparență al votului prin internet din Elveția din 2019 și lecțiile învățate despre verificabilitate, transparență și certificare).39

39. Driza Maurer, Ardita (2019), *Exercițiul de transparență Swiss Post/Scytl și posibilul impact al acestuia asupra reglementării votului pe internet*, în R. Krimmer și colab. (Ed.) : E-Vote-ID 2019, LNCS 11759, pp. 83-99, 2019

Îndrumările din Recomandarea CM/Rec(2017)5 a Consiliului Europei au fost importante pentru țări în eforturile lor de reglementare pentru votul electronic. Cel mai recent val de întrebări nu a fost încă discutat temeinic, inclusiv următoarele: controlul mecanismelor de verificare a votului, evaluarea ipotezelor de încredere care sunt, în mod necesar, prezente în votul electronic verificabil, urmărirea transparenței (de exemplu, ceea ce se întâmplă după publicarea codului sursă), etc.

Dintre toate noile tehnologii utilizate în ciclul electoral, votul electronic pare să fi beneficiat de cea mai mare atenție, din perspectiva reglementării. Alte soluții digitale utilizate în ciclul electoral sunt reglementate, în cel mai bun caz, doar din perspectiva gestionării IT. Încercările OE-urilor de a introduce/actualiza astfel de reglementări se întâlnesc adesea cu rezistență.40 Cu toate acestea, lucrurile se schimbă, în special după tematizarea interferenței țărilor străine după alegerile prezidențiale din SUA din 2016 și presupusa piratare a unor soluții susținute de electronice. Exemplele recente de la alegerile din 2017 din Olanda (software de numărare și tabulare) și Germania (software de transmitere a rezultatelor) arată că procesele vitale pentru rezultatul alegerilor se confruntă cu provocări similare cu cele ale votului electronic și trebuie să fie mai bine reglementate. Conformitatea acestora cu articolul 3 din Protocolul nr. 1 la Convenție și cu principiile electorale naționale trebuie să fie mai bine investigată.

Conformitatea cu articolul 3 din Protocolul Nr. 1 la Convenție impune ca soluțiile digitale să implementeze/să respecte anumite condiții: introducerea treptată a noilor tehnologii, răspundere (certificare, audituri), repartizarea responsabilităților, transparență și observare, credibilitate și securitate și interoperabilitate, printre altele. Răspunsurile la chestionarul CEDG arată că țările salută îndrumările Consiliului Europei. De exemplu, Recomandarea CM/Rec(2017)5 privind votul electronic este considerată importantă de către țări, inclusiv cele care permit exprimarea electronică a votului (Belgia, Estonia și Elveția) și cele care practică doar numărarea electronică pură (Republica Cehă), Danemarca sau Ungaria). Răspunsurile țărilor sugerează că sunt necesare discuții ulterioare la nivel regional pe probleme de securitate cibernetică în alegeri, verificarea votului, identitate digitală, proceduri de urgență în caz de întrerupere a comunicațiilor și că aceste aspecte trebuie să beneficieze de mai multă atenție la nivel de reglementare.

II. Planificare si pregătire

OE supraveghează etapele detaliate ale ciclului electoral: calendarul electoral, recrutarea și formarea personalului, logistică și securitate, politicile electorale naționale sau regionale, serviciile electorale, achizițiile pentru servicii externalizate, recrutarea și formarea personalului electoral etc. Suportul IT adaptat la necesităților acestuia este utilizat în acest scop.

Principala problemă aici este măsura în care aceste soluții nu pot fi sparte de hackeri (securitate), măsura în care procesele ciclului electoral sunt dependente de acestea și dacă sunt prevăzute sau nu soluții de rezervă.

40. Un exemplu este discuția referitoare la reglementarea federală a soluțiilor de numărare electronică în Elveția și reticența inițială, și anume, a cantoanelor, care se ocupă de introducerea, operarea și monitorizarea acestor soluții.

III. Formare și educație

OE desfășoară, de obicei, informarea și educarea alegătorilor și civică. Acesta sprijină accesul pentru toți, promovează politici și practici de egalitate și echitate și poate oferi facilități de cercetare electorală. Pe lângă alegători, acesta angajează și formează personal electoral temporar. OE asigură acreditarea observatorilor și reglementează conduita acestora. Acesta pregătește observatorii de votare ai partidelor politice și ai candidaților. Activitățile OE se extind la mass-media: acesta oferă acces mass-media, reglementează conduita mass-media în timpul alegerilor și reglementează sondajele de opinie.

IT este utilizat pentru a susține astfel de activități. Aceleași probleme identificate în cadrul planificării și pregătirii se aplică și aici.

IV. Înregistrare

După cum s-a menționat la digitizare, există, în principal, două tipuri de registre: listele electorale sau ale alegătorilor și registrele partidelor. În timpul votului se înregistrează, de asemenea, și utilizarea drepturilor de vot (faptul că o persoană a votat). Toate sunt, probabil, digitalizate în toate țările Consiliului Europei.

Registrele alegătorilor includ alegătorii care locuiesc în țară, alegătorii care locuiesc în străinătate care au dreptul de a vota și, în unele cazuri, străinii stabiliți în țară. OE înregistrează, de asemenea, și forțe politice (partide, mișcări etc.). Înainte de fiecare alegere, acesta primește și validează nominalizările candidaților. În plus, acesta poate supraveghea preselecțiile sau primarele partidelor politice.

În ceea ce privește respectarea articolului 3 din Protocolul Nr. 1 la Convenție, o problemă cu care se confruntă toate registrele este identificarea unică a persoanelor, și anume, a alegătorilor și candidaților. Identificarea unică are scopul de a asigura sufragiul egal (o persoană, un vot), precum și respectarea regulilor electorale privind candidatura. În sistemele analogice pe hârtie, persoanele sunt identificate manual: procedura este greoaie și predispusă erorilor în verificare. Într-o lume digitală, soluțiile susținute electronic oferă avantajul verificării rapide și al prevenirii efective a voturilor multiple sau a candidaturilor multiple. O soluție luată în considerare este identificarea electronică unică. Estonia utilizează ID-urile electronice pentru autentificarea alegătorilor. În unele țări fără ID-uri electronice, s-a încercat utilizarea de identificatori unici alternativi, cum ar fi numerele de securitate socială, de exemplu, pentru identificarea candidaților. Inițial, organele de supraveghere a protecției datelor s-au opus cu înverșunare. Preocupările privind protecția datelor au prevalat asupra respectării principiilor electorale (reguli de candidatură sau o persoană, un vot). Mai recent, agenții de protecție a datelor au început să accepte o astfel de utilizare. În paralel, ID-urile electronice devin din ce în ce mai frecvente. Se presupune că acestea facilitează tranzacțiile în toate domeniile vieții. Votul și secretul participării rămân importante și trebuie luate în considerare cu atenție, deoarece utilizarea ID-urilor electronice și a altor instrumente de e-identificare devine obișnuită.

V. Campanie electorală

Utilizarea noilor tehnologii în campania electorală se referă, în principal, la formarea opiniei. După cum s-a menționat anterior, utilizarea noilor tehnologii pentru probleme de formare a opiniei este în afara domeniului de aplicare al acestei lucrări.

VI. Operațiuni de vot

Această fază se referă la procesul electoral, de la deschiderea până la închiderea votului și numărarea, verificarea și publicarea rezultatelor ulterioare. Pe parcursul acestei faze pot fi utilizate mai multe soluții digitale, inclusiv identificarea electronică a alegătorilor, votul electronic, numărarea electronică, transmiterea electronică a rezultatelor. Problemele de conformitate au fost discutate mai sus, în perspectiva tehnologiei/digitizării.

VII. Rezultatele alegerilor

Pe lângă colectarea, tabelarea și publicarea rezultatelor (a se vedea mai sus), OE-urile utilizează, de asemenea, și soluții digitale pentru a efectua audituri și verificări ale corectitudinii rezultatelor. Există instrumente care verifică plauzibilitatea rezultatelor, adică identifică neregulile electorale prin metode statistice.41 Metodele statistice evaluează probabilitățile de corectitudine a rezultatelor pe baza datelor de la alegerile anterioare. Acestea trebuie „alimentate” cu date de la alegerile curente și anterioare. În ceea ce privește IA, calitatea și cantitatea acestor date sunt cruciale pentru ca aceste metode să funcționeze optim.

OE-urile pot acționa, de asemenea, și ca o autoritate de soluționare a litigiilor. Soluțiile digitale pot fi utilizate pentru a prelua și procesa informații. Aici nu se vorbește despre justiție predictivă; totuși, astfel de instrumente pot fi interesante și pot ajuta OE-urile să ia decizii corecte și rapide. Ele pot fi utilizate, de asemenea, pentru a ajuta alegătorii să își înțeleagă mai bine drepturile și cum să le apere, îmbunătățind astfel accesul la justiție pentru utilizatorii reclamanți (alegători, partide etc.). În toate aceste cazuri, trebuie să se acorde atenție conformității soluției, în mod specific, cu sufragiul liber și secret și cu dreptul la un sistem efectiv de apel.

VIII. Atribuții postelectorale

Astfel de atribuții includ ștergerea sau arhivarea datelor referitoare la alegeri, munca de actualizare a informațiilor și instrumentelor, revizuirea și evaluarea adecvării cadrului electoral și performanța proprie a OE, precum și consilierea guvernului și a legislativului în probleme de reformă electorală. Aceleași observații pentru planificare și pregătire se aplică instrumentelor digitale utilizate aici. În plus, secretul privind votul și participarea trebuie respectat.

41. Comisia Europeană pentru Democrație prin Drept (Comisia de la Veneția), 2018, „Raport privind identificarea neregulilor electorale prin metode statistice”, CDL-AD(2018)009

3. PROBLEME DE SINTEZĂ ȘI TRANSVERSAL

Această prezentare rapidă arată că cea mai răspândită și necesară tehnologie este digitizarea. Aceasta este fundamentul oricărei alte tehnologii noi, cum ar fi biometria, blockchain-ul, informatica dematerializată sau inteligența artificială.

Este important ca soluțiile digitale utilizate în ciclul electoral să respecte principiile și condițiile pentru alegeri democratice. Întrebarea a fost tratată într-o oarecare profunzime în ceea ce privește votul electronic. Conformitatea soluțiilor digitale utilizate în ciclul electoral, altele decât votul electronic, a trecut până acum neobservată. Evoluțiile recente arată că utilizarea unor astfel de soluții trebuie planificată și reglementată cu atenție. Cerințele pentru documentele și procesele sensibile pot fi aliniate la cerințele Recomandării CM/Rec(2017)5 pentru votul electronic.

Unele întrebări sunt transversale: acestea sunt de interes pentru toate tehnologiile digitale și pentru toate fazele ciclului electoral. Astfel de întrebări includ securitatea cibernetică, protecția datelor, procedurile de urgență sau cooperarea public-privată. Instrumentele existente ale Consiliului Europei se ocupă deja de acestea. Cu toate acestea, alegerile rămân un caz aparte, căruia i se pot aplica cerințe mai stricte, cum ar fi protecția datelor sau securitatea cibernetică. Răspunsurile țărilor la chestionarul CEDG sugerează că este necesară munca la nivel regional, în special în ceea ce privește securitatea cibernetică, verificarea votului, identitatea digitală și procedurile de urgență în cazul întreruperii comunicațiilor.

Protecția datelor este o problemă atât de transversală. Aceasta este reglementată de Convenția modernizată a Consiliului Europei pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal (Convenția 108+). La nivelul UE, principalul instrument juridic este Regulamentul general privind protecția datelor (RGPD) al (UE) 2016/679. Convenția Consiliului Europei 108+ și RGPD au fost elaborate în paralel și sunt consecvente una cu cealaltă. RGPD amplifică unele principii ale Convenției 108+. Datele utilizate în alegeri sau privind opinia politică sunt date calificate, a căror prelucrare trebuie permisă numai dacă sunt consacrate prin lege garanții adecvate (articolul 6 din Convenția 108+). Cu toate acestea, pentru cei responsabili de alegeri, nu este clar cum trebuie să arate garanțiile adecvate. Trebuie avută în vedere interacțiunea dintre diferitele instrumente și specificul alegerilor. Este necesară o expertiză combinată; de exemplu, utilizarea criptografiei poate fi o măsură importantă pentru a proteja unele dintre aceste date.

O altă problemă transversală este securitatea cibernetică. Convenția de la Budapesta privind criminalitatea informatică reglementează un aspect important al securității cibernetice, care este cooperarea între țări pentru urmărirea penală a infracțiunilor împotriva alegerilor libere, corecte și curate. Alte aspecte sunt reglementate la nivel național, de exemplu, prin reglementări privind securitatea cibernetică a infrastructurilor critice. Alegerile sunt clasificate drept infrastructură critică. Securitatea acestora este deosebit de importantă. La fel și planificarea de a face față atacurilor (corupție de date, întreruperea serviciului etc.). Exemple de

administrații a căror activitate a fost compromisă, de exemplu, de ransomware (Baltimore, mai 2018) arată ce ar putea merge prost în alegeri și cum procesele critice ar putea deveni ținta hackerilor motivați politic sau financiar etc.

Cooperarea public-privată este încă o altă problemă transversală importantă, deoarece soluțiile digitale și controlul acestora sunt asigurate, în principal, de sectorul privat. Condițiile de achiziție trebuie să reflecte cerințele care sunt importante pentru conformitatea soluției cu articolul 3 din Protocolul nr. 1 la Convenția Europeană a Drepturilor Omului. Este importantă clarificarea responsabilităților. Responsabilitatea politică pentru utilizarea soluțiilor digitale în alegeri trebuie să revină OE. Încă de la începutul cooperării dintre OE și furnizorii privați trebuie să fie clar cum vor fi abordate întrebările de neconformitate.

4. REFERINȚE SELECTATE

- Consiliul Europei, Comitetul de experți (MSI-AUT), *Proiectul de recomandare al Comitetul de Miniștri către statele membre privind impactul sistemelor algoritmice asupra drepturilor omului,* 26 iunie 2019.

- Consiliul Europei, *Convenția 108+, Convenția pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal* (iunie 2018).

- Consiliul Europei, Comitetul Consultativ al Convenției pentru Protecția Persoanelor cu privire la prelucrarea datelor cu caracter personal, *Raport privind Inteligența Artificială. Inteligența artificială și protecția datelor: provocări și posibile remedii,* din 25 ianuarie 2019.

- Consiliul Europei, Comitetul Convenției privind criminalitatea informatică (T-CY), *Nota orientativă Nr. 9, Aspecte ale ingerinței electorale prin intermediul sistemelor informatice acoperite de Convenția de la Budapesta, 08.07.2019.*

- Consiliul Europei, *Declarația Comitetului de Miniștri privind capacitățile manipulative ale proceselor algoritmice*, 13 februarie 2019.

- Consiliul Europei, *Recomandarea Comitetului de Miniștri către statele membre privind standardele pentru votul electronic, CM/Rec(2017)5.*

- Comisia Europeană, *Alegeri libere și corecte. Document de orientare. Ghiduri ale Comisiei privind aplicarea legislației Uniunii în domeniul protecției datelor în context electoral.* O contribuție a Comisiei Europene la reuniunea liderilor de la Salzburg din 19-20 septembrie 2018.

- Comisia Europeană, Grupul de experți la nivel înalt privind inteligența artificială, *O definiție a IA: principalele capacități și discipline*, 8 aprilie 2019.

- Comisia Europeană pentru Democrație prin Drept (Comisia de la Veneția) *și colab., Raport comun privind tehnologiile digitale și alegerile 21-22 iunie 2019.*

- IDEA, *Securitatea cibernetică în alegeri. Modele de colaborare interagenții*, 2019.

- IDEA, *Proiect de management electoral, Ediție revizuită, 2014.*

- OSCE/OIDDO, *Manual pentru observarea noilor tehnologii de vot, 2013.*

- Comisia la nivel înalt a Secretarului General al ONU, *Era interdependenței digitale, iunie* 2019

Soluțiile digitale sunt tot mai mult utilizate în alegeri. Securitatea acestora a atras multă atenție în ultimii ani, deoarece are impact asupra integrității alegerilor. Legiuitorul are sarcina importantă de a introduce reglementări care să asigure că numai soluțiile digitale care respectă principiile constituționale pot fi utilizate în alegeri. Aceasta nu este o sarcină ușoară, deoarece domeniul este încă experimental. Cele două studii prezentate aici ridică întrebări juridice, se bazează pe experiențele anterioare din mai multe țări și sugerează posibile abordări. Această publicație va fi de interes pentru legiuitori și autorități executive și anume Organele Electorale care sunt invitate să decidă cu privire la utilizarea soluțiilor digitale în alegeri.

www.coe.int

Consiliul Europei este principala organizație a drepturilor omului de pe continent. Acesta cuprinde 47 de state membre, inclusiv toți membrii Uniunii Europene. Toate statele membre ale Consiliului Europei au semnat Convenția Europeană a Drepturilor Omului, un tratat menit să protejeze drepturile omului, democrația și statul de drept. Curtea Europeană a Drepturilor Omului supraveghează punerea în aplicare a Convenției în statele membre.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE