Școala Națională de Studii Politice și Administrative
Facultatea de Administrație Publică

Securitatea informației în Administrația Publică. Studiu de caz.

- lucrare de licență, specializarea Administrație Publică -

Coordonator

Conf. Univ. Dr. Cătălin VRABIE

Absolvent

Ene Sergiu-Alexandru

București
2024

Instrucțiuni de redactare (A se citi cu atenție!!)

1. Introduceți titlul lucrării în zona aferentă acestuia – nu modificați mărimea sau tipul fontului;
2. Sub titlul lucrării alegeți dacă aceasta este de licență sau de disertație;
3. Introduceți specializarea sau masteratul absolvit în zona aferentă acestuia de pe prima pagină a lucrării;
4. Introduceți numele dvs. complet în zona aferentă acestuia (sub Absolvent (ă));
5. Introduceți anul în care este susținută lucrarea sub București;

NB: Asigurați-vă că ați șters parantezele pătrate din pagina de gardă și cuprins.

6. Trimiteți profesorului coordonator lucrarea doar în format **Microsoft Word** – alte formate nu vor fi procesate;
7. **Nu ștergeți declarațiaanti-plagiat și nici instrucțiunile** –acestea trebuie să rămână pe lucrare atât în forma tipărită cât și în cea electronică;
8. **Semnați declarația anti-plagiat;**
9. **Cuprinsul este orientativ** – numărul de capitole / subcapitole poate varia de la lucrare la lucrare. **Introducerea, Contextul, Concluziile / Discuțiile și Referințele bibliografice sunt însă obligatorii;**
10. **Este obligatorie folosirea template**-ului. Abaterea de la acesta va cauza întârzieri în depunerea la timp a lucrării.

NB. Lucrările vor fi publicate în extenso pe pagina oficială a hub-ului Smart-EDU, secțiunea Smart Cities and Regional Development: https://scrd.eu/index.php/spr/index.

ATENȚIE:Lucrarea trebuie să fie un produs intelectual propriu. Cazurile de plagiat vor fi analizate în conformitate cu legislația în vigoare.

Declarație anti-plagiat

1. Cunosc că plagiatul este o formă de furt intelectual și declar pe proprie răspundere că această lucrare este rezultatul propriului meu efort intelectual și creativ și că am citat corect și complet toate informațiile preluate din alte surse bibliografice (de ex: cărți, articole, clipuri audio-video, secțiuni de text și sau imagini / grafice).

2. Declar că nu am permisși nu voi permitenimănui să preia secțiuni din prezenta lucrare pretinzând că este rezultatul propriei sale creații.

3. Sunt de acord cu publicarea on-line *in extenso* a acestei lucrări și verificarea conținutului său în vederea prevenirii cazurilor de plagiat.

Numele și prenumele: Ene Sergiu-Alexandru

Data și semnătura: 09.12.2023

Cuprins

Abstract

Lucrarea de licență "Securitatea informațiilor în Administrația Publică" abordează în mod detaliat aspectele legate de securitatea datelor în cadrul administrației publice, cu o atenție deosebită acordată protecției informațiilor sensibile.Capitolul 3 prezintă un studiu de caz complex, concentrat asupra securității informațiilor într-un context specific, cu accent pe evaluarea și îmbunătățirea practicilor de securitate folosite în prezent.Studiul își propune să evalueze nivelul de securitate al informațiilor într-un mediu administrativ specific și să ofere soluții pentru optimizarea acestuia. Obiectivele includ identificarea amenințărilor potențiale, analiza riscurilor cibernetice și prezentarea de măsuri de protecție adecvate.Baza teoretică a lucrării se întemeiază pe cercetările anterioare în domeniul securității informațiilor în administrația publică și în cadrul proceselor administrative digitalizate. Literatura de specialitate și cercetările relevante constituie fundamentul abordării și contextualizării studiului.Metodele utilizate includ analiza detaliată a practicilor existente, evaluarea tehnologiilor implicate și identificarea potențialelor vulnerabilități. Studiul adoptă o abordare empirică pentru evidențierea riscurilor și pentru a propune soluții eficiente în domeniul securității informațiilor.Rezultatele obținute aduc în prim plan aspectele cheie ale securității informațiilor în administrația publică, oferind un cadru clar pentru înțelegerea amenințărilor și a vulnerabilităților. Măsurile propuse sunt prezentate în detaliu pentru a susține îmbunătățirea securității informațiilor și pentru a consolida încrederea în administrația publică.Studiul aduce implicații semnificative pentru administratorii și decidenții din administrația publică, subliniind necesitatea adoptării unor măsuri proactive pentru protejarea datelor cu caracter sensibil în mediul digital. Rezultatele pot contribui la dezvoltarea cunoștințelor în domeniul securității informațiilor și al administrației publice, având impact asupra practicii administrative și a cercetărilor viitoare.

Cuvinte cheie: Securitate cibernetică, Confidențialitate, Integritate, Tehnologii informaționale, Protecția datelor.

Introducere

În epoca tehnologiei avansate și a conectivității globale, în care informațiile circulă cu viteză și se extind rapid, securitatea informației devine un pilon fundamental pentru funcționarea eficientă a instituțiilor din administrația publică. Această lucrare de licență își propune să exploreze în profunzime complexitatea și provocările securității informaționale într-un mediu guvernamental în continua evoluție, acordând o atenție deosebită menținerii integrității, confidențialității și disponibilității datelor. Capitolul introductiv nu se rezumă doar la a stabili direcția cercetării, ci adaugă un strat suplimentar de înțelegere a contextului actual, subliniind esențialul unei abordări proactive pentru a anticipa și gestiona riscurile din ce în ce mai sofisticate.

Capitolul 1, având rolul de a stabili temelia conceptuală a lucrării, nu doar definește conceptul de securitate a informațiilor, ci oferă o explorare în detaliu a caracteristicilor cheie care definesc acest domeniu într-o perpetuă schimbare. Se adâncește în relația complexă dintre administrația publică și securitatea informațiilor, oferind o perspectivă asupra necesității unei strategii integrate și adaptabile pentru a răspunde eficient provocărilor contemporane. De asemenea, se explorează aspecte precum evoluția amenințărilor cibernetice și schimbările legislative care influențează peisajul securității informaționale în administrația publică.

În Capitolul 2, focalizarea se îndreaptă către aspecte practice legate de protejarea datelor cu caracter sensibil în procesele administrative. Se evidențiază importanța vitală a acestor date pentru funcționarea corespunzătoare a instituțiilor publice, iar impactul pozitiv al digitalizării asupra prelucrării și protejării informațiilor este abordat într-un limbaj accesibil. Detaliind mijloacele disponibile pentru protecția datelor în administrația publică digitalizată, lucrarea explorează, de asemenea, modul în care riscurile cibernetice pot afecta mediul digital, oferind perspective critice pentru dezvoltarea unor strategii robuste de securitate.

Capitolul 3 aduce în discuție un studiu de caz detaliat asupra securității informațiilor într-un sistem de vot electronic. Prin această analiză aprofundată, lucrarea își propune să demonstreze nu doar teoria și conceptele prezentate, ci și aplicabilitatea și eficacitatea acestora într-un context real și dinamic, cum este cel al alegerilor electronice. Se explorează aspecte precum arhitectura sistemului, vulnerabilitățile potențiale și soluțiile inovatoare de securitate care pot fi implementate. Acest capitol se axează pe un cadru specific, mai precis pe Autoritatea Electorală Permanentă (AEP), și aduce în discuție un studiu de caz detaliat care explorează aplicabilitatea conceptelor în contextul real al alegerilor electronice coordonate de AEP. Focalizându-se pe elemente cheie, cum ar fi arhitectura sistemului de vot electronic, potențialele

vulnerabilități și soluțiile inovatoare de securitate, studiul are ca obiectiv oferirea unei înțelegeri profunde a modului în care AEP gestionează securitatea informațiilor în desfășurarea alegerilor electronice. Acest demers nu se limitează doar la aspectele teoretice, ci propune și o abordare practică și aplicabilă.

Această lucrare de licență nu se oprește doar la prezentarea cunoștințelor teoretice, ci se angajează să ofere un cadru practic și accesibil pentru implementarea securității informațiilor în cadrul administrației publice. Prin abordarea detaliată a subiectelor și prin integrarea unui studiu de caz relevant, lucrarea propune nu doar soluții teoretice, ci și instrumente și strategii aplicabile în vederea consolidării și îmbunătățirii practicilor de securitate într-un mediu guvernamental tot mai digitalizat și interconectat. Astfel, această lucrare se dorește a fi un ghid util pentru cei interesați să înțeleagă, să implementeze și să îmbunătățească securitatea informațiilor în cadrul administrației publice.

Context

Procesul de digitalizare a administrației publice din România a înregistrat o accelerare semnificativă în ultimii doi ani. Această creștere în ritm este evidențiată în mod vizibil, fiind determinată atât de efectele directe ale crizei sanitare, care au impus migrarea interacțiunilor cu cetățenii în mediul online din cauza restricțiilor impuse de pandemia de COVID-19, cât și de eforturile constante de digitizare la nivelul administrației publice centrale și locale. [1]

De-a lungul anilor 1960, s-a conturat ideea votului electronic, inițial conceput pentru a reduce riscul de fraudare a proceselor electorale. Odată cu expansiunea accesului la Internet, obiectivul a evoluat și către sporirea participării cetățenilor cu drept de vot la alegeri, inclusiv a celor din Diaspora sau a celor care nu pot să ajungă la secții de votare. Cu toate acestea, implementarea unui sistem de vot online pare a fi o provocare peste limitele tehnologiei actuale. [2]

Scopul inițial, acela de numărare manuală a voturilor, un proces meticulos și vulnerabil, continuă să fie o opțiune ideală pentru procesul de digitalizare. În ciuda dorinței de a facilita exprimarea votului prin intermediul internetului, se pare că tehnologia curentă întâmpină dificultăți semnificative în ceea ce privește implementarea eficientă a unui astfel de sistem. Astfel, povestea votului electronic se întâlnește cu provocări tehnologice, iar procesul tradițional de numărare manuală a voturilor rămâne în continuare un candidat ideal pentru adaptarea la era digitală. [2]

Cu toate acestea, implementarea eficientă a votului electronic se confruntă cu provocări tehnologice complexe. În ciuda dorinței de a facilita participarea cetățenilor din Diaspora sau a celor care nu se pot deplasa la secții, este crucial să ne asigurăm că sistemele folosite sunt securizate, transparente și rezistente la manipulare.Povestea votului electronic reflectă nu doar aspirațiile către o democrație mai accesibilă, ci și provocările ce apar în procesul de implementare. Importanța acestui concept stă nu doar în evitarea fraudelor, ci și în adaptarea la o eră digitală în continuă expansiune, cu impact direct asupra modului în care cetățenii își exprimă voința. În acest context, explorarea soluțiilor viabile și durabile pentru votul electronic devine o necesitate pentru consolidarea democrației în era digitală.

Capitolul 1. Securitatea Informației în Administrația Publică

Societatea se angajează din ce în ce mai mult în utilizarea tehnologiei informației, cu schimbarea informației de la suportul tradițional, hârtia, la forma electronică. Deși utilizarea hârtiei pentru documentele oficiale, unde semnătura sau stampila sunt esențiale, rămâne încă valabilă, introducerea semnăturii electronice deschide calea către o digitalizare completă a documentelor, cel puțin în ceea ce privește funcționalitatea.Această nouă paradigmă, în care calculatorul devine un instrument indispensabil și un canal de comunicare prin tehnologii precum poșta electronică sau internetul, aduce cu sine anumite riscuri specifice. O gestionare adecvată a documentelor în format electronic necesită implementarea unor măsuri specifice pentru protejarea informațiilor împotriva pierderii, distrugerii sau divulgării neautorizate. Un aspect deosebit de sensibil este asigurarea securității informațiilor gestionate de sistemele informatice în acest nou context tehnologic.

După părerea mea, paragraful subliniază transformarea în evoluție a societății către utilizarea din ce în ce mai extinsă a tehnologiei informației și a mediului electronic pentru schimbul de informații. Deși digitalizarea documentelor și introducerea semnăturii electronice au deschis noi posibilități în ceea ce privește eficiența și funcționalitatea acestor documente, trebuie să conștientizăm că această tranziție către mediul electronic nu este fără riscuri.

Securitatea informației acoperă un domeniu mai larg, concentrându-se pe garantarea integrității, confidențialității și disponibilității informației. Progresul tehnologiei informației implică apariția unor noi riscuri pentru care organizațiile trebuie să implementeze noi măsuri de control. De exemplu, popularizarea unităților de înregistrare CD-uri sau a dispozitivelor de stocare portabile de mare capacitate generează riscuri de copiere neautorizată sau furt de date.Utilizarea rețelelor și conectarea la internet introduc, de asemenea, riscuri suplimentare, cum ar fi accesul neautorizat la date sau frauda. Dezvoltarea tehnologică a fost însoțită de soluții de securitate, cu producătorii de echipamente și aplicații incluzând metode tehnice de protecție din ce în ce mai avansate. Cu toate acestea, în timp ce în domeniul tehnologiilor informaționale schimbarea este rapidă, elementul uman rămâne la fel de important. Asigurarea securității informațiilor nu poate fi realizată exclusiv prin măsuri tehnice, ci reprezintă în principal o problemă umană.[8]

Paragraful anterior evidențiază importanța securității informațiilor în contextul tehnologiei informației. Într-adevăr, avansul tehnologic aduce cu sine noi riscuri și amenințări, iar organizațiile trebuie să acționeze proactiv pentru a implementa măsuri adecvate de control. Este evident că popularizarea dispozitivelor de stocare portabile și creșterea conectivității la internet au deschis noi oportunități pentru copierea neautorizată a datelor și pentru accesul neautorizat la informații sensibile.

Cele mai multe incidente de securitate sunt cauzate de o gestionare și organizare necorespunzătoare, mai degrabă decât de deficiențele mecanismelor de securitate. Este esențial ca organizațiile să conștientizeze riscurile asociate cu utilizarea tehnologiei și gestionarea informațiilor și să abordeze această problemă printr-o conștientizare a importanței securității informațiilor printre angajați, înțelegând tipurile de amenințări, riscurile și vulnerabilitățile specifice mediilor informatizate și aplicând practici de control.Organizația Internațională pentru Standardizare (ISO) și Comisia Internațională Electrotehnică (IEC) constituie un forum specializat pentru standardizare. Statele membre ale ISO și IEC participă la elaborarea standardelor internaționale prin intermediul comitetelor tehnice. Statele Unite ale Americii, prin Institutul Național de Standardizare, îndeplinește funcția de secretar, în timp ce alte 24 de țări sunt participante (cum ar fi Brazilia, Franța, Regatul Unit, Coreea, Cehia, Germania, Danemarca, Belgia, Portugalia, Japonia, Olanda, Irlanda, Norvegia, Africa de Sud, Australia, Canada, Finlanda, Suedia, Slovenia, Elveția, Noua Zeelandă și Italia), iar alte 40 de țări au statut de observator. [3]

Din punctul meu de vedere, paragraful subliniază importanța unei bune gestionări și organizări în asigurarea securității informațiilor. Majoritatea incidentelor de securitate sunt rezultatul unor erori umane și a unor probleme în gestionarea și organizarea informațiilor, mai degrabă decât a

deficiențelor în mecanismele tehnice de securitate. Prin urmare, este crucial ca organizațiile să fie conștiente de riscurile asociate utilizării tehnologiei și gestionării informațiilor și să abordeze această problemă prin educarea și sensibilizarea angajaților cu privire la importanța securității informațiilor.

Societatea se angajează din ce în ce mai mult în utilizarea tehnologiei informației, cu schimbarea informației de la suportul tradițional, hârtia, la forma electronică. Deși utilizarea hârtiei pentru documentele oficiale, unde semnătura sau stampila sunt esențiale, rămâne încă valabilă, introducerea semnăturii electronice deschide calea către o digitalizare completă a documentelor, cel puțin în ceea ce privește funcționalitatea.

Această nouă paradigmă, în care calculatorul devine un instrument indispensabil și un canal de comunicare prin tehnologii precum poșta electronică sau internetul, aduce cu sine anumite riscuri specifice. O gestionare adecvată a documentelor în format electronic necesită implementarea unor măsuri specifice pentru protejarea informațiilor împotriva pierderii, distrugerii sau divulgării neautorizate. Un aspect deosebit de sensibil este asigurarea securității informațiilor gestionate de sistemele informatice în acest nou context tehnologic[2].

Din punctul meu de vedere, paragraful subliniază că în era tehnologiei avansate, unde calculatoarele și tehnologiile precum poșta electronică și internetul sunt indispensabile, există riscuri specifice legate de securitatea informațiilor. Pentru a asigura o gestionare adecvată a documentelor în format electronic, este necesară implementarea unor măsuri specifice pentru a proteja informațiile împotriva pierderii, distrugerii sau divulgării neautorizate. În acest nou context tehnologic, securitatea informațiilor gestionate de sistemele informatice devine un aspect extrem de important și sensibil.

Securitatea informației acoperă un domeniu mai larg, concentrându-se pe garantarea integrității, confidențialității și disponibilității informației. Progresul tehnologiei informației implică apariția unor noi riscuri pentru care organizațiile trebuie să implementeze noi măsuri de control. De exemplu, popularizarea unităților de înregistrare CD-uri sau a dispozitivelor de stocare portabile de mare capacitatea generează riscuri de copiere neautorizată sau furt de date. Utilizarea rețelelor și conectarea la internet introduc, de asemenea, riscuri suplimentare, cum ar fi accesul neautorizat la date sau frauda. [4] Dezvoltarea tehnologică a fost însoțită de soluții de securitate, cu producătorii de echipamente și aplicații incluzând metode tehnice de protecție din ce în ce mai avansate.

Cu toate acestea, în timp ce în domeniul tehnologiilor informaționale schimbarea este rapidă, elementul uman rămâne la fel de important. Asigurarea securității informațiilor nu poate fi realizată exclusiv prin măsuri tehnice, ci reprezintă în principal o problemă umană. Cele mai multe incidente de securitate sunt cauzate de o gestionare și organizare necorespunzătoare, mai degrabă decât de deficiențele mecanismelor de securitate. Este esențial ca organizațiile să conștientizeze riscurile asociate cu utilizarea tehnologiei și gestionarea informațiilor și să abordeze această problemă printr-o conștientizare a importanței securității informațiilor printre angajați, înțelegând tipurile de amenințări, riscurile și vulnerabilitățile specifice mediilor informatizate și aplicând practici de control[6].

Paragraful subliniază că, în ciuda schimbărilor rapide din domeniul tehnologiilor informaționale, rolul uman rămâne la fel de esențial în garantarea securității informațiilor. Se evidențiază că securitatea informațiilor nu poate fi asigurată doar prin mijloace tehnice, ci necesită în mod predominant implicarea oamenilor. Importanța unei gestionări și organizări adecvate pentru a preveni incidentele de securitate este subliniată, iar organizațiile sunt îndemnate să conștientizeze riscurile legate de utilizarea tehnologiei și să-și educe angajații în ceea ce privește importanța securității informațiilor, pentru a înțelege și a gestiona amenințările și vulnerabilitățile specifice.

Organizația Internațională pentru Standardizare (ISO) și Comisia Internațională Electrotehnică (IEC) constituie un forum specializat pentru standardizare. Statele membre ale ISO și IEC

participă la elaborarea standardelor internaționale prin intermediul comitetelor tehnice. Statele Unite ale Americii, prin Institutul Național de Standardizare, îndeplinește funcția de secretar, în timp ce alte 24 de țări sunt participante (cum ar fi Brazilia, Franța, Regatul Unit, Coreea, Cehia, Germania, Danemarca, Belgia, Portugalia, Japonia, Olanda, Irlanda, Norvegia, Africa de Sud, Australia, Canada, Finlanda, Suedia, Slovenia, Elveția, Noua Zeelandă și Italia), iar alte 40 de țări au statut de observator. [4]

Puterea este conferită deținerii informației, deoarece informația reprezintă cunoaștere. Schimbul de informații este esențial în societate și a evoluat în conținut și intensitate de-a lungul timpului. Odată cu diversificarea informațiilor și complexitatea mesajelor, au apărut specializări, noi forme de organizare și modalități de memorizare. În era modernă, odată cu avansul tehnologiilor informaționale, informația a devenit omniprezentă în sfera comunicării și guvernării. Fluxul informațiilor în societate poate fi gestionat și organizat, ducând la apariția rețelelor și a structurilor informaționale extinse. Etapele de dezvoltare ale societăților reflectă de fapt etapele procesului informațional[8].

Paragraful evidențiază importanța informației în societate și schimbările în schimbul de informații de-a lungul timpului. Este notabil cum diversificarea și complexitatea informațiilor au influențat domenii precum specializările, organizarea și metodele de memorizare. În epoca contemporană, progresul tehnologiilor informaționale a amplificat rolul informației în comunicare și guvernare, contribuind la dezvoltarea unor rețele și structuri informaționale sofisticate.

Progresul unei țări este strâns legat de modul în care statul și instituțiile publice gestionează procesul informațional. În prezent, obținerea abilităților și utilizarea modalităților eficiente de a obține informații reprezintă un aspect valoros. În același timp, problemele legate de securitatea informațională devin tot mai relevante în diferite domenii precum administrația publică locală, mediul de afaceri și societatea civilă. Securitatea continuă să fie o problemă fundamentală în societatea umană, iar definirea sa este un subiect de mare importanță în documentele oficiale ale organizațiilor internaționale. Organizația Națiunilor Unite definește sectorul de securitate ca fiind ansamblul instituțiilor, grupurilor, organizațiilor și persoanelor, atât de stat cât și non-statale, care participă și sunt responsabile de administrarea, promovarea și monitorizarea securității într-un stat. [5]

- Elementele fundamentale ale domeniului securității, care includ instituțiile responsabile de menținerea ordinii și a dreptului, cum ar fi forțele armate, poliția, carabinierii, instituțiile penitenciare, forțele paramilitare, serviciile de informații, instituțiile de pază de frontieră, autoritățile vamale și serviciile pentru situații de urgență.
- Elementele de gestionare și monitorizare includ entități legislative și comisii corespunzătoare, executivul, cuprinzând ministerele apărării, afacerilor interne și afacerilor externe, instituțiile consultative naționale, autoritățile financiare de conducere și reprezentanții societății civile, precum mass-media, mediul academic și organizațiile neguvernamentale.
- Elementele sistemului judiciar includ ministerele responsabile de justiție, autoritățile de urmărire penală și procuratura, instanțele judiciare, organizațiile de aplicare a legii, comisiile pentru drepturile omului și avocații desemnați în parlament.
- Elementele ne-guvernamentale ale forțelor de securitate includ organizații militare neoficiale, unități paramilitare private și firme private de securitate.

Fiecare națiune se vede nevoită să garanteze securitatea, care este acum într-o formă nouă. În prezent, amenințările vizează mai mult elementele de sprijin ale comunităților umane și sunt mai subtile decât cele tradiționale. Informația și modul său de transmitere au fost mereu de o importanță crucială pentru stat, pentru exercitarea guvernării la toate cele trei niveluri existente, iar utilizarea tehnologiilor informaționale și a rețelelor de calculatoare reprezintă un aspect definitoriu al epocii noastre, unde informația este considerată materia primă[5].

Paragraful evidențiază necesitatea securității într-o perioadă în care amenințările devin tot mai subtile și afectează aspecte esențiale ale comunităților umane. Transmiterea și gestionarea informațiilor sunt vitale pentru buna funcționare a statului și pentru exercitarea guvernării la toate nivelurile.

Tehnologia informațională și rețelele de calculatoare sunt elemente fundamentale în societatea contemporană, în care informația este considerată resursa-cheie. În termeni simpli, informația reprezintă fundamentul acestei ere a tehnologiilor informaționale. În plus, relevanța informației și a sistemelor de comunicații pentru societate crește odată cu valoarea și volumul informației transmise și stocate. Pe măsură ce tehnologia avansează, spațiile virtuale, care cândva erau doar concepte abstracte, acum încep să prindă viață și să devină parte integrantă a realității. În contrast cu informația tipărită pe hârtie, informația în format electronic poate fi susceptibilă la furt la distanță și, în general, este mult mai ușor de interceptat, modificat și utilizat în scopuri malefice, ceea ce poate provoca daune semnificative atât financiare, cât și de destabilizare în societate[10].

Aplicarea normelor în vigoare privind protecția informațiilor clasificate funcționează în mod unitar la nivel național. În cadrul acestui sistem, se implementează și se emit măsuri de securitate pentru protejarea informațiilor clasificate stocate, procesate sau transmise de către Serviciul de Protecție și Pază a Datelor (SPAD) sau de către Departamentul de Tehnologia Informației și Comunicațiilor - Sistemul Informatic Centralizat (RTD-SIC). De asemenea, se efectuează și controlul modului în care sunt implementate aceste măsuri de securitate. Această activitate este realizată de o structură funcțională care are atribuții de reglementare, control și autorizare și care include[11]:

- O instituție responsabilă cu acordarea acreditării pentru funcționarea într-un regim de securitate.
- O instituție însărcinată cu asigurarea securității criptografice.
- O entitate care dezvoltă și pune în aplicare strategii, tehnici și proceduri de securitate.

Agențiile menționate sunt supuse autorității instituției naționale desemnate pentru protecția informațiilor clasificate, respectiv Oficiului Registrului Național al Informațiilor Secrete de Stat (ORNISS). Actualizarea constantă a măsurilor de protecție a informațiilor clasificate în format electronic necesită identificarea, documentarea și gestionarea continuă a amenințărilor și vulnerabilităților la adresa acestor informații și a sistemelor care le manipulează, stochează și transmit.

Paragraful evidențiază relevanța organizației naționale responsabile de protecția informațiilor clasificate, cum ar fi Oficiul Registrului Național al Informațiilor Secrete de Stat (ORNISS). Se subliniază necesitatea permanentă de a actualiza măsurile de securitate pentru informațiile clasificate în format electronic prin identificarea, documentarea și gestionarea continuă a amenințărilor și vulnerabilităților.

Măsurile de securitate INFOSEC vor fi organizate în funcție de nivelul de clasificare al informațiilor pe care le protejează și în conformitate cu caracteristicile acestora. Conducătorul unității care deține informații clasificate este responsabil de securitatea propriilor informații stocate, procesate sau transmise în cadrul Sistemului de Procesare Automată a Datelor (SPAD) sau în Rețeaua de Transmisie a Datelor (RTD) - Sistemul Informatic Centralizat (SIC) [13].

Procesul de acreditare în domeniul securității este subordonat instituției desemnate la nivel național pentru protecția informațiilor clasificate, implicând reprezentanți delegați din cadrul Autorității Delegației de Securitate (ADS) care sunt implicați în funcție de Sistemul de Procesare Automată a Datelor (SPAD) și Rețeaua de Transmisie a Datelor (RTD) - Sistemul Informatic Centralizat (SIC) care trebuie să fie acreditate, și are următoarele atribuții principale:

La nivel național, se ocupă de acreditarea și reacreditarea în domeniul securității pentru Sistemul de Procesare Automată a Datelor (SPAD) și Rețeaua de Transmisie a Datelor (RTD) -

Sistemul Informatic Centralizat (SIC) care gestionează, procesează sau transmite informații clasificate, în conformitate cu nivelul lor de clasificare[6].

- stabileşte criteriile de acreditare de securitate pentru SPAD şi RTD - SIC.
- se ocupă de evaluarea și certificarea sistemelor SPAD și RTD - SIC sau a componentelor lor individuale.
- se ocupă de acreditarea și reacreditarea în domeniul securității pentru Sistemul de Procesare Automată a Datelor (SPAD) și Rețeaua de Transmisie a Datelor (RTD) - Sistemul Informatic Centralizat (SIC) care gestionează, procesează sau transmite informații clasificate, în conformitate cu nivelul lor de clasificare.

Agenția de acreditare de securitate își desfășoară activitățile în domeniul INFOSEC în numele instituției desemnate la nivel național pentru protecția informațiilor clasificate și are însărcinarea de a stabili standarde de securitate în acest sector. Agenția pentru securitatea informatică și comunicații este o entitate subordonată instituției naționale desemnate pentru protecția informațiilor electronice clasificate, având reprezentanți delegați din cadrul Autorității Delegației de Securitate (ADS) care operează la nivel național[3].

Paragraful subliniază rolul și responsabilitățile agențiilor de securitate în domeniul INFOSEC și protecția informațiilor clasificate și electronice la nivel național. Se evidențiază structura organizatorică și relațiile dintre diferitele entități implicate în asigurarea securității informaționale. Este importantă coordonarea și colaborarea între aceste agenții pentru a garanta un mediu sigur pentru informațiile sensibile.

Agenția are atribuția de a dezvolta și implementa mijloace, metode și măsuri pentru protejarea informațiilor clasificate care sunt gestionate, procesate sau transmise prin intermediul SPAD și RTD - SIC, având ca principale responsabilități următoarele:

a) coordonează activităţile de protecţie a informaţiilor clasificate care sunt stocate, procesate sau transmise prin intermediul SPAD şi RTD - SIC;
b) elaborează şi promovează reglementări şi standarde specifice;
c) analizează cauzele incidentelor de securitate şi gestionează baza de date privind ameninţările şi vulnerabilităţile din sistemele de comunicaţie şi informatice, necesare pentru elaborarea managementul de risc;
d) semnalează agenţiei de acreditare de securitate incidentele de securitate în domeniu;
e) integrează măsurile privind protecţia fizică, de personal, a documentelor administrative, COMPUSEC, COMSEC, TEMPEST şi criptografică,
f) execută inspecţii periodice asupra SPAD şi RTD - SIC în vederea reacreditării;
g) supune certificării şi autorizării sistemele de securitate specifice SPAD şi RTD - SIC.

Pentru a-și îndeplini responsabilitățile, agenția pentru securitatea informatică și comunicațiilor colaborează cu agenția de acreditare de securitate, cu agenția de protecție criptografică și cu alte entități specializate în acest domeniu. Agenția de protecție criptografică funcționează la nivel național, fiind subordonată instituției naționale desemnate pentru protecția informațiilor clasificate și are ca principale sarcini următoarele[9]:

- Colaborează cu agenția de acreditare de securitate, cu agenția responsabilă de conceperea și implementarea metodelor, mijloacelor și măsurilor de securitate, precum și cu alte entități cu atribuții în domeniu.
- Furnizează rapoarte instituției naționale desemnate pentru protecția informațiilor clasificate cu privire la incidentele de securitate întâlnite.
- Se ocupă de distribuția materialelor și echipamentelor criptografice.
- Se ocupă de gestionarea materialelor și echipamentelor criptografice.

1.1. Definirea conceptului

Conceptul de securitate informatică sau cibernetică poate fi definit ca starea de echilibru obținută prin implementarea unui set de acțiuni proactive și reactive menite să asigure confidențialitatea, integritatea, disponibilitatea, autenticitatea și necontestabilitatea informațiilor în format electronic, a resurselor și serviciilor publice sau private din mediul cybernetic. [6]
Acest concept al securității informaționale a apărut odată cu evoluția tehnologiilor moderne care permit transferul și prelucrarea informațiilor. Instituțiile publice și companiile au realizat că acest bun virtual numit informație este adesea mai valoros decât bunurile materiale și că furtul, distrugerea, alterarea sau blocarea accesului la informație ar putea cauza daune semnificative.

Paragraful evidențiază relevanța securității informaționale în contextul progresului tehnologic contemporan și influența sa asupra societății. Se subliniază importanța protejării informațiilor electronice și a resurselor cibernetice pentru a garanta confidențialitatea, integritatea și disponibilitatea acestora.

În prezent, din nefericire, mediul online continuă să fie afectat de atacuri similare celor menționate anterior, care au loc cu o frecvență destul de ridicată. Legislația curentă oferă o protecție limitată împotriva acestor tipuri de atacuri, iar deseori atacatorii scapă nepedepsiți și nu se poate identifica întregul prejudiciu cauzat. Conceptul de securitate acoperă o gamă largă de aspecte, dar pentru a simplifica, poate fi împărțit în trei niveluri[8]:

- Securitatea fizică poate fi văzută ca nivelul extern al securității, implicând acțiuni pentru prevenirea, detectarea și restricționarea accesului direct la bunuri, valori și informații.

Să luăm în considerare un exemplu: într-un sistem distribuit, prima măsură de securitate importantă este securitatea fizică. Aceasta implică prevenirea accesului fizic la echipamente; un potențial infractor care dorește să fure informații din sistem trebuie să aibă acces fizic la echipamente în primul rând. Pe lângă aceste aspecte, securitatea fizică implică, de asemenea, implementarea măsurilor de protecție împotriva incendiilor, inundațiilor, scurgerilor de gaze și a altor calamități naturale. Toate aceste acțiuni sunt strâns legate de protecția generală a clădirilor împotriva potențialelor pericole.

- Securitatea logică constă în ansamblul tehnicilor utilizate pentru a gestiona accesul la resursele și serviciile unui sistem. Acest aspect al securității poate fi, la rândul său, împărțit în două niveluri majore.

a) nivelul de securitate a accesului;
b) nivelul de securitate a serviciilor.
Componentele cheie ale securității accesului includ: [7]

- Accesul la sistem este responsabil de nivelul de accesibilitate al utilizatorilor în sistem, de conectarea sau deconectarea unor stații.
- Accesul la cont verifică dacă utilizatorul dispune de un profil valid pentru sistem.
- După ce utilizatorul trece cu succes de cele două etape menționate anterior, sistemul îi va acorda anumite privilegii de conectare.
- Securitatea serviciilor este compusă din următoarele component: [7]
- Controlul serviciilor este responsabil pentru monitorizarea și raportarea stării serviciilor, precum și pentru emiterea avertismentelor corespunzătoare.
- Drepturile deținute în cadrul unui serviciu sunt cele care stabilesc modul în care un anumit cont de servicii poate fi utilizat.
- Securitatea juridică se referă la nivelul constituit dintr-o serie de legi naționale care reglementează încălcările celor două niveluri de securitate menționate anterior și care stabilesc sancțiuni penale pentru aceste acțiuni [8].

Sistemul de securitate fizică trebuie să fie proiectat astfel încât să permită o analiză post-eveniment care să servească drept "martor" în procesul de atingere a obiectivului de securitate juridică. Cele trei niveluri de securitate stabilesc, într-un moment dat, securitatea generală a

obiectivului protejat. Astfel, se poate observa că există o strânsă interconectare între aceste niveluri de securitate, ele influențându-se reciproc și, în anumite situații, stabilindu-și existența ca niveluri de securitate valide [8].

Paragraful evidențiază relevanța sistemului de securitate fizică și importanța oferirii de suport pentru o analiză post-eveniment, aceasta fiind crucială în asigurarea securității legale. Se remarcă conexiunea strânsă între cele trei niveluri de securitate, acestea contribuind la stabilitatea și eficacitatea generală a obiectivului protejat.

Cele menționate până acum în cadrul lucrării evidențiază că abordarea cea mai eficientă pentru asigurarea securității constă în analiza cuprinzătoare a nivelului de securitate oferit de fiecare componentă în parte și în compensarea nivelului care, într-un anumit moment, furnizează un grad de securitate mai scăzut prin aplicarea de măsuri ferme pentru consolidarea securității celorlalte două niveluri sau chiar a unuia singur, astfel încât să se asigure că protecția obiectivului să atingă sau să depășească un nivel minim necesar.

1.2. Caracteristici

Securitatea informației este esențială în administrația publică, având în vedere caracterul sensibil și importanța datelor administrate de către instituțiile guvernamentale. Dat fiind avansul rapid al tehnologiei și creșterea riscurilor complexe de securitate cibernetică, protejarea confidențialității, integrității și disponibilității datelor devine din ce în ce mai esențială. Caracteristicile securității informației în administrația publică sunt esențiale pentru protejarea informațiilor cruciale și menținerea încrederii publicului în cadrul sistemului guvernamental. Aceste aspecte cuprind: confidențialitatea, integritatea, disponibilitatea, autenticitatea, non-repudierea și auditabilitatea[14].

Securitatea în domeniul IT și al informațiilor este, de obicei, caracterizată de trei elemente principale: confidențialitatea, integritatea și disponibilitatea. Aceste concepte sunt considerate obiective ale securității informatice și sunt adesea denumite CIA triad [9]. Definițiile acestor trei aspecte pot varia în funcție de activele cărora li se acordă atenție. De exemplu, acestea pot include un calculator specific sau un sistem IT, un sistem de informații sau alte active de informare menționate anterior.

Paragraful subliniază cele trei elemente esențiale ale securității în domeniul IT și al informațiilor: confidențialitatea, integritatea și disponibilitatea, cunoscute sub numele de CIA triad. Aceste concepte reprezintă obiectivele fundamentale în asigurarea securității informaționale și pot fi adaptate în funcție de activele specifice asupra cărora se concentrează

În contextul obiectivelor securității informatice, cele trei concepte pot fi definite după cum urmează:
Confidențialitatea, uneori denumită și protecție a confidențialității, vizează prevenirea accesului neautorizat al persoanelor la informația care nu le este destinată. [10]Din cele mai vechi timpuri, omenirea a recunoscut că informația conferă putere, iar în era informațională actuală, accesul la informație este mai crucial ca niciodată. Aceasta este una dintre cele mai esențiale caracteristici ale securității informațiilor în administrația publică. Implică asigurarea protecției datelor sensibile și limitarea accesului la acestea doar pentru persoanele autorizate.

În administrația publică, confidențialitatea este fundamentală pentru securizarea informațiilor vitale, precum datele personale ale cetățenilor, informațiile privind securitatea națională, politici guvernamentale sensibile și alte informații clasificate. Menținerea confidențialității implică asigurarea protejării informațiilor sensibile împotriva accesului neautorizat și a dezvăluirii acestora. Acest lucru poate implica utilizarea tehnologiilor de securitate, precum criptografia și autentificarea, pentru a proteja datele atât în timpul stocării, cât și în timpul transmiterii lor[15].

În plus, regulile și procedurile bine definite pentru administrarea informațiilor, care includ reguli stricte privind accesul și distribuția acestora, sunt esențiale pentru menținerea confidențialității

în cadrul administrației publice. Respectarea confidențialității este crucială nu doar pentru protejarea intereselor personale și a drepturilor cetățenilor, ci și pentru consolidarea încrederii publice în autoritățile guvernamentale. Cetățenii ar trebui să fie siguri că datele lor sunt tratate cu atenție și că nu vor fi folosite în mod incorect sau dezvăluite fără consimțământul lor[13].

Prin menținerea confidențialității, administrația publică poate încuraja transparența, responsabilitatea și încrederea în instituțiile guvernamentale. În concluzie, confidențialitatea reprezintă un aspect esențial al securității informațiilor în administrația publică, având o semnificație vitală în protejarea datelor sensibile și în menținerea încrederii cetățenilor în guvern. Prin aplicarea unor politici și proceduri corespunzătoare de administrare a informațiilor și de securitate cibernetică, administrația publică poate garanta protecția informațiilor împotriva accesului neautorizat și utilizării lor incorecte, sprijinind astfel o guvernare mai deschisă și mai eficientă[13].

Accesul neautorizat la informații confidențiale poate avea repercusiuni serioase, nu doar în domeniul securității la nivel național, ci și în sfera comerțului și industriei. Principalii piloni ai protejării confidențialității în sistemele informatice sunt criptografia și controalele de acces. Ca exemplu de amenințări la adresa confidențialității, putem menționa malware-ul, intruziunile, ingineria socială, rețelele nesigure și sistemele gestionate necorespunzător. State precum Statele Unite, Canada, Australia, Japonia etc. au reglementat prin lege protecția confidențialității[11].

Integritatea, uneori denumită și exactitate, se referă la încrederea, autenticitatea, completitudinea și corectitudinea informațiilor, precum și la prevenirea modificărilor necorespunzătoare sau neautorizate ale datelor. În cadrul securității informațiilor, integritatea nu se referă doar la integritatea informației în sine, ci și la autenticitatea sursei acesteia. Mecanismele de protejare a integrității pot fi împărțite în două categorii principale. [11]

- mecanisme de prevenire- Cum ar fi, controalele de acces care previn modificările neautorizate ale informațiilor;
- mecanisme de detectare- Mecanisme care au rolul de a identifica modificările neautorizate, în situația în care mecanismele de prevenire nu și-au îndeplinit funcția.

Integritatea constituie unul dintre aspectele fundamentale ale securității informațiilor în administrația publică. Acest lucru presupune garanția că datele și informațiile rămân nealterate și necorupte în timpul transmiterii, stocării și procesării acestora, în conformitate cu politicile și regulamentele stabilite.

În administrația publică, asigurarea integrității informațiilor este crucială pentru a menține precizia și încrederea acestora. Păstrarea integrității informațiilor necesită implementarea unor tehnologii de securitate eficiente, cum ar fi sistemele de control al accesului și monitorizarea activității, cu scopul de a împiedica modificările neautorizate sau coruperea datelor. În plus, utilizarea tehnologiilor de criptare și semnături digitale este indispensabilă pentru a confirma autenticitatea și integritatea datelor în timpul transferului acestora[15].

Este esențial ca administrația publică să dezvolte politici și proceduri clare pentru gestionarea datelor și pentru a se conforma standardelor de integritate. Aceste politici ar putea include implementarea unor procese de actualizare a datelor, efectuarea de copii de siguranță și verificarea regulată a integrității lor. Prin menținerea integrității informațiilor, administrația publică poate garanta că datele sunt precise, nealterate și de încredere, aspecte esențiale pentru procesul de luare a deciziilor informate și pentru consolidarea încrederii cetățenilor în guvern[14].

Disponibilitatea reprezintă obiectivul principal al asigurării accesului la datele stocate în calculatoare numai de către persoanele autorizate. Este important ca utilizatorii să aibă acces doar la datele care le sunt destinate, iar aceasta implică existența a două categorii distincte de utilizatori cu drepturi de acces diferite: administratorii de sistem și utilizatorii generali. Aceasta constituie un aspect crucial al caracteristicilor securității informațiilor în administrația publică, vizând capacitatea de a accesa și utiliza datele în momentul necesar, fără a fi afectați de

întreruperi sau întârzieri neplanificate. În administrația publică, disponibilitatea este esențială pentru a asigura funcționarea corespunzătoare a serviciilor și pentru a oferi rapid informațiile necesare cetățenilor și altor organizații. Păstrarea disponibilității informațiilor necesită punerea în aplicare a unor strategii de securitate și gestionare a riscurilor, cu scopul de a evita sau limita amenințările care ar putea să interfereze cu accesul la informații[10].

Aceste tactici pot implica implementarea de soluții de rezervă și redundanță pentru a garanta accesul permanent la date în situații neprevăzute, cum ar fi defecțiunile tehnice sau atacurile cibernetice. De asemenea, este crucial ca autoritățile publice să dezvolte politici și protocoale bine definite pentru a gestiona situațiile de urgență și pentru a recupera datele, asigurând o restabilire rapidă a accesului la informații în cazul unor incidente sau calamități.

Paragraful accentuează importanța instaurării de soluții de rezervă și redundanță pentru menținerea continuității operaționale în situații neprevăzute, precum defecțiunile tehnice sau atacurile cibernetice. Totodată, subliniază necesitatea ca autoritățile publice să elaboreze politici și protocoale clare pentru a gestiona situațiile de urgență și a recupera datele, asigurând astfel o restabilire rapidă a accesului la informații în caz de incidente sau calamități.

De asemenea, monitorizarea și menținerea constantă a infrastructurii IT sunt vitale pentru a garanta disponibilitatea neîntreruptă a serviciilor și a informațiilor. Prin menținerea disponibilității informațiilor, administrația publică poate sprijini creșterea eficienței operaționale și îmbunătățirea serviciilor oferite cetățenilor și altor părți interesate. Aceasta poate, de asemenea, consolida încrederea publicului în instituțiile guvernamentale și poate promova transparența și responsabilitatea în administrația publică. Cu toate acestea, trebuie menționat că anumite sisteme de operare instalate pe calculatoarele desktop pot permite accesul utilizatorilor generali la configurările de securitate ale sistemului sau chiar posibilitatea de a le anula. [9]

Autenticitatea informațiilor se concentrează pe garantarea faptului că acestea au provenit din surse legitime și că sunt veridice. În contextul administrației publice, este de o importanță crucială să se confirme că datele și comunicările provin într-adevăr de la surse autorizate și să se evite orice formă de falsificare sau manipulare. Aceasta este o trăsătură esențială în domeniul securității informațiilor în administrația publică. Aceasta implică asigurarea că datele și informațiile sunt corecte, autentice și provenite de la surse legitime și de încredere. În mediul guvernamental, autenticitatea este esențială pentru menținerea integrității proceselor decizionale și pentru furnizarea de informații corecte cetățenilor.

Pentru a garanta autenticitatea informațiilor, autoritățile publice pot adopta diverse soluții, inclusiv sisteme de autentificare a utilizatorilor și a datelor, semnături digitale și criptare. Aceste tehnologii sunt utile pentru a confirma că datele nu au fost alterate în timpul transferului sau stocării și că au fost furnizate de surse autentice și autorizate. În plus, este crucial ca autoritățile publice să stabilească și să urmeze standarde riguroase de securitate și autenticitate în administrarea informațiilor, inclusiv prin implementarea unor politici și proceduri clare și prin oferirea de formare și educație adecvată pentru angajați[10].

Prin confirmarea autenticității informațiilor, autoritățile publice pot întări încrederea cetățenilor în guvern și pot sprijini creșterea transparenței, responsabilității și eficienței în cadrul administrației publice.

Non-repudierea se referă la situația în care o parte nu poate nega faptul că a trimis sau primit un mesaj sau o informație. În administrația publică, este crucial ca comunicările să fie autentice și să nu poată fi contestate într-un stadiu ulterior. Non-repudierea este un aspect crucial al securității informațiilor în administrația publică, indicând capacitatea de a certifica că o anumită acțiune sau tranzacție s-a produs și că nicio parte implicată nu poate nega mai târziu participarea sau semnătura sa în acele evenimente. În mediul guvernamental, non-repudierea este esențială pentru menținerea transparenței și responsabilității în procesele administrative și pentru confirmarea acțiunilor și deciziilor luate[7].

Pentru a integra non-repudierea în administrația publică, se pot utiliza o varietate de tehnologii și protocoale, precum semnăturile digitale și jurnalele de auditare. Aceste mijloace contribuie la înregistrarea și validarea acțiunilor și tranzacțiilor, furnizând dovezi robuste în eventualitatea unor dispute sau contestații ulterioare. În plus, este esențial ca autoritățile publice să dezvolte politici și proceduri bine definite pentru administrarea non-repudierii și să ofere formare adecvată angajaților în privința participării lor în aceste procese. Prin adoptarea non-repudierii, administrația publică poate consolida încrederea cetățenilor în guvern și poate sprijini consolidarea transparenței și responsabilității în cadrul administrației publice.

Paragraful evidențiază necesitatea încorporării conceptului de non-repudiere în cadrul administrației publice, evidențiind utilizarea diferitelor tehnologii și protocoale, precum semnăturile digitale și jurnalele de auditare. Aceste instrumente sunt esențiale pentru înregistrarea și confirmarea acțiunilor și tranzacțiilor, furnizând dovezi fiabile în eventualitatea unor contestații ulterioare.

Auditabilitatea se concentrează pe capacitatea de a monitoriza și înregistra activitățile legate de accesul și utilizarea informațiilor. În administrația publică, este crucial să se implementeze mecanisme de auditare pentru a asigura respectarea politicilor și reglementărilor de securitate, precum și pentru a investiga orice incidente de securitate sau utilizări neautorizate. În general, aceste caracteristici ale securității informațiilor sunt de importanță crucială pentru protejarea datelor guvernamentale și menținerea încrederii publicului în administrația publică[6].

Prin implementarea unor politici și practici adecvate de securitate a informațiilor, instituțiile guvernamentale pot asigura că datele sensibile sunt protejate împotriva amenințărilor cibernetice și că sunt utilizate într-un mod responsabil și eficient în beneficiul cetățenilor. Auditabilitatea reprezintă o caracteristică fundamentală a securității informațiilor în administrația publică. Aceasta constă în capacitatea de a supraveghea și înregistra activitățile și evenimentele asociate securității informațiilor, pentru a garanta respectarea politicilor și standardelor stabilite.

În mediul administrației publice, auditabilitatea este esențială pentru a furniza o evidență concretă și verificabilă a acțiunilor și deciziilor luate în contextul securității informațiilor. Aceasta facilitează identificarea și investigarea incidentelor de securitate, detectarea utilizării neautorizate a datelor și respectarea normelor și reglementărilor aplicabile. Pentru a introduce auditabilitatea în administrația publică, se pot utiliza diferite instrumente și tehnologii, cum ar fi jurnalele de auditare, sistemele de monitorizare a activității și instrumentele de analiză a datelor[13].

De asemenea, este crucial să se instituie politici și proceduri clare pentru administrarea auditării și pentru a garanta că aceasta este efectuată în mod regulat și eficace. Prin asigurarea auditabilității în cadrul administrației publice, se poate îmbunătăți încrederea cetățenilor în guvern și se pot promova transparența și responsabilitatea în procesele administrative. De asemenea, acest lucru poate contribui la îmbunătățirea securității informațiilor și la reducerea riscurilor asociate cu amenințările cibernetice și cu utilizarea neautorizată a datelor.cu atribuţii specifice în domeniul INFOSEC. [12]

Se aplică măsuri de protecție a informațiilor clasificate în format electronic sistemelor care stochează, procesează sau transmit astfel de informații, cum ar fi SPAD și RTD - SIC. Unitățile care dețin informații clasificate sunt responsabile să stabilească și să pună în aplicare un set complet de măsuri de securitate pentru sistemele SPAD și RTD - SIC, care includ măsuri fizice, de personal, administrative, de tip TEMPEST și criptografice. Măsurile de securitate pentru protejarea sistemelor SPAD și RTD - SIC trebuie să garanteze controlul accesului, cu scopul de a preveni sau detecta divulgările neautorizate de informații. Procesul de certificare și acreditare va evalua dacă aceste măsuri sunt adecvate.

Paragraful evidențiază necesitatea implementării măsurilor de securitate pentru informațiile clasificate în format electronic, în special în ceea ce privește sistemele cum ar fi SPAD și RTD - SIC.

Cerințele de securitate specifice (CSS) sunt stabilite printr-un acord între agenția de acreditare de securitate și CSTIC. Acest document va include principii și măsuri de securitate care trebuie respectate în procesul de certificare și acreditare a sistemelor SPAD sau RTD - SIC. Pentru fiecare sistem SPAD și RTD - SIC care prelucrează, stochează sau transmite informații clasificate, se elaborează cerințe specifice de securitate (CSS). Acestea sunt stabilite de CSTIC și apoi aprobate de către agenția de acreditare de securitate[4].

Cerințele specifice de securitate (CSS) sunt elaborate încă din faza de proiectare a sistemului SPAD sau RTD - SIC și sunt dezvoltate pe întregul ciclu de viață al acestora. Aceste cerințe sunt fundamentate pe standardele naționale de protecție, pe parametrii esențiali ai mediului operațional, pe nivelul minim de autorizare a personalului, pe nivelul de clasificare a informațiilor gestionate și pe modul de operare al sistemului ce urmează să fie acreditat. SPAD și RTD - SIC care gestionează, prelucrează sau transmit informații clasificate trebuie să fie certificate și acreditate pentru operare în unul dintre următoarele moduri, pentru anumite perioade de timp: [4]
a) dedicat;
b) de nivel înalt;
c) multi-nivel.

În regimul de operare dedicat, toți cei care au acces la SPAD sau RTD trebuie să dețină un certificat de securitate corespunzător nivelului maxim de clasificare a informațiilor gestionate de aceste sisteme. Persoanele respective trebuie să aibă acces la toate informațiile stocate, procesate sau transmise în cadrul SPAD sau RTD - SIC. În acest mod de operare, principiul necesității de a cunoaște nu necesită o segregare a informațiilor în cadrul SPAD sau RTD ca metodă de securitate a SIC. Celelalte precauții luate vor garanta respectarea cerințelor impuse de cel mai ridicat nivel de clasificare al informațiilor gestionate și de toate categoriile de informații cu destinație specială stocate, procesate sau transmise în cadrul SPAD sau RTD.

Paragraful subliniază relevanța implementării unui regim de operare dedicat pentru sistemele SPAD sau RTD - SIC, unde accesul este permis doar celor care dețin un certificat de securitate adecvat nivelului maxim de clasificare a informațiilor. Acest mod de operare facilitează accesul la toate informațiile gestionate de aceste sisteme, fără a necesita segregarea acestora în cadrul SPAD sau RTD - SIC.

În modul de operare de nivel înalt, fiecare persoană autorizată să aibă acces la SPAD sau RTD SIC trebuie să dețină un certificat de securitate pentru cel mai înalt nivel de clasificare a informațiilor stocate, procesate sau transmise în cadrul acestora. Accesul la informații va fi gestionat diferențiat, în conformitate cu principiul necesității de a cunoaște. Pentru a respecta principiul necesității de a cunoaște și pentru a asigura accesul diferențiat la informații, se implementează facilități de securitate care permit un acces selectiv la informații în cadrul SPAD sau RTD - SIC[3].

Alte dispoziții de securitate vor fi conforme cu cerințele pentru cel mai înalt nivel de clasificare și pentru toate categoriile de informații cu destinație specială stocate, procesate și transmise în cadrul SPAD sau RTD - SIC. Toate datele gestionate în cadrul unui SPAD sau RTD - SIC în această configurație vor fi tratate ca informații cu destinație specială, cu cel mai înalt nivel de clasificare identificat în totalitatea datelor stocate, procesate sau transmise prin sistem. În modul de operare multi-nivel, accesul la informaţiile clasificate se face diferențiat, potrivit principiului necesităţii de a cunoaşte, conform următoarelor reguli [13]:
a) nu toate persoanele cu drept de acces la SPAD sau RTD -SIC au certificat de securitate pentru acces la informaţii de cel mai înalt nivel de clasificare care sunt stocate, procesate sau transmise prin aceste sisteme;
b) nu toate persoanele cu acces la SPAD sau RID - SIC au acces la toate informaţiile stocate, procesate sau transmise prin aceste sisteme.

Aplicarea regulilor prevăzute la alin. (1) impune instituirea, în compensaţie, a unor facilităţi de securitate care să asigure un mod selectiv, individual, de acces la informaţiile clasificate din

cadrul SPAD sau RTD -SIC. Securitatea SPAD a reţelei şi a obiectivului SIC se asigură prin funcţiile de administrator de securitate, care sunt:
a) administratorul de securitate al SPAD;
b) administratorul de securitate al reţelei;
c) administratorul de securitate al obiectivului SIC.

Funcţiile de administratori de securitate trebuie să asigure îndeplinirea atribuţiilor CSTIC. Dacă este cazul, aceste funcţii pot fi cumulate de către un singur specialist. CSTIC desemnează un administrator de securitate al SPAD responsabil cu supervizarea dezvoltării, implementării şi administrării măsurilor de securitate dintr-un SPAD, inclusiv participarea la elaborarea procedurilor operaţionale de securitate. La recomandarea autorităţii de acreditare de securitate, CSTIC poate desemna structuri de administrare ale SPAD care îndeplinesc aceleaşi atribuţii[3].

Administratorul de securitate al reţelei este desemnat de CSTIC pentru un SIC de mari dimensiuni sau în cazul interconectării mai multor SPAD şi îndeplineşte atribuţii privind managementul securităţii comunicaţiilor. Administratorul de securitate al obiectivului SIC este desemnat de CSTIC sau de autoritatea de securitate competentă şi răspunde de asigurarea implementării şi menţinerea măsurilor de securitate aplicabile obiectivului SIC respectiv.

Paragraful evidențiază importanța administratorului de securitate în asigurarea securității rețelei, fie că este vorba de un SIC de mari dimensiuni sau de interconectarea mai multor SPAD. El are atribuții cruciale în gestionarea securității comunicațiilor și trebuie să garanteze implementarea și menținerea adecvată a măsurilor de securitate pentru obiectivul SIC respectiv.

Responsabilităţile unui administrator de securitate al obiectivului SIC pot fi îndeplinite de către structura/funcţionarul de securitate al unităţii, ca parte a îndatoririlor sale profesionale. Obiectivul SIC reprezintă un amplasament specific sau un grup de amplasamente în care funcţionează un SPAD şi/sau RTD. Responsabilităţile şi măsurile de securitate pentru fiecare zonă de amplasare a unui terminal/staţie de lucru care funcţionează la distanţă trebuie explicit determinate. [3]

Toţi utilizatorii de SPAD sau RTD - SIC poartă responsabilitatea în ce priveşte securitatea acestor sisteme - raportate, în principal, la drepturile acordate şi sunt îndrumaţi de către administratorii de securitate. Utilizatorii vor fi autorizaţi pentru clasa şi nivelul de secretizare a informaţiilor clasificate stocate, procesate sau transmise în SPAD sau RTD - SIC. La acordarea accesului la informaţii, individual, se va urmări respectarea principiului necesităţii de a cunoaşte. Informarea şi conştientizarea utilizatorilor asupra îndatoririlor lor de securitate trebuie să asigure o eficacitate sporită a sistemului de securitate.

Vizitatorii trebuie să aibă autorizare de securitate de nivel corespunzător şi să îndeplinească principiul necesităţii de a cunoaşte, în situaţia în care accesul unui vizitator fără autorizare de securitate este considerat necesar, vor fi luate măsuri de securitate suplimentare pentru ca acesta să nu poată avea acces la informaţiile clasificate public. [13]

1.3. Relația dintre administrația publică și securitatea informației

Relația dintre administrația publică și securitatea informației este de o importanță critică în protejarea datelor și asigurarea funcționării eficiente a guvernului. Securitatea informației în administrația publică se concentrează pe protejarea datelor și informațiilor sensibile gestionate de instituțiile guvernamentale, cu scopul de a le menține confidențiale, integre și accesibile doar utilizatorilor autorizați [14].

Administrația publică este obligată să se conformeze unor reglementări și standarde riguroase privind securitatea informațiilor, impuse de legislația și directivele naționale și internaționale. Respectarea acestor reguli este crucială pentru protejarea datelor și pentru a evita consecințele legale. Reglementările și standardele au o importanță fundamentală în cadrul relației dintre administrația publică și securitatea informațiilor. Pentru a garanta securitatea datelor,

administrația publică trebuie să se conformeze cu cerințele și standardele riguroase stabilite de legislația națională și internațională. [15]

Aceste norme și reguli pot să se concentreze pe protecția datelor, evaluarea și gestionarea riscurilor cibernetice, precum și aplicarea măsurilor de securitate pentru informațiile clasificate. Respectarea acestor reglementări și standarde este crucială pentru a asigura securitatea datelor și pentru a evita consecințele legale. Administrația publică deține o varietate de informații sensibile, incluzând date personale ale cetățenilor, informații de securitate națională, politici guvernamentale delicate și alte date clasificate. Este vital să se protejeze aceste informații pentru securitatea națională și pentru a respecta drepturile și confidențialitatea cetățenilor.

Paragraful subliniază importanța normelor și regulilor în protejarea datelor, evaluarea riscurilor cibernetice și implementarea măsurilor de securitate pentru informațiile clasificate. Respectarea acestor standarde este esențială pentru a garanta securitatea datelor și pentru a preveni eventualele consecințe legale. Este evident că adoptarea și aplicarea acestor reguli sunt fundamentale într-o lume digitală tot mai interconectată.

Sensibilitatea datelor este de o importanță crucială în cadrul colaborării dintre administrația publică și securitatea informației. Instituțiile guvernamentale au în gestiune o diversitate de informații sensibile, cuprinzând datele personale ale cetățenilor, informații de securitate națională și politici guvernamentale cu caracter delicat. Asigurarea securității acestor date este vitală pentru protejarea securității naționale și pentru respectarea drepturilor și vieții private ale cetățenilor.

Pentru a garanta securitatea datelor sensibile, administrația publică trebuie să adopte politici și măsuri riguroase de Securitate a informațiilor. Aceste acțiuni pot implica criptarea datelor, controlul strict al accesului la informații și monitorizarea constantă a sistemelor informatice. Păstrarea confidențialității datelor este crucială pentru a menține încrederea publicului în instituțiile guvernamentale și pentru a promova transparența și responsabilitatea în gestionarea informațiilor. Aceasta este expusă la riscuri din ce în ce mai avansate în mediul online, cum ar fi atacurile cibernetice, hacking-ul și sustragerea de date. Este crucial ca administrația să se protejeze împotriva acestor amenințări pentru a preveni pierderea de date și perturbările în funcționarea activităților guvernamentale [13].

Amenințările din mediul cibernetic sunt un factor important în legătura dintre administrația publică și securitatea informației. În acest context, administrația publică se expune la o varietate de riscuri, cum ar fi atacurile cibernetice, incursiunile în sistem și sustragerea de date.Este vital ca autoritățile guvernamentale să fie înarmate împotriva acestor riscuri și să pună în aplicare strategii de securitate cibernetică eficiente pentru a-și proteja datele și infrastructura IT. Prin urmare, asigurarea securității informațiilor este fundamentală pentru a preveni pierderea de date și pentru a menține integritatea și buna funcționare a guvernului.

Paragraful evidențiază relevanța amenințărilor cibernetice în contextul relației dintre administrația publică și securitatea informației. Provocările precum atacurile cibernetice, intruziunile în sistem și furtul de date constituie probleme semnificative cu care se confruntă administrația publică în epoca digitală.

Elaborarea și punerea în aplicare a unor politici și proceduri bine definite pentru securitatea informațiilor sunt esențiale pentru a asigura o abordare unitară și eficientă în administrația publică. Aceste politici ar trebui să vizeze aspecte precum gestionarea accesului la informații, utilizarea criptografiei, supravegherea și raportarea incidentelor de securitate. Politiciile și procedurile joacă un rol semnificativ în relația dintre administrația publică și securitatea informației. Acestea reprezintă ghiduri și reguli stabilite pentru a asigura protecția adecvată a datelor și a sistemelor informatice în cadrul instituțiilor guvernamentale. Implementarea unor politici și proceduri clare în domeniul securității informațiilor este esențială pentru gestionarea riscurilor de securitate și pentru prevenirea incidentelor de securitate cibernetică [13].

Aceste politici și proceduri pot include reguli privind gestionarea accesului la informații, criptarea datelor, monitorizarea activităților și raportarea incidentelor de securitate. Prin stabilirea și respectarea acestor politici și proceduri, administrația publică poate promova o cultură a securității informațiilor și poate contribui la protejarea datelor și a activităților guvernamentale împotriva amenințărilor cibernetice. Instruirea și educarea angajaților sunt fundamentale pentru cultivarea unei culturi a securității informațiilor în cadrul administrației publice. Este important ca personalul să fie conștient de riscurile de securitate și să fie instruit în practici și proceduri sigure pentru protejarea datelor.

Paragraful evidențiază relevanța stabilirii și respectării unor politici și proceduri clare în administrația publică pentru a proteja datele și activitățile împotriva amenințărilor cibernetice. Implementarea regulilor referitoare la gestionarea accesului, criptarea datelor și raportarea incidentelor de securitate poate încuraja o cultură a securității informațiilor.

Colaborarea și cooperarea cu alte organizații sunt esențiale pentru administrația publică în vederea consolidării capacităților sale de securitate și pentru a face față cu mai multă eficiență amenințărilor cibernetice. Acest lucru poate implica schimbul de informații, partajarea de bune practici și cooperarea în gestionarea incidentelor. Implementarea tehnologiei moderne, inclusiv a soluțiilor de securitate cibernetică, a criptografiei și a autentificării în doi factori, poate juca un rol esențial în asigurarea protecției datelor și în întărirea securității informațiilor în cadrul administrației publice. [14]

Prin abordarea detaliată a acestor aspecte și prin acordarea unei atenții constante securității informațiilor, administrația publică poate garanta protejarea informațiilor sensibile, asigurarea funcționării eficiente a guvernului și consolidarea încrederii publicului în instituțiile guvernamentale.

Prin examinarea în detaliu și acordarea unei atenții constante securității informațiilor în administrația publică, se subliniază importanța. Prin protejarea informațiilor sensibile și asigurarea funcționării eficiente a guvernului, se poate consolida încrederea publicului în instituțiile guvernamentale

Capitolul 2. Protejarea datelor cu caracter sensibil în administrația publică

Asigurarea securității datelor cu caracter sensibil în cadrul administrației publice reprezintă un aspect crucial pentru garantarea confidențialității și integrității informațiilor personale ale cetățenilor. Aceste date sensibile includ informații personale, medicale, financiare sau orice alte informații care ar putea fi exploatate în detrimentul persoanei respective. Pentru a garanta securitatea acestor informații sensibile, administrația publică trebuie să adopte politici și măsuri riguroase de securitate cibernetică. Aceste acțiuni pot implica criptarea datelor, autentificarea în doi pași, limitarea accesului la informațiile sensibile, politici clare referitoare la stocarea și partajarea datelor, și instruirea periodică a personalului în ceea ce privește standardele de securitate.[17]

Paragraful evidențiază importanța securizării datelor sensibile în administrația publică, pentru a proteja informațiile personale ale cetățenilor. Este esențial ca administrația să pună în aplicare politici și măsuri stricte de securitate cibernetică, precum criptarea datelor și autentificarea în doi pași, pentru a preveni accesul neautorizat și utilizarea incorectă a acestor informații.

În plus, este esențial ca administrația publică să colaboreze cu autoritățile competente pentru a detecta și preveni potențialele amenințări cibernetice sau încălcări de securitate. Totodată, o comunicare transparentă și deschisă cu cetățenii privind modalitățile de protejare și utilizare a datelor lor sensibile de către administrația publică este necesară. Prin garanția unei protecții corespunzătoare a datelor cu caracter sensibil, administrația publică dobândește încrederea cetățenilor și evidențiază angajamentul față de protejarea informațiilor personale. Acest aspect este vital pentru eficiența serviciilor publice și pentru menținerea unui stat de drept transparent și echitabil.

2.1. *Importanța datelor cu caracter sensibil în procesele administrative*

În societatea contemporană, procesele administrative reprezintă un element fundamental pentru buna funcționare a instituțiilor guvernamentale și a altor entități organizaționale. Aceste procese presupun colectarea, gestionarea și utilizarea unei cantități semnificative de informații, printre care se numără și datele cu caracter sensibil. Informațiile cu caracter sensibil sunt acele date ce pot furniza detalii personale, precum informații medicale, financiare, etnice, religioase sau politice, fiind protejate conform legilor și reglementărilor referitoare la protecția datelor personale. Rolul crucial al acestor date în cadrul proceselor administrative este extins și substanțial, iar în continuare sunt expuse câteva aspecte esențiale care subliniază această importanță [16]:

Asigurarea intimității și confidențialității în contextul importanței datelor cu caracter sensibil în procesele administrative este un aspect esențial și de primă importanță pentru orice entitate guvernamentală sau organizație publică. Această măsură de siguranță este indispensabilă pentru a consolida încrederea cetățenilor în sistemul administrativ și pentru a garanta respectarea drepturilor individuale ale acestora.

Consider că asigurarea intimității și confidențialității în administrarea datelor sensibile în procesele administrative este esențială pentru orice entitate guvernamentală sau publică. Această acțiune nu numai că întărește încrederea cetățenilor în sistemul administrativ, dar și garantează respectarea drepturilor individuale ale acestora Mai jos sunt prezentate detalii suplimentare referitoare la importanța asigurării intimității și confidențialității în acest context[23]:

- Dreptul la intimitate este garantat cetățenilor, asigurându-le protecția vieții private. Informațiile de natură sensibilă, cum ar fi cele medicale sau legate de orientarea sexuală, sunt adesea privite ca aspecte intime și, în consecință, trebuie gestionate cu cea mai mare atenție și confidențialitate în contextul proceselor administrative.
- Crearea încrederii este crucială: cetățenii trebuie să fie convinși că datele lor cu caracter sensibil sunt în siguranță și vor fi gestionate responsabil de către autoritățile guvernamentale. O protecție corespunzătoare a intimității și a confidențialității este esențială pentru a câștiga și a menține această încredere.
- Există riscul ca datele cu caracter sensibil să conțină informații care ar putea expune persoanele la riscul de stigmatizare sau discriminare. De exemplu, informațiile despre starea de sănătate mentală sau despre statutul HIV pot fi folosite în mod inadecvat pentru a evalua sau exclude indivizii. Protejarea confidențialității acestor date este crucială pentru a preveni apariția unor astfel de situații.
- În lipsa unei protecții adecvate a intimității și confidențialității, există pericolul ca datele cu caracter sensibil să fie folosite în mod inadecvat sau abuziv. Aceasta poate implica accesul neautorizat la informații sau folosirea acestora pentru șantaj, hărțuire sau alte forme de abuz.
- În diverse țări, există reguli și norme stricte care reglementează colectarea, stocarea și utilizarea datelor cu caracter sensibil. Respectarea acestor reglementări este crucială nu doar pentru a evita consecințele juridice, ci și pentru a rămâne în conformitate cu principiile etice și morale ale unei societăți democratice și progresiste.
- Protejarea intimității și confidențialității în procesele administrative joacă un rol esențial în susținerea unei societăți democratice și în apărarea drepturilor civile.Cetățenii trebuie să fie siguri că informațiile lor nu vor fi folosite în mod neadecvat pentru a amenința libertățile individuale sau pentru a împiedica implicarea lor în procesul democratic.
- În încheiere, asigurarea intimității și confidențialității în cadrul datelor cu caracter sensibil în procesele administrative nu reprezintă doar o chestiune teoretică, ci este o imperativă practică și morală.Această măsură este crucială pentru a respecta drepturile individuale, pentru a consolida și a menține încrederea în instituțiile guvernamentale și pentru a promova o societate justă și egalitară.

Asigurarea respectării drepturilor individuale reprezintă un aspect crucial în cadrul gestionării datelor cu caracter sensibil în procesele administrative. Drepturile individuale, precum dreptul la intimitate, confidențialitate, autodeterminare și acces la informație, trebuie să fie protejate și tratate cu atenție în orice context în care sunt implicate date sensibile. Iată câteva modalități prin care aceste drepturi sunt fundamentale în cadrul proceselor administrative [17]:

- Dreptul la intimitate și confidențialitate este garantat cetățenilor în ceea ce privește informațiile lor personale, inclusiv cele de natură sensibilă.
- Dreptul la autodeterminare presupune că indivizii au dreptul de a decide modalitatea și momentul în care datele lor cu caracter sensibil sunt colectate și utilizate în contextul proceselor administrative. Transparența și controlul asupra modului în care sunt administrate datele personale ale cetățenilor sunt aspecte esențiale pe care organizațiile trebuie să le ofere în mod obligatoriu.
- Indivizii au dreptul să acceseze informațiile personale pe care organizațiile le dețin despre ei, inclusiv datele sensibile, conform dreptului la acces la informație. Procesele administrative trebuie să asigure un acces ușor pentru cetățeni la aceste informații și să ofere modalități clare și eficiente pentru exercitarea acestui drept.
- Cetățenii au dreptul să ceară rectificarea sau ștergerea informațiilor inexacte sau depășite cu caracter sensibil. Procedurile administrative ar trebui să ofere mijloace corespunzătoare pentru a permite cetățenilor să-și exercite acest drept într-un mod eficient și transparent.
- Protejarea împotriva discriminării este un drept important, întrucât datele sensibile pot fi folosite în mod necorespunzător pentru a discrimina sau exclude anumite grupuri de persoane. Procesele administrative trebuie să garanteze că utilizarea datelor sensibile este justificată și conformă cu legea, asigurând în același timp protecția cetățenilor împotriva oricărei forme de discriminare sau abuz.
- Procesele administrative ar trebui să urmeze principiul minimizării datelor, adică să colecteze și să utilizeze doar informațiile sensibile strict necesare pentru scopurile legale și legitime. Adunarea nejustificată sau folosirea excesivă a informațiilor sensibile poate duce la încălcarea drepturilor individuale și poate crește probabilitatea de abuzuri sau încălcări ale securității datelor.

În concluzie, este de o importanță capitală să se respecte drepturile individuale în cadrul gestionării datelor sensibile în procesele administrative. Procesele administrative ar trebui să fie structurate și implementate într-un mod care să garanteze protecția și respectarea drepturilor individuale ale cetățenilor, contribuind, în consecință, la promovarea unei societăți mai juste și mai responsabile.

Pericolul de stigmatizare și discriminare este fundamental în cadrul gestionării datelor cu caracter sensibil în procesele administrative. Informațiile cu caracter sensibil, precum cele medicale, etnice, religioase sau referitoare la orientarea sexuală, pot fi utilizate în mod incorect sau abuziv pentru a evalua sau discrimina anumite grupuri de persoane. Iată câteva puncte relevante despre această temă [17]:

- Riscul de stigmatizare: Datele cu caracter sensibil pot supune indivizii la pericolul de a fi stigmatizați sau etichetați negativ de către societate. De exemplu, informațiile referitoare la sănătatea mentală sau la istoricul medical pot fi folosite în mod necorespunzător pentru a evalua sau marginaliza acele persoane.
- Informațiile cu caracter sensibil ar putea fi utilizate în scopuri discriminatorii împotriva unor anumite grupuri sau indivizi. Ca exemplu, informațiile legate de apartenența etnică sau religioasă ar putea fi folosite pentru a izola sau exclude anumite grupuri de la diverse oportunități sau servicii.
- Impactul asupra drepturilor individuale: Utilizarea improprie a datelor cu caracter sensibil poate submina drepturile individuale, precum dreptul la egalitate, nediscriminare și intimitate. Este vital ca procesele administrative să protejeze aceste drepturi și să prevină orice formă de discriminare sau stigmatizare.

- Limitarea în exercitarea drepturilor: Indivizii ar putea fi descurajați să beneficieze de anumite servicii sau să-și exercite anumite drepturi din cauza temerii că informațiile sensibile despre ei ar putea fi utilizate împotriva lor. Această situație ar putea conduce la o subutilizare a serviciilor publice sau la o lipsă de acces la resursele necesare.
- Necesitatea Educației și Conștientizării: Este esențial ca entitățile guvernamentale să furnizeze educație și să consolideze conștientizarea cetățenilor cu privire la importanța protejării datelor cu caracter sensibil și la riscurile asociate stigmatizării și discriminării.
- Pentru a evita riscul de stigmatizare și discriminare, este fundamental să se asigure protecția cu cea mai mare atenție a integrității și confidențialității datelor cu caracter sensibil, limitând accesul la ele doar pentru persoanele autorizate.Asigurarea unei securități adecvate a datelor și respectarea principiilor de confidențialitate și anonimat sunt cruciale pentru a proteja integritatea și intimitatea datelor.

În final, preocuparea majoră pentru protejarea drepturilor individuale și pentru promovarea unei societăți juste și incluzive este reprezentată de riscul de stigmatizare și discriminare în cadrul gestionării datelor cu caracter sensibil în procesele administrative. Entitățile guvernamentale și instituțiile publice trebuie să pună în aplicare politici și proceduri care să prevină astfel de circumstanțe și să garanteze că datele cu caracter sensibil sunt gestionate cu respect și responsabilitate. [25]

O prioritare pentru instituțiile guvernamentale și organizațiile publice este să îmbunătățească serviciile oferite cetățenilor în cadrul gestionării datelor cu caracter sensibil în procesele administrative. Corecta utilizare a acestor informații poate avea un impact semnificativ în furnizarea de servicii mai eficiente, personalizate și orientate spre nevoile cetățenilor. Mai jos sunt enumerate câteva metode prin care acest lucru poate fi realizat [16]:

- Adaptarea Serviciilor: Informațiile cu caracter sensibil pot furniza detalii esențiale despre cerințele individuale ale cetățenilor. Prin examinarea acestor informații, organizațiile pot elabora servicii și programe personalizate, ajustate la necesitățile unice ale fiecărui cetățean.
- Îmbunătățirea Accesului la Servicii: Utilizarea corespunzătoare a datelor cu caracter sensibil poate facilita accesul cetățenilor la serviciile publice. Spre exemplu, informațiile medicale pot fi folosite pentru a identifica persoanele cu necesități speciale de sănătate și pentru a le oferi servicii prioritare și adecvate.
- Scăderea Timpului de Așteptare și a Birocrației: Informațiile sensibile pot fi folosite pentru a automatiza și simplifica procedurile administrative. Acest lucru ar putea duce la diminuarea timpului de așteptare și a birocrației pentru cetățeni atunci când solicită sau accesează servicii publice.
- Supravegherea Eficienței și a Impactului: Adunarea și examinarea datelor cu caracter sensibil poate asista organizațiile în evaluarea eficienței serviciilor furnizate și în identificarea potențialelor domenii de îmbunătățire. Această supraveghere regulată poate sprijini optimizarea proceselor administrative și intensificarea satisfacției cetățenilor.
- Prevenirea Fraudei și Abuzurilor: Integrarea datelor cu caracter sensibil în procesele administrative poate contribui la prevenirea fraudelor și abuzurilor. Prin analiza informațiilor, organizațiile pot identifica tipare suspecte sau comportamente neobișnuite și pot lua măsuri preventive adecvate.
- Promovarea Transparenței și Responsabilității: Folosirea responsabilă și transparentă a datelor cu caracter sensibil poate spori încrederea cetățenilor în instituțiile guvernamentale. Instituțiile ar trebui să furnizeze cetățenilor informații despre modalitățile de colectare și utilizare a datelor personale, respectând în același timp legislația referitoare la protecția datelor.

După părerea mea, integrarea datelor cu caracter sensibil în procesele administrative poate aduce multiple avantaje pentru îmbunătățirea serviciilor oferite cetățenilor. Totuși, este fundamental ca organizațiile să gestioneze aceste date cu responsabilitate și să protejeze în mod constant confidențialitatea și drepturile individuale ale cetățenilor. Prin adoptarea unor politici

transparente, etice și respectuoase referitoare la datele cu caracter sensibil, organizațiile pot juca un rol important în promovarea unei societăți mai echitabile, eficiente și centrate pe nevoile cetățenilor.

Respectarea legislației și standardelor în gestionarea datelor sensibile în procesele administrative este crucială pentru garantarea drepturilor cetățenilor și pentru menținerea securității și integrității informațiilor personale. Iată câteva aspecte esențiale care subliniază importanța conformării la aceste reglementări și norme [16]:

- Legislația, cum ar fi Regulamentul General privind Protecția Datelor (GDPR) în Uniunea Europeană sau alte legi referitoare la confidențialitatea datelor în alte regiuni, instituie standarde ridicate pentru protejarea datelor sensibile. Respectarea acestor norme este fundamentală pentru a asigura că informațiile personale sunt adunate, păstrate și utilizate într-un mod care să respecte drepturile individuale și cerințele legale.
- Prin respectarea reglementărilor și standardelor, organizațiile administrative se asigură că datele sensibile sunt menținute într-o stare sigură și integră. Aceasta presupune instituirea unor măsuri corespunzătoare pentru securitatea datelor, precum și prevenirea accesului neautorizat sau a modificărilor inadecvate ale acestor informații.
- Respectarea reglementărilor și standardelor privind protecția datelor susține promovarea transparenței și responsabilității în cadrul organizațiilor administrative. Cetățenii au dreptul să fie informați despre modul în care sunt colectate și utilizate datele lor personale și să aibă încredere că organizațiile respectă normele legale în această privință.
- Normele și reglementările stabilesc limite precise asupra modului în care pot fi utilizate datele sensibile. Respectarea acestor reguli contribuie la prevenirea abuzurilor și utilizării inadecvate a datelor, cum ar fi accesul neautorizat sau dezvăluirea informațiilor personale fără consimțământul adecvat.
- Încălcarea reglementărilor și normelor referitoare la protecția datelor poate aduce consecințe serioase organizațiilor administrative, printre care amenzi financiare semnificative și prejudicierea reputației lor. De aceea, respectarea acestor reguli este crucială pentru a preveni sancțiunile și repercusiunile negative asociate.
- Respectarea reglementărilor și standardelor privind protecția datelor încurajează promovarea unei culturi de respect și etică în cadrul organizațiilor administrative. Acest lucru implică conștientizarea de către angajați a importanței protejării datelor personale și acțiunea în conformitate cu principiile etice și legale.

Aspectele de mai sus relevă faptul că respectarea reglementărilor și standardelor privind protecția datelor este vitală în contextul datelor cu caracter sensibil în procesele administrative. Aceasta nu numai că protejează drepturile individuale și integritatea informațiilor personale, ci și încurajează transparența, responsabilitatea și o cultură de respect și etică în cadrul organizațiilor administrative.

Autoritățile publice sunt supuse unor cerințe și responsabilități distincte în ceea ce privește Regulamentul General privind Protecția Datelor (GDPR), uneori divergente față de cele ale entităților private. În administrația publică, responsabilitatea este mai accentuată, deoarece datele cu caracter sensibil nu sunt doar stocate, ci adesea și transferate. Mai mult, trebuie să se țină cont și de legislația specifică care trebuie să se conformeze principiilor GDPR[24].
Principalele dificultăți întâmpinate de sectorul public în ceea ce privește GDPR includ [18]:

- colectarea și transferul datelor;
- respectarea drepturilor persoanelor vizate;
- numirea responsabilului cu protecția datelor (DPO);
- implementarea procedurilor specifice pentru autorități;
- instituții publice și aplicarea regimului sancționator.

Conform prevederilor Legii nr. 190/2018, *termenul autorități și organisme publice* se referă la[30]:

- „Camera Deputaților și Senatul
- Administrația Prezidențială

- Guvernul, ministerele, celelalte organe de specialitate ale administrației publice centrale
- autoritățile și instituțiile publice autonome
- autoritățile administrației publice locale și deja la nivel județean
- alte autorități publice, precum și instituțiile din subordinea/coordonarea acestora.
- unitățile de cult și asociațiile și fundațiile de utilitate publică (asimilate autorităților/organismelor publice în sensul legii)."

În ceea ce privește domeniul penal, există o lege specială, respectiv Legea nr. 363 din 28 decembrie 2018, care reglementează protecția datelor cu caracter personal în activitățile desfășurate de autoritățile competente în scopul prevenirii, descoperirii, investigării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind transferul liber al acestor date[19].

Principalele probleme din sectorul public în domeniul GDPR[16]:

- Colectarea și transferul de date rămân problematici, deoarece există încă legislație care impune acestor entități să efectueze aceste activități.
- Demonstrarea obținerii consimțământului persoanelor vizate reprezintă o preocupare, chiar și în cazurile în care majoritatea datelor sunt prelucrate în baza prevederilor legale sau, eventual, ale contractului. Obținerea consimțământului este esențială și nu este satisfăcătoare doar furnizarea informațiilor pe site-uri (în cazul cookie-urilor, chestionarelor și altor sondaje, atunci când nu sunt anonime, a softwarului, aplicațiilor, sau transferul datelor în alte scopuri decât cele inițiale pentru care au fost colectate/stocate) [19].
- Entitățile publice trebuie să efectueze, așa cum fac toți operatorii, o verificare a surselor fizice în care sunt stocate datele, în special în ceea ce privește mediile informatice utilizate. Verificarea este, fără îndoială, efectuată la nivel intelectual, prin examinarea clauzelor contractuale, pentru a se asigura că orice încălcare a securității datelor este minimizată.
- În încercarea de a obține un cost redus în cadrul licitațiilor sau pentru a stoca date personale gratuit, uneori se recurge la serviciile de cloud, iar în absența unui contract încheiat, entitățile publice rămân expuse la riscuri. Licitațiile prezintă o provocare atunci când sunt selectate produse cu costuri reduse, care nu sunt conform GDPR (inclusiv impactul asupra vieții private pentru produs), crescând riscul de incidente și încălcări ale securității datelor.
- Reducerea la minim a prelucrării datelor implică ca entitățile publice să argumenteze necesitatea prelucrării anumitor date și să implementeze măsuri tehnice și organizatorice pentru a minimiza riscurile asociate acestui proces.
- Transparența în prelucrarea datelor: este crucială pentru respectarea GDPR, conform Orientărilor GL29, care subliniază că este obligatoriu ca persoanele vizate să fie informate cu privire la prelucrarea datelor în mod echitabil, comunicarea operatorilor cu aceste persoane în legătură cu drepturile lor conform GDPR și facilitarea exercitării drepturilor acestora.

Drepturile persoanelor vizate – GDPR sector public

Într-un articol publicat în Pandectele Române nr. 2/2019 se subliniază că în sectorul public se evidențiază două riscuri care sunt rar întâlnite în sectorul privat: [18]

a)Diversitatea contextelor în care sunt procesate datele persoanelor vulnerabile.

b)Imposibilitatea de a folosi temeiul legal stipulat în articolul 6 litera f), interesul legitim (care nu este aplicabil în situația prelucrării efectuate de către autoritățile publice în exercitarea atribuțiilor lor).

Potrivit analizelor specialiștilor, se anticipează o creștere a exercitării drepturilor persoanelor vizate prin solicitări. În acest context, se întâlnesc următoarele provocări:

Gestionarea informațiilor și autentificarea identității solicitantului.

Este necesar să se examineze toate opțiunile legale disponibile pentru a descuraja solicitările abuzive, luând în considerare faptul că operatorul, inclusiv autoritatea sau organizația publică,

este responsabil de demonstrarea caracterului abuziv. Cereri repetate, solicitări anonime și cereri de date deja cunoscute de către persoana vizată reprezintă forme de hărțuire a entităților publice, însă acestea trebuie să fie demonstrate de către aceste entități. [19] Specialiștii subliniază faptul că în conformitate cu art. 12 din GDPR, excepțiile nu pot restricționa dreptul la informare și dreptul la exprimare, deoarece dreptul la protecția datelor nu este absolut. Operatorul are dreptul să impună o taxă rezonabilă sau să refuze cererea în cazul în care aceasta este considerată nefondată sau excesivă, cu condiția să demonstreze motivul pentru care a luat această decizie.

Paragraful evidențiază importanța gestionării corecte a cererilor de informații în conformitate cu GDPR și rolul operatorului în descurajarea cererilor abuzive. Este esențial să se demonstreze caracterul abuziv al acestor cereri, cum ar fi cele repetate sau anonime, iar drepturile individuale, precum dreptul la informare și la exprimare, trebuie să fie respectate întotdeauna.

Dreptul la ștergere, deși recunoscut și popular, poate avea excepții în sectorul public conform regulamentului. Astfel, acest drept nu poate fi invocat atunci când este vorba despre protecția dreptului la liberă exprimare și informare, respectarea obligațiilor legale în temeiul dreptului Uniunii sau al dreptului intern al operatorului, sau în situațiile în care informațiile sunt necesare în interes public, pentru arhivare, cercetare științifică sau istorică, scopuri statistice sau pentru apărarea unui drept în instanță [art. 17 alin. (3)]. Firește, acest drept ar putea fi exercitat atunci când datele sunt prelucrate de către autoritatea sau organizația publică în scopuri de marketing, cu condiția ca persoana vizată să fi acordat consimțământul pentru prelucrare. Entitățile publice trebuie să implementeze dreptul la ștergere fără a aștepta solicitarea persoanelor vizate, în cazul în care se aplică alte reglementări, precum cele referitoare la accesul liber la informațiile de interes public sau la Legea nr. 109/2007 privind reutilizarea informațiilor din instituțiile publice. [19]

După părerea mea, dreptul la ștergere, deși crucial în protejarea datelor personale, trebuie să fie ponderat în raport cu alte valori și interese legitime, precum libertatea de exprimare și informare sau obligațiile legale. Este necesar să se stabilească excepții clare pentru a preveni abuzul acestui drept și pentru a asigura accesul la informații esențiale pentru scopuri cum ar fi cercetarea sau apărarea în instanță.

Cererile trebuie să fie procesate de operator în termen de o lună de la primirea acestora, cu condiția ca operatorul să analizeze cu atenție temeiul legal al cererii. În cazul în care solicitantul se referă la Legii nr. 544/2001 privind liberul acces la informațiile de interes public, dar solicitarea vizează drepturile referitoare la datele cu caracter personal ale persoanei vizate, atunci cererea va fi corect încadrată conform legislației în vigoare și va primi un răspuns conform prevederilor legale aplicabile. [19]
Exercitarea anumitor drepturi nu este doar o chestiune de interpretare a termenilor, ci și de aplicare efectivă a acestora. Aceasta implică o influență asupra activității responsabilului cu protecția datelor, care nu ar trebui să avizeze toate contractele doar pentru că conțin date personale. Dreptul la rectificare are particularități importante, fiind posibil să intre în conflict cu reglementările speciale referitoare la drepturile civile. [18]

Consider că exercitarea unor drepturi nu se limitează doar la înțelegerea lor teoretică, ci și la aplicarea lor în practică. Acest aspect poate influența maniera în care responsabilul cu protecția datelor își desfășoară activitatea, evitând să avizeze în exces contractele care conțin date personale.

Nominalizarea responsabilului cu protecția datelor (DPO) în conformitate cu GDPR în sectorul public. În ceea ce privește numirea responsabilului cu protecția datelor (DPO) în cadrul autorităților publice, specialiștii subliniază elementele specifice: „Pentru toate entitățile publice, fără excepție, este obligatorie numirea unui responsabil cu protecția datelor (DPO), cu excepția instanțelor care își desfășoară activitatea în cadrul funcției lor jurisdicționale”. Anumite prevederi din Regulament facilitează numirea unui responsabil unic pentru protecția datelor, cu toate acestea există încă aspecte neclare în legislația națională și dificultăți practice legate de

numirea unui DPO pentru mai multe entități publice, conform articolului 37 alineatul (3) din GDPR [19].

Proceduri distinctive aplicate de către autoritățile și organizațiile publice în conformitate cu prevederile GDPR.
Coduri de conduită:
Din perspectiva proceselor implicate, este esențial să se inițieze discuții în cadrul organizațiilor relevante, cu accent special pe asociații, pentru a dezvolta coduri de conduită destinate unor categorii specifice de entități din sectorul public, cum ar fi primăriile. În situația în care entitatea deține pagini pe platformele de socializare, este imperativ ca aceasta să notifice adecvat părțile interesate despre acest lucru atât pe propriul său site web, cât și pe rețelele sociale respective. [25]

Actualizarea constantă a informațiilor importante:
Chiar și după un an de la implementare, este imperativ ca toate organizațiile să efectueze în mod constant evaluări ale datelor, să actualizeze înregistrările referitoare la activitățile desfășurate conform Articolului 30, să evalueze impactul asupra protecției datelor personale conform Articolului 35 și să depună eforturi adecvate pentru a asigura conștientizarea întregului personal cu privire la respectarea Regulamentului, inclusiv a posibilelor sancțiuni sau daune pe care persoanele vizate le pot cere. [22]

Tratarea posibilelor încălcări de securitate a datelor:
Abordarea posibilelor încălcări de securitate a datelor trebuie să respecte prevederile legale, fie prin solicitarea sprijinului instituțiilor competente sau autorizate. Este imperativ ca angajații să fie instruiți să raporteze imediat responsabilului cu protecția datelor orice incident de securitate și să fie conștienți că nu trebuie să intervină individual pentru a remedia posibilele consecințe.
Toate supravegherile extinse efectuate de anumite entități sau împuterniciți trebuie să fie înregistrate și documentate corespunzător.

După părerea mea, este crucial ca abordarea potențialelor încălcări de securitate a datelor să respecte normele legale, inclusiv posibila implicare a instituțiilor competente sau autorizate pentru asistență. Este vital să se ofere instruire angajaților pentru a raporta imediat orice incident de securitate responsabilului cu protecția datelor, subliniind faptul că intervenția individuală pentru remedierea consecințelor nu este recomandată.

2.2. *Digitalizarea proceselor administrative și prelucrarea datelor cu caracter sensibil*

În timpurile actuale dominate de tehnologie digitală, adoptarea digitalizării în cadrul proceselor administrative este imperativă pentru instituțiile publice și guvernamentale la nivel global. Această schimbare către sfera digitală presupune administrarea datelor cu caracter sensibil într-un mod eficient și securizat, deoarece informațiile personale și confidențiale sunt adesea colectate, reținute și utilizate în aceste procese.

Ordonanța de Urgență Nr. 38/2020 datată 30 martie 2020, referitoare la utilizarea documentelor electronice în cadrul autorităților și instituțiilor publice, a fost publicată în Monitorul Oficial Nr. 289 din 7 aprilie 2020 și detaliază mai multe aspecte tehnice legate de digitalizarea în administrația publică din România.Documentele eliberate în format electronic de către autoritățile și instituțiile publice vor fi autentificate cu semnătura electronică având calitatea de semnătură electronică calificată. Actele sunt asimilate înscrisurilor autentice. Documentele emise de autorități și instituții publice, care sunt semnate cu semnătura electronică calificată, sunt considerate autentice și au aceeași valoare juridică ca și documentele fizice semnate în mod tradițional. Pentru a primi documentele electronice, autoritățile și instituțiile publice vor furniza portaluri proprii sau vor utiliza instrumente similare oferite de terți. Dacă nu este posibilă primirea documentelor electronice conform dispozițiilor din primul alineat, autoritățile și instituțiile publice vor utiliza în acest scop poșta electronică [19].

Conform Ordonanței de Urgență nr. 39/2020 din 2 aprilie 2020, pentru completarea Legii nr. 455/2001 privind semnătura electronică, publicată în Monitorul Oficial nr. 281 din 3 aprilie 2020, Serviciul de Telecomunicații Speciale este desemnat să ofere servicii de certificare calificată exclusiv personalului autorizat din instituțiile și autoritățile publice, în vederea îndeplinirii atribuțiilor lor funcționale. [19]

Comitetul pentru debirocratizare, cunoscut și sub numele de DEBIRO, a fost înființat prin decizia prim-ministrului Ludovic Orban. Acest comitet este condus de secretarul general al Guvernului, Antonel Tănase, care îndeplinește funcția de președinte. Activitatea comitetului este coordonată de către secretarul de stat Tony Romani din cadrul Cancelariei Prim-Ministrului. Acesta se întâlnește lunar pentru a examina și aproba propunerile specifice venite de la subgrupurile sectoriale de lucru, care includ reprezentanți din mediul privat, din societatea civilă și din ministerele sau instituțiile subordonate acestora. Totodată, acest comitet are responsabilități pentru extinderea activităților realizate în domeniul digitalizării și e-guvernării de către alte entități din interiorul instituțiilor guvernamentale. Misiunea Comitetului pentru debirocratizare este de a simplifica și elimina redundanțele din legislație [19].

Obiectivele principale ale Comitetului pentru debirocratizare includ finalizarea proiectului Strategiei Naționale de Debirocratizare și Simplificare administrativă, lansarea portalului simplificare.gov.ro și punerea în aplicare a primelor inițiative în sectoare precum construcțiile și infrastructura, industria hotelieră și de restaurante (HoReCa), domeniul financiar-bancar, producția nonalimentară, dereglementarea IMM-urilor, documentele medicale-administrative, relațiile de muncă și altele[24].

Opinia mea este că obiectivele principale ale Comitetului pentru debirocratizare sunt deosebit de importante pentru îmbunătățirea eficienței administrative și economice a unei țări. Finalizarea proiectului Strategiei Naționale de Debirocratizare și Simplificare administrativă este esențială pentru a identifica și aborda principalele probleme birocratice și pentru a implementa soluții adecvate.

Transformarea digitală reprezintă una dintre prioritățile fundamentale ale administrației publice, oferind instituțiilor publice un nivel crescut de eficiență și transparență, precum și îmbunătățirea calității vieții cetățenilor. Prin adoptarea digitalizării, întreaga funcționare a instituțiilor publice devine mai eficientă, acoperind toate aspectele: de la gestionarea internă la interacțiunile cu cetățenii și alte instituții. Din păcate, conform ultimelor rapoarte europene, în special raportul DESI (Digital Economy and Society Index), România se clasează pe ultimul loc în rândul celor 28 de state membre ale Uniunii Europene, având un scor de 33,21, comparativ cu media europeană de 52,25. [16]

Conform aceluiași raport, în România, doar 6% dintre utilizatorii de internet folosesc serviciile publice digitale de e-guvernare, iar mulți nu își rezolvă problemele și necesitățile în doar 55% din cazuri. Totodată, în ceea ce privește încărcarea de către autoritățile guvernamentale a informațiilor pe site-uri și aplicații, acoperim aproximativ 65%. Regretabil, digitalizarea în România întâmpină dificultăți și este greu de implementat în administrația publică, constituind astfel un obstacol pentru dezvoltarea și modernizarea țării. Această situație afectează administrația, care contribuie în medie cu 13% la creșterea PIB-ului și cu 11% la crearea de noi locuri de muncă, precum și la reducerea costurilor administrative cu 12%.[27]

Deși sectorul IT a cunoscut o creștere semnificativă și o dezvoltare rapidă în ultimii ani, autoritățile nu au reușit să integreze eficient acest aspect în administrația publică. Nu s-au făcut demersuri pentru a susține și a promova dezvoltarea serviciilor digitale și a comunicării între instituții, ceea ce reprezintă un impediment semnificativ pentru inițiativele antreprenoriale și influențează negativ mediul de afaceri. Mai presus de toate, această absență de inițiativă împiedică modernizarea eficientă și bine coordonată a administrației publice.

Examinând această situație și concentrându-mă pe realitatea actuală, pot afirma că cei trei piloni ai unei societăți - autoritățile (în special Guvernul), mediul de afaceri și, nu în ultimul rând,

cetățenii - pot contribui la dezvoltarea și recuperarea decalajului existent. Din perspectiva mea, Guvernul ar trebui să reglementeze într-un mod mai riguros și mai precis, oferind un nivel mai mare de siguranță pentru cetățeni, în special în ceea ce privește utilizarea semnăturii electronice. De asemenea, ar trebui să definească clar procesul de emitere a facturilor sau chitanțelor electronice și să pună în aplicare legi care să întărească securitatea datelor personale.

În continuare voi oferi o scurtă prezentare a câtorva aplicații digitale dezvoltate de către autoritățile publice din România, inclusiv:
Platforma electronică pentru achiziții publice este un sistem online destinat realizării achizițiilor publice prin proceduri licitaționare, cu scopul de a garanta transparența în procesele de achiziții. Acest instrument permite tuturor autorităților administrative să achiziționeze bunuri și servicii necesare pentru satisfacerea nevoilor publice. [20]
Portalul oficial al administrației publice din România, cunoscut sub denumirea de Sistemul Electronic Național, oferă cetățenilor acces la procedurile de soluționare a problemelor, informații de contact ale instituțiilor publice din țară și link-uri pentru depunerea declarațiilor către Agenția Națională a Finanțelor Publice. [20]
Platforma Ghișeul.ro[15] este o soluție utilă pentru cetățenii din România, oferind posibilitatea de a plăti taxe, impozite, amenzi, penalizări și alte taxe utilizând metode electronice de plată. Această facilitate reprezintă un avans semnificativ în modernizarea administrației publice și aduce numeroase beneficii, cum ar fi procesarea rapidă a plăților, efectuarea acestora fără efort suplimentar, o interfață prietenoasă și reducerea timpului petrecut în cozi la ghișeele tradiționale, contribuind astfel la eficientizarea relațiilor administrative.

Unele autorități locale din România au inițiat proiecte de digitalizare și implementare a platformelor online, iar un exemplu notabil este comuna Ciugud, recunoscută pentru eforturile sale în dezvoltarea și modernizarea administrației. Printre aceste inițiative se numără crearea și implementarea unei platforme de tip aprozar virtual, care servește drept piață publică pentru comercializarea produselor locale ale producătorilor autohtoni. Această inițiativă este un model de succes care este urmat și de alte administrații locale și este considerată benefică pentru cetățenii României.

Un alt exemplu notabil în ceea ce privește digitalizarea administrației publice în România este orașul Oradea. Aici s-a implementat o platformă numită e-citizen, care facilitează eliberarea certificatelor digitale pentru semnătura electronică. Această platformă este folosită în special în cadrul fluxurilor de lucru interne și în interacțiunea cu cetățenii. [21]Prin urmare, acest program aduce o serie de avantaje, cum ar fi scurtarea timpului de așteptare pentru cetățeni, accesul rapid la documente și reducerea costurilor asociate cu utilizarea hârtiei și arhivarea documentelor.

Transformarea digitală a procedurilor administrative și manipularea informațiilor confidențiale sunt elemente cruciale în modernizarea organizațiilor și a instituțiilor publice către o administrație mai contemporană și mai eficientă. Implementarea acestor proceduri digitale aduce o serie de avantaje, precum sporirea eficienței, diminuarea birocrației, facilitarea accesului cetățenilor la serviciile publice și optimizarea gestionării resurselor disponibile. Cu toate acestea, sunt prezente și dificultăți majore, cum ar fi protecția informațiilor sensibile, garantarea securității cibernetice și conformitatea cu standardele și legile referitoare la confidențialitatea și protecția datelor[21].

Consider că digitalizarea procedurilor administrative și gestionarea informațiilor confidențiale reprezintă aspecte fundamentale în procesul de modernizare al organizațiilor și instituțiilor publice, în vederea obținerii unei administrații mai actuale și mai eficiente.

Este crucial ca instituțiile să implementeze strategii corespunzătoare pentru a aborda aceste probleme și pentru a câștiga încrederea în privința utilizării și manipulării datelor cu caracter sensibil în sfera digitală. Prin aplicarea unor politici și proceduri responsabile, adoptarea digitalizării în procesele administrative poate conduce la o îmbunătățire a calității serviciilor publice și la o mai mare satisfacție a cetățenilor, în timp ce promovează transparența și responsabilitatea în guvernare. [24]

Prin urmare, beneficiile acestui program includ reducerea timpului. Astfel, se observă că administrația publică din România continuă să depună eforturi pentru digitalizarea și modernizarea sistemului. Guvernul României joacă un rol important în acest proces prin programe și parteneriate cu organizații specializate în domeniul IT, iar administrațiile publice locale se implică prin proiecte, platforme și aplicații menite să faciliteze atât cetățenii, cât și funcționarii publici în realizarea unei bune guvernări și comunicări eficiente.

Într-o altă direcție, mediul de afaceri are o importanță extrem de semnificativă în evoluția administrației publice din România. Astfel, numeroase organizații din domeniul IT dezvoltă noi concepte, platforme și aplicații care pot fi utilizate de către administrație pentru a reduce decalajul în ceea ce privește modernizarea sistemului administrativ. Un aspect crucial în relația dintre Guvern și mediul de afaceri constă în parteneriatele solide și comunicarea eficientă, în vederea adoptării și implementării celor mai noi tehnologii disponibile pe piața IT[17].

În final, cetățenii pot aduce numeroase beneficii și inovații importante. Este crucial ca aceștia să fie educați și informați și să învețe să utilizeze tehnologiile moderne, cum ar fi telefoanele, tabletele și calculatoarele, și să acceseze site-urile online pentru a avea o bună înțelegere a acestora. Cetățenii pot exercita presiune asupra autorităților pentru a utiliza licitațiile publice online, astfel creând o transparență mai mare. Implicarea cetățenilor prin intermediul organizațiilor non-guvernamentale este o practică obișnuită în occident și este adoptată și în România, cu exemple precum OpenBudget, Geeks for Democracy, Code of Romania sau Civic Tech.

În opinia mea, digitalizarea administrației publice este esențială pentru progresul și modernizarea României. Așa cum am menționat anterior, atât autoritățile, cât și cetățenii trebuie să depună eforturi considerabile pentru a dezvolta aplicații, platforme, site-uri și alte tehnologii similare. Deși este un domeniu crucial pentru progresul administrației publice, România se confruntă în continuare cu deficiențe semnificative în implementarea și conceperea digitalizării, conform rapoartelor Uniunii Europene care ne plasează pe ultimele locuri la utilizarea internetului în administrație și la adoptarea tehnologiilor moderne. Soluția la această problemă vine de la organizațiile non-guvernamentale, presiunile exercitate de Uniunea Europeană și o implicare mai mare a Guvernului în acest aspect esențial pentru o dezvoltare durabilă, sănătoasă și pentru îndeplinirea nevoilor publice prin cele mai bune practici de digitalizare.

2.3. *Mijloace pentru Protecția Datelor în Administrația Publică Digitalizată Gestionarea riscurilor cibernetice în mediul digitalizat*

Securitatea datelor în cadrul administrației publice este o chestiune deosebit de importantă în epoca digitală, în care o cantitate considerabilă de informații este adunată, reținută și procesată în context administrativ.Este crucial să dispunem de instrumente eficiente pentru a proteja datele, garantând că informațiile sensibile ale cetățenilor și instituțiilor sunt în siguranță, protejate împotriva accesului neautorizat, a pierderii sau a furtului. Mai jos este o expunere detaliată a instrumentelor folosite pentru protejarea datelor în administrația publică [22]:

1. Politici și proceduri:

Crearea și aplicarea unor politici și proceduri bine definite pentru administrarea datelor sunt esențiale. Aceste politici ar trebui să includă norme și instrucțiuni referitoare la confidențialitatea, securitatea și protecția datelor. Politica ar trebui să clarifice procesele de colectare, stocare, prelucrare și distribuire a datelor sensibile, precum și modalitățile de reacție în cazul incidentelor de securitate.

2. Criptare:

Implementarea criptării este crucială pentru securizarea datelor sensibile în timpul tranzacționării și păstrării acestora. Criptarea garantează că informațiile sunt convertite într-un format ilegibil pentru cei neautorizați, până când sunt decodate utilizând o cheie de decriptare adecvată.

3. Autentificare și autorizare:

Stabilirea unor sisteme robuste de verificare a identității și a permisiunilor este esențială pentru a gestiona accesul la informațiile sensibile. Aceste proceduri pot implica autentificare dublă,

utilizarea de parole complexe, administrarea permisiunilor de acces și autentificare în funcție de roluri.

4. Soluții de securitate cibernetică:

Este crucial să se utilizeze instrumente specializate de securitate cibernetică, cum ar fi firewall-uri, programe antivirus, sisteme de detectare a intruziunilor și soluții de gestionare a vulnerabilităților, pentru a proteja rețelele și sistemele împotriva atacurilor cibernetice.

5. Formare și conștientizare:

Este fundamental să se ofere o formare corespunzătoare a personalului în ceea ce privește securitatea datelor și să se promoveze o cultură a securității informațiilor. Angajații ar trebui să fie conștienți de riscurile de securitate și de practicile recomandate pentru protejarea informațiilor sensibile.

6. Monitorizare și auditare:

Este crucial să se implementeze sisteme de monitorizare și auditare pentru a supraveghea activitățile legate de date și pentru a identifica comportamente suspecte sau anomalii care ar putea semnala o posibilă încălcare a securității.

7. Conformitate legală:

Este esențial să se respecte legislația și regulamentele aplicabile în domeniul protecției datelor. Acest lucru implică conformarea cu Regulamentul General privind Protecția Datelor (GDPR) în Uniunea Europeană și cu alte legi naționale referitoare la confidențialitatea și securitatea datelor. Prin aplicarea acestor metode, administrațiile publice pot gestiona riscurile de securitate cibernetică într-un mod mai eficient și pot consolida încrederea în utilizarea și manipularea datelor sensibile.

Administrațiile locale se angajează în fața unor dificultăți și amenințări în procesul de implementare a strategiilor de digitalizare, influențate de o serie de factori, fie interni, fie externi. Maniera în care interacționează cu beneficiarii serviciilor publice, evoluția tehnologică din piață și gradul de urbanizare al comunității sunt elemente cruciale care pot susține sau dimpotrivă, pot compromite eforturile de digitalizare. Toate aceste aspecte trebuie analizate într-un cadru mai amplu, în care orașele se confruntă cu diverse provocări legate de demografie, schimbările climatice, accesul la serviciile publice, îmbunătățirea mobilității urbane și menținerea calității mediului înconjurător [23].

Mărirea complexității vieții comunităților, cererea crescută de servicii publice de calitate superioară, atât din punct de vedere cantitativ, cât și calitativ, au transformat localitățile în entități dinamice, în care tehnologia a devenit elementul de legătură esențial și punctul comun al tuturor activităților desfășurate și al comunicației dintre administrație și părțile interesate. Aceste aspecte constituie limite ce trebuie luate în considerare în procesul de implementare a strategiei. Infrastructura urbană nu se mai limitează doar la rețeaua de drumuri și utilități, ci include și infrastructura de comunicații, având o importanță similară pentru comunitate. [21]

După părerea mea, scopul principal al strategiei de digitalizare este să reducă sau să elimine ineficiența administrativă în furnizarea serviciilor către cetățeni, susținând în același timp o transformare continuă și durabilă. Generarea de valoare pentru toți cei implicați prin digitalizare este un obiectiv cheie al strategiei și un criteriu pentru evaluarea succesului acesteia. Pentru a asigura succesul, strategia de digitalizare trebuie să fie încorporată în strategia globală de dezvoltare a orașului sau cel puțin să fie strâns legată de aceasta.

Spiritul inovator și capacitatea de a inova demonstrată de liderii autorității publice locale pot facilita integrarea unor concepte tehnologice avansate în strategie, contribuind la formularea unei viziuni pe termen lung pentru comunitate, în care conceptul de oraș inteligent să se combine armonios cu principiile dezvoltării durabile. Cerințele individuale ale cetățenilor, în special în ceea ce privește mobilitatea și accesul rapid la informații, sunt fundamentale în formularea și implementarea strategiei de digitalizare. [22]

În opinia mea, scăderea riscurilor în procesul de implementare poate fi realizată prin crearea unui cadru favorabil care să susțină și să faciliteze adoptarea extensivă a tehnologiilor inteligente. Transformarea completă digitală a serviciilor publice poate fi un proces complex și de lungă durată. Implementarea digitalizării în etape și obținerea de succese parțiale pot încuraja

angajații să continue eforturile. În plus, simplificarea formularelor online și furnizarea de asistență pentru navigarea pe site-ul primăriei și utilizarea platformei poate stimula și utilizatorii.

Dezvoltarea unei culturi organizaționale orientate către transformarea digitală poate fi atât o provocare, cât și o soluție. Un leadership puternic și abilitatea de a motiva personalul pot contribui la formarea unei culturi organizaționale solide în cadrul instituției publice, favorabilă adoptării tehnologiei digitale. Organizațiile cu o structură solidă sunt capabile să conducă și să îndrume schimbarea. În schimb, în organizațiile mai slabe, angajații mai puțin motivați pot încetini procesul de transformare. Reticența față de schimbare, teama de a adopta noi tehnologii și lipsa încrederii în propriile competențe digitale reprezintă obstacole care trebuie să fie gestionate corespunzător de către cei care iau decizii [13].

Consider că personalul din sectorul public are obiceiul să urmeze proceduri și regulamente birocratice, care sunt concepute pentru a minimiza riscurile decizionale și de flux informațional. Cu toate acestea, această abordare nu este potrivită pentru furnizarea acelorași servicii prin intermediul canalelor digitale. Interacțiunile dintre angajați și între departamente devin mai puțin formale în ceea ce privește furnizarea serviciilor digitale, ceea ce duce la accelerarea fluxurilor de lucru. Schimbarea mentalității angajaților și ajustarea procedurilor de lucru pot fi soluții în acest sens.

Calificarea inadecvată a personalului și lipsa unei înțelegeri complete a tendințelor în domeniul tehnologiei informației și comunicațiilor (ITC) afectează negativ implementarea eficientă a strategiei. În plus, recrutarea angajaților cu abilități digitale avansate reprezintă o altă provocare pentru sectorul public. De obicei, programatorii talentați preferă sectorul privat, ceea ce face ca recrutarea de personal calificat în domeniul tehnologiei informației și comunicațiilor să fie o provocare pentru administrația locală [24].

Angajamentul public asumat pentru promovarea digitalizării în administrație reprezintă o provocare semnificativă, dar marchează totodată începutul unui proces ireversibil, caracterizat de schimbări profunde. Investiția în echipamente IT, aplicații și programe software, precum și în formarea personalului APL pentru îmbunătățirea competențelor digitale nu sunt de un real ajutor pentru garantarea succesului strategiei. Este necesară o transformare a mentalității atât în rândul personalului administrației publice, cât și al beneficiarilor serviciilor publice, care vor impune o presiune continuă pentru adoptarea schimbării digitale de către autorități [23].

După părerea mea, este crucial să gestionăm în mod adecvat problema canalelor tradiționale de furnizare a serviciilor publice. Este esențial să menținem operațiunile curente ale administrației pe durata implementării noilor soluții tehnologice. Nuse poate renunța brusc la aceste canale tradiționale, iar menținerea lor în paralel cu introducerea canalelor digitale generează preocupări legate de costuri suplimentare și de o posibilă supraîncărcare a personalului. Există riscul real de încetinire a proceselor și a operațiunilor. O soluție de compromis ar putea fi implementarea unei combinații între cele două tipuri de canale pentru o perioadă de tranziție.

Comunitatea așteaptă ca strategia de digitalizare să faciliteze interacțiunile și să conducă la reducerea costurilor serviciilor, ceea ce ar putea, în final, să se traducă în taxe mai mici sau într-o creștere a investițiilor în comunitate. Din perspectiva administrației, evaluarea eficienței strategiei în termeni financiari prezintă dificultăți. Unele beneficii sunt de natură calitativă și nu pot fi cuantificate, în timp ce costurile trebuie analizate în contextul întregii structuri organizaționale și a interdependențelor lor. Prin urmare, economiile de costuri înregistrate în anumite sectoare sau ca urmare a digitalizării unor servicii ar putea fi realocate către alte sectoare, unde costurile pot fi mai mari[27].

Între administrație și stakeholderii implicați există întotdeauna o discrepanță în ceea ce privește informațiile disponibile. Nivelul lor de înțelegere a funcționării platformei, a proceselor digitalizate și a tehnologiilor folosite poate varia, ceea ce înseamnă că nevoile lor de informare și suport sunt diferite. Instrucțiunile pentru accesarea și folosirea platformei informatice pot fi

uneori exprimate într-un limbaj tehnic, dificil de înțeles pentru utilizatori. Completarea formularelor online poate fi la fel de dificilă ca și completarea celor tipărite. De asemenea, crearea și păstrarea credențialelor de acces pe platformă pot reprezenta o provocare pentru utilizatori [21].

Mulți utilizatori sunt familiarizați deja cu navigarea pe site-urile organizațiilor private, ceea ce își reflectă așteptările în ceea ce privește experiența lor și utilizarea unei interfețe de platformă cât mai similară cu aceasta. Prin urmare, accesarea serviciilor publice în mediul digital trebuie să ofere o experiență apropiată de ceea ce experimentează atunci când fac achiziții online de bunuri și servicii. Măsurile de implementare a strategiei ar trebui să vizeze și îmbunătățirea abilităților digitale ale grupurilor vulnerabile. Există un risc crescut de a adânci decalajul digital pentru populația cu venituri mai reduse. [17]

Consider că este deosebit de important ca serviciile publice oferite în mediul digital să se adapteze la așteptările utilizatorilor, astfel încât aceștia să aibă o experiență similară cu cea pe care o au în interacțiunea cu site-urile organizațiilor private. Având în vedere că mulți utilizatori sunt familiarizați cu navigarea online și au dezvoltat anumite așteptări în ceea ce privește utilizarea platformelor digitale, este esențial ca serviciile publice să răspundă acestor așteptări și să ofere o interfață intuitivă și ușor de utilizat.

Actorii vulnerabili ar trebui să fie implicați activ în procesul de digitalizare, în ciuda resurselor limitate pentru conectare digitală. Acest sprijin logistic, financiar sau de consultanță ar trebui să fie disponibil pentru ei. Accesul lor la serviciile digitale ar trebui să fie la latitudinea lor, permițându-le să progreseze în ritmul lor. Implementarea pe o scară mai largă a strategiei și dezvoltarea unor noi instrumente digitale vor implica inevitabil crearea de baze de date, care necesită protecție. Securitatea cibernetică a informațiilor colectate va necesita o pregătire adecvată a personalului pentru a aplica protocoalele de securitate și pentru a înțelege ce date trebuie păstrate confidențiale și care pot fi făcute publice. [22]Este important să se protejeze viața privată a cetățenilor, iar publicul trebuie să aibă încredere că datele personale sunt colectate, stocate și procesate în siguranță.

2.4. Perspective Viitoare și Inovații în digitalizarea proceselor de securitate

În decursul ultimelor decenii, digitalizarea proceselor a devenit un factor esențial ce a modificat esențial modalitatea în care organizațiile își desfășoară operațiunile și interacționează cu datele și informațiile. Această trecere rapidă către mediul digital a adus cu sine avantaje semnificative, dar și provocări considerabile în domeniul securității cibernetice. Într-o societate din ce în ce mai interconectată și cu o dependență crescândă de tehnologie, asigurarea securității datelor și a infrastructurii devine o preocupare esențială pentru organizații din diverse domenii[22].

Perspectivele în viitor și noile abordări în digitalizarea proceselor de securitate reprezintă un angajament constant pentru a gestiona provocările și oportunitățile generate de progresul rapid al mediului digital. Acest lucru presupune adoptarea de abordări noi și creative în gestionarea riscurilor, identificarea și evitarea amenințărilor cibernetice, și asigurarea respectării cerințelor legate de protecția datelor. În acest document, ne vom concentra asupra diferitelor aspecte ale perspectivei viitoare și a inovațiilor în procesele de securitate digitală. Vom analiza tendințele noi și emergente în domeniul securității cibernetice, precum și tehnologiile și practicile recente care afectează modul în care organizațiile gestionează securitatea în contextul digital [25].

De asemenea, voi examina atât potențialele riscuri, cât și beneficiile legate de aceste inovații și vom cerceta strategiile prin care organizațiile pot să-și dezvolte capacitățile de securitate și să-și securizeze resursele digitale în fața amenințărilor cibernetice în perpetuă transformare. Prin asimilarea și aplicarea unor strategii inovatoare în ceea ce privește securitatea cibernetică, organizațiile pot să valorifice pe deplin avantajele oferite de procesele de digitalizare, în timp ce garantează protecția și confidențialitatea datelor lor sensibile.

Inteligența Artificială în Securitate:

Utilizarea Inteligenței Artificiale în domeniul securității poate fi un subiect de discuție relevant, în care se poate explora modul în care algoritmii de învățare automată și deep learning sunt folosiți pentru identificarea modelelor și a anomaliilor în datele de securitate, precum și pentru automatizarea proceselor de detectare a amenințărilor și de gestionare a incidentelor. Beneficiile aduse de utilizarea IA în sfera securității pot fi semnificative în identificarea și contracararea amenințărilor, în analiza comportamentului utilizatorilor și a modelelor de trafic, precum și în îmbunătățirea eficienței operaționale. Iată câteva aspecte esențiale referitoare la impactul pe care îl poate avea în evoluția viitoare a securității[29]:

- Detectarea și Prevenirea Amenințărilor
- Tehnicile de învățare automată și deep learning pot fi aplicate pentru analizarea datelor extinse de securitate în timp real, identificând modele și semnale care pot indica activități suspecte sau posibile amenințări cibernetice.
- Identificarea și prevenirea amenințărilor
- Tehnicile de învățare automată și deep learning pot fi aplicate pentru analizarea datelor extinse de securitate în timp real, identificând modele și semnale care pot indica activități suspecte sau posibile amenințări cibernetice.Această abilitate de detectare avansată poate contribui la prevenirea atacurilor și la diminuarea intervalului de timp necesar pentru identificarea și gestionarea incidentelor.
- Răspuns automat la incidente
- Sistemele de securitate care se bazează pe inteligența artificială pot fi configurate pentru a reacționa automat la amenințări, inclusiv pentru a bloca sau izola dispozitivele compromițate sau pentru a iniția corecții în timp real. Această abordare poate reduce considerabil timpul necesar pentru reacție și poate limita impactul unui atac cibernetic.
- Analiza comportamentului utilizatorilor
- Inteligența artificială poate fi utilizată pentru a examina modelele de utilizare și acces la resursele digitale, în scopul de a detecta comportamente neobișnuite sau potențial periculoase. De exemplu, algoritmii pot identifica utilizatori care accesează sisteme sau date sensibile în afara programului de lucru obișnuit sau care încearcă să acceseze resurse pentru care nu au autorizație.
- Optimizarea securității rețelelor
- Inteligența artificială poate juca un rol crucial în îmbunătățirea arhitecturilor de securitate și în descoperirea vulnerabilităților în infrastructurile IT și în rețelele de comunicații. Aceasta poate implica identificarea și remedierea automată a configurațiilor de securitate slabe sau depășite, precum și adaptarea politicilor de securitate în funcție de modificările survenite în mediul digital.
- Analiza și identificarea amenințărilor emergente
- Prin utilizarea inteligenței artificiale, este posibilă efectuarea unei analize rapide și precise a noilor tipuri de amenințări și a tacticii folosite de atacatori. Algoritmii pot detecta semnale și anomalii care sugerează activități neobișnuite și pot contribui la elaborarea de soluții și strategii de apărare flexibile.
- Îmbunătățirea eficienței operaționale
- Utilizarea inteligenței artificiale în procesele de securitate poate diminua sarcinile repetitive și manuale ale angajaților din domeniul securității, oferindu-le oportunitatea de a se axa pe activități de analiză și răspuns la amenințări mai sofisticate și mai strategice.
- Pe scurt, introducerea inteligenței artificiale în sectorul securității este un element esențial al perspectivei viitoare și a inovațiilor în procesele digitale de securitate, furnizând capacitatea de a îmbunătăți detectarea, prevenirea și gestionarea amenințărilor cibernetice într-un mod mai eficient și mai adaptabil.

Blockchain și Securitatea Cibernetică:
Blockchain și securitatea cibernetică pot fi analizate în sensul în care tehnologia blockchain poate fi aplicată pentru a garanta integritatea și confidențialitatea datelor într-un mediu digital, inclusiv prin asigurarea securității stocării datelor de autentificare și a altor informații sensibile.
Integrarea tehnologiei blockchain în sfera securității cibernetice reprezintă un aspect crucial în ceea ce privește perspectivele viitoare și inovațiile în digitalizarea proceselor de securitate.

[23]Caracteristicile de securitate și transparență ale tehnologiei blockchain pot contribui la consolidarea securității datelor și a infrastructurilor IT într-un mediu digital tot mai complex și interconectat.

Consider că tehnologia blockchain prezintă un potențial semnificativ în asigurarea securității cibernetice și a confidențialității datelor în mediul digital. Integrarea blockchain în sfera securității cibernetice reprezintă o perspectivă inovatoare și promițătoare în procesul de digitalizare a proceselor de securitate. Iată câteva modalități în care tehnologia blockchain poate influența evoluția securității cibernetice în viitor[23]:

- Stocarea sigură a datelor
- Tehnologia blockchain utilizează criptografia și distribuirea descentralizată pentru a garanta integritatea și confidențialitatea datelor. Prin stocarea datelor în blocuri criptografice și distribuirea lor pe întreaga rețea, blockchain-ul poate furniza o soluție securizată și imună la modificări pentru administrarea și protejarea datelor sensibile.
- Autentificarea și autorizarea
- Tehnologia blockchain poate fi aplicată pentru a dezvolta sisteme de autentificare și autorizare mai fiabile și mai transparente. Prin implementarea identității digitale pe baza blockchain-ului, utilizatorii pot avea gestionare directă a datelor personale și a accesului la resursele digitale, diminuând riscul de fraude și de acces neautorizat.
- Gestionarea identității digitale
- Blockchain-ul poate acționa ca o infrastructură pentru administrarea identității digitale într-un mod securizat și confidențial. Prin utilizarea tehnologiilor de criptare și distribuire descentralizată, blockchain-ul poate furniza un cadru solid pentru autentificarea și verificarea identității digitale fără a fi nevoie de intermediari centralizați.
- Urmărirea și auditarea tranzacțiilor
- Abilitatea blockchain-ului de a înregistra și valida tranzacțiile într-un mod imutabil și transparent poate fi utilizată pentru a garanta integritatea și verificabilitatea acestora. Această caracteristică poate fi de ajutor în monitorizarea și auditarea accesului la resursele digitale și a schimburilor de date între diferite părți. Aplicațiile descentralizate care funcționează pe platforme blockchain se pot bucura de avantajele de securitate încorporate ale tehnologiei blockchain, cum ar fi imutabilitatea datelor și distribuirea descentralizată. Aceste caracteristici pot ajuta la minimizarea riscului de atacuri cibernetice și la garantarea securității și integrității aplicațiilor descentralizate.

Internetul Lucrurilor (IoT) și Securitatea Dispozitivelor Conectate:
Se pot analiza dificultățile și opțiunile referitoare la securitatea dispozitivelor Internet of Things (IoT), în plus, se poate discuta despre modul în care standardele și protocoalele de securitate se dezvoltă pentru a asigura protecția rețelelor și a datelor împotriva amenințărilor cibernetice.
Încorporarea Internetului Lucrurilor (IoT) în contextul securității cibernetice reprezintă un proces cu provocări semnificative și necesită dezvoltări constante pentru a garanta protecția dispozitivelor conectate și a rețelelor în care acestea funcționează. În contextul perspectivei viitoare și al inovațiilor în digitalizarea proceselor de securitate, se acordă o atenție deosebită securității dispozitivelor IoT. Iată câteva puncte esențiale [25]:

- Identificarea și autentificarea dispozitivelor
- Dispozitivele IoT sunt adesea caracterizate de resurse limitate și pot fi susceptibile la atacuri de tip spoofing, în care un intrus încearcă să își mascheze identitatea pentru a accesa rețeaua sau alte dispozitive în mod neautorizat. Crearea unor tehnici solide de identificare și autentificare a dispozitivelor IoT, inclusiv prin utilizarea certificatelor digitale și a protocoalelor de autentificare avansate, este o inovație esențială pentru securitatea dispozitivelor conectate.
- Criptarea comunicațiilor
- Informațiile transmise între dispozitivele IoT și serverele de gestionare trebuie să fie securizate împotriva interceptării și modificării. Utilizarea criptografiei robuste pentru criptarea comunicațiilor dintre dispozitivele IoT și servere, și pentru autentificarea și

autorizarea datelor, este crucială pentru a garanta confidențialitatea și integritatea informațiilor.

- Monitorizarea și detecția amenințărilor
- Implementarea unor soluții de monitorizare și detecție a amenințărilor pentru dispozitivele IoT poate contribui la identificarea și gestionarea atacurilor în timp real. Astfel de soluții pot cuprinde aplicarea tehnologiilor de analiză comportamentală, detectare a anomaliilor și învățare automată pentru identificarea schemelor de activitate suspecte și pentru declanșarea măsurilor corective adecvate.
- Actualizări de securitate și managementul ciclului de viață al dispozitivelor:
- O componentă esențială a securității IoT constă în garantarea că dispozitivele beneficiază întotdeauna de cele mai recente actualizări de securitate și sunt administrate adecvat pe întreaga durată a ciclului lor de viață. Progresele în domeniul gestionării actualizărilor de securitate și al managementului dispozitivelor pot contribui la diminuarea riscului de exploatare a vulnerabilităților cunoscute.
- Segmentarea rețelelor și izolarea dispozitivelor vulnerabile
- Separarea rețelelor și izolarea dispozitivelor IoT vulnerabile în rețele distincte sau în segmente de rețea dedicate poate contribui la reducerea impactului în cazul compromiterii unui dispozitiv și la împiedicarea propagării potențialelor amenințări în întreaga infrastructură. În ansamblu, progresul în securitatea dispozitivelor IoT este fundamental pentru a gestiona riscurile și amenințările în evoluție din mediul conectat. Un angajament proactiv și constant, împreună cu investiții în cercetare și dezvoltare, sunt esențiale pentru a menține securitatea și integritatea ecosistemului IoT în era digitală viitoare.

Analiza Big Data în Securitate:
Încorporarea analizei Big Data în sfera securității cibernetice este un aspect esențial în contextul perspectivei viitoare și al inovațiilor în digitalizarea proceselor de securitate. Conceptul de Big Data se referă la volumul masiv de date care pot fi adunate, stocate și examinate pentru a identifica modele, trenduri și anomalii semnificative. Utilizată în domeniul securității cibernetice, analiza Big Data poate furniza o înțelegere amplă a amenințărilor și vulnerabilităților, facilitând astfel adoptarea unor măsuri preventive și reactivă într-un mod mai eficient și mai proactiv.

Consider că este extrem de important să integrăm analiza Big Data în domeniul securității cibernetice, deoarece acest lucru poate aduce beneficii semnificative și poate deschide perspective viitoare în digitalizarea proceselor de securitate. Integrarea analizei Big Data în sfera securității cibernetice poate contribui la o gestionare mai eficientă a amenințărilor și la o protecție mai puternică a sistemelor și datelor într-o eră digitală în continuă evoluție.Iată câteva exemple ale modului în care analiza Big Data poate influența evoluția securității cibernetice în viitor[23]:

- Detectarea și prevenirea amenințărilor
- Prin analiza Big Data, este posibil să se supravegheze și să se evalueze în timp real activitățile din rețea, identificând tipare și semnale care indică posibile amenințări cibernetice. Utilizând algoritmi sofisticați de analiză a datelor, este posibil să se detecteze și să se prevină atacurile cibernetice înainte ca acestea să cauzeze pagube semnificative.
- Analiza comportamentului utilizatorilor
- Prin intermediul Big Data, este posibil să se examineze modelele de comportament ale utilizatorilor și să se identifice activități neobișnuite sau suspecte care ar putea sugera o compromitere a contului sau a dispozitivului.Prin supravegherea și analizarea interacțiunilor utilizatorilor cu sistemele și rețelele, este posibil să se identifice amenințări potențiale atât din interior, cât și din exterior.
- Gestionarea și analiza logurilor de securitate
- Prin analiza Big Data, este posibil să se ușureze analiza și gestionarea eficientă a volumelor masive de jurnale de securitate generate de dispozitivele și aplicațiile din rețea. Identificând și interpretând evenimentele semnificative din jurnale, este posibil să se identifice potențiale amenințări și să se răspundă rapid la incidentele de securitate.

- Modelarea și proiectarea de securitate
- Prin utilizarea analizei Big Data, este posibil să se modeleze și să se simuleze scenarii de securitate pentru a evalua eficacitatea strategiilor de apărare și pentru a identifica posibile puncte slabe sau vulnerabilități în infrastructura de securitate. Aceasta poate ajuta la îmbunătățirea planificării și implementării strategiilor de securitate cibernetică.
- Anticiparea și prevenirea amenințărilor viitoare
- Prin examinarea Big Data pentru a identifica tendințe și modele de atac, este posibil să se prevadă și să se prevină potențiale amenințări cibernetice în viitor. Identificarea și evaluarea amenințărilor emergente pot ajuta organizațiile să adopte măsuri proactive pentru a-și proteja infrastructura și datele împotriva atacurilor iminente. În final, integrarea analizei Big Data în securitatea cibernetică reprezintă oportunități considerabile pentru a îmbunătăți detecția, prevenirea și răspunsul la amenințările cibernetice. Folosirea în mod eficient a volumelor mari de date poate spori eficiența și eficacitatea operațiunilor de securitate, oferind organizațiilor posibilitatea de a gestiona riscurile și vulnerabilitățile din mediul digital într-un mod mai eficient, având în vedere caracterul în continuă schimbare al acestuia.

Inovații în Autentificare și Autorizare:
Se pot explora noi tehnici de autentificare și autorizare, inclusiv autentificarea bazată pe biometrie, autentificarea multifactorială și tehnologiile de autentificare fără parole, și modul în care acestea pot aduce îmbunătățiri în securitatea mediului digital. În contextul perspectivei viitoare și al inovațiilor în digitalizarea proceselor de securitate, progresul în autentificare și autorizare este crucial pentru a menține securitatea într-un mediu digital în perpetuă schimbare. Autentificarea și autorizarea sunt două elemente esențiale ale securității cibernetice, având rolul de a verifica identitatea utilizatorilor și de a gestiona accesul adecvat la resursele și datele sensibile. [29]

Consider că este extrem de important să explorăm și să implementăm noi tehnici de autentificare și autorizare pentru a asigura securitatea mediului digital. Tehnologii avansate, precum autentificarea bazată pe biometrie, autentificarea multifactorială și autentificarea fără parole, pot aduce îmbunătățiri semnificative în domeniul securității cibernetice.Mai jos sunt prezentate câteva inovații semnificative în acest domeniu[23]:

- Autentificare bazată pe biometrie
- Aplicarea trăsăturilor biometrice distinctive ale utilizatorilor, cum ar fi amprentele digitale, scanările faciale sau recunoașterea vocii, înlocuiește tehnicile tradiționale de autentificare bazate pe parole. Aceasta furnizează un nivel crescut de securitate și confort, eliminând riscul utilizării sau compromiterii parolelor. Autentificarea multifactorială (MFA) presupune folosirea a cel puțin două sau mai multe modalități de autentificare pentru a valida identitatea utilizatorului. Aceste modalități pot cuprinde informații pe care utilizatorul le cunoaște (parola), dispozitive pe care le deține (tokenuri de securitate) și caracteristici biometrice.Utilizarea MFA sporește semnificativ nivelul de securitate, diminuând riscul de acces neautorizat, chiar și atunci când o metodă de autentificare este compromisă.
- Autentificare fără parole
- Tehnologii recente, precum autentificarea prin token-uri sau certificate digitale, elimină necesitatea folosirii parolelor și a riscurilor asociate acestora, cum ar fi expunerea la atacuri de tip phishing sau brute-force. Aceste soluții furnizează o alternativă mai sigură și mai comodă pentru autentificare.
- Autentificare adaptivă
- Autentificarea adaptivă se bazează pe utilizarea inteligenței artificiale și analiza comportamentului utilizatorilor pentru a evalua riscul și a aplica niveluri de securitate variabile, în funcție de contextul autentificării. Aceasta poate implica impunerea unor cerințe suplimentare de autentificare în situații neobișnuite sau atunci când se utilizează dispozitive necunoscute.
- Blockchain în autentificare

- Implementarea tehnologiei blockchain în procesul de autentificare poate oferi o înregistrare distribuită și imutabilă a identității digitale, oferind utilizatorilor posibilitatea de a-și gestiona și controla datele de identitate într-un mod sigur și confidențial.
- Autorizare bazată pe politici și roluri
- Sistemele de autorizare bazate pe politici și roluri sunt responsabile de definirea și gestionarea accesului utilizatorilor la resursele digitale, luând în considerare permisiunile și rolurile alocate acestora. Înnoirile în acest sector includ introducerea politiciilor fine-grained și adapabile, împreună cu utilizarea tehnologiilor de securitate bazate pe blockchain pentru a garanta integritatea și confidențialitatea politicilor de autorizare. Aceste progrese în autentificare și autorizare aduc îmbunătățiri în securitatea digitală și în capacitatea sistemelor de securitate de a se adapta la amenințările cibernetice în evoluție.Prin incorporarea și utilizarea acestor tehnologii în strategiile lor de securitate, organizațiile pot întări securitatea datelor și a infrastructurii lor în peisajul digital în continuă schimbare de astăzi și de mâine [25].

Evoluția Tehnologiilor de Criptare:
Se poate investiga modul în care algoritmii de criptare se dezvoltă pentru a aborda noile amenințări cibernetice și pentru a menține confidențialitatea datelor într-un mediu digital în creștere în complexitate și interconectivitate. Progresul tehnologiilor de criptare este esențial pentru protejarea securității datelor și a comunicațiilor în contextul perspectivelor viitoare și a inovațiilor în digitalizarea proceselor de securitate. Criptografia constituie un element fundamental al securității cibernetice, având rolul de a proteja împotriva accesului neautorizat și de a garanta confidențialitatea și integritatea datelor. Urmează câteva elemente cheie ale progresului tehnologiilor de criptare și a direcțiilor viitoare în acest domeniu[23]:

- Criptarea omomorfică
- Criptografia omomorfică reprezintă capacitatea de a efectua operații matematice asupra datelor criptate, fără a fi necesară decriptarea acestora. Această inovație are potențialul de a fi utilizată în diverse domenii, inclusiv în prelucrarea datelor sensibile în cadrul cloud computing, reprezentând o soluție robustă pentru protecția datelor și păstrarea confidențialității informațiilor.
- Criptarea cu cheie multiplă
- Criptografia cu cheie multiplă implică utilizarea mai multor chei de criptare pentru a adăuga un strat suplimentar de securitate. Această abordare poate include criptarea hibridă, care combină tehnicile simetrice și asimetrice, sau criptarea în straturi multiple, care utilizează mai multe niveluri de criptare pentru a proteja datele împotriva atacurilor sofisticate.
- Criptarea bazată pe blockchain
- Utilizarea tehnologiei blockchain poate garanta securitatea și integritatea datelor prin intermediul protocolului și algoritmilor criptografici. Integrarea criptografiei în blockchain aduce un nivel adițional de securitate pentru tranzacțiile și informațiile stocate pe blockchain.
- Criptografia cu consum redus de energie
- În cadrul Internetului Lucrurilor (IoT), este crucială dezvoltarea de tehnologii de criptare care să fie eficiente energetic și care să poată fi implementate pe dispozitivele cu resurse limitate. Criptografia cu consum redus de energie poate asigura securitatea dispozitivelor IoT și a comunicațiilor acestora fără a afecta performanța sau autonomia bateriei. În final, progresul în tehnologiile de criptare aduce o serie de inovații și perspective promițătoare pentru securitatea cibernetică viitoare. Prin implementarea și integrarea acestor tehnologii în operațiunile lor de securitate, organizațiile pot întări protecția datelor și a infrastructurilor lor împotriva amenințărilor cibernetice în evoluție constantă.

Tendințe în Securitatea Cloud:
Această temă ar putea explora modul în care serviciile și soluțiile de securitate în cloud se dezvoltă pentru a asigura protecția datelor și a aplicațiilor într-un mediu de calcul distribuit și

virtualizat. În lumina progresului viitorului și a inovațiilor în digitalizarea proceselor de securitate, securitatea în cloud capătă o importanță crescândă, odată cu migrația tot mai extinsă a organizațiilor către infrastructuri cloud pentru gestionarea și procesarea datelor lor. Transformările în securitatea cloud-ului reflectă interesele și cerințele organizațiilor în gestionarea amenințărilor și în garantarea securității datelor lor sensibile în spațiul digital. Iată câteva dintre aceste evoluții [23]:

- Securitatea bazată pe zero trust (Zero Trust Security)
- Idea de securitate de tip „zero trust" implică faptul că niciun utilizator sau dispozitiv nu este presupus a fi de încredere automat, chiar și atunci când acestea se află în interiorul rețelei interne.În mediul cloud, aceasta implică necesitatea ca accesul la resursele cloud să fie acordat și verificat în mod regulat, în conformitate cu politici de securitate strict monitorizate.
- Protecția datelor în mișcare
- Pe măsură ce datele sunt transferate între dispozitive și centrele de date, securitatea trebuie să fie asigurată pe întreaga lor traiectorie. Criptarea de la un capăt la altul, administrarea centralizată a cheilor și monitorizarea continuă a traficului sunt vitale pentru a proteja integritatea datelor în tranzit.
- Securitatea multicloud
- Multe companii utilizează o mixtură de servicii cloud de la mai mulți furnizori, ceea ce impune necesitatea unei abordări coezive și integrate în ceea ce privește securitatea. În acest sens, instrumentele și platformele de securitate care sunt interoperabile și pot funcționa cu diferite medii cloud devin din ce în ce mai cruciale.
- Automatizarea și orchestarea securității
- În fața creșterii amenințărilor cibernetice, automatizarea și orchestrarea proceselor de securitate devin vitale pentru detectarea și gestionarea incidentelor în timp real. Implementarea acestor tehnologii poate diminua timpul necesar pentru a răspunde la amenințări și poate optimiza eficiența operațională a echipelor de securitate.
- Analiza comportamentală și detecția amenințărilor avansate
- Tehnologiile de analiză comportamentală și machine learning sunt utilizate pentru detectarea și prevenirea amenințărilor avansate care pot evita detecția de către soluțiile de securitate convenționale. Aceste tehnologii sunt capabile să identifice modele de activitate suspectă și să implementeze măsuri preventive în timp real.
- Conformitatea și protecția datelor
- Pe măsură ce îngrijorările privind conformitatea cu reglementările privind protecția datelor, cum ar fi GDPR sau CCPA, cresc, securitatea în cloud trebuie să garanteze respectarea acestor reglementări și să furnizeze instrumente pentru gestionarea și protejarea datelor sensibile.
- Educația și conștientizarea securității
- Educația și conștientizarea securității sunt esențiale în prevenirea atacurilor cibernetice, instruind utilizatorii să identifice și să raporteze posibile amenințări, deoarece oamenii rămân unul dintre cei mai vulnerabili factori în ceea ce privește securitatea cibernetică. Aceste evoluții în domeniul securității cloud-ului ilustrează necesitatea permanentă de a dezvolta și implementa soluții inovatoare pentru protejarea datelor și infrastructurii în mediul digital într-o continuă transformare. Prin adoptarea și integrarea acestor tendințe, organizațiile pot gestiona riscurile mai eficient și pot asigura securitatea datelor lor în era digitală.

*R*iscuri și Oportunități ale Tehnologiilor Emergente

Secțiunea ar putea explora atât aspectele de risc, cum ar fi escaladarea amenințărilor cibernetice sofisticate și punctele vulnerabile legate de adoptarea tehnologiilor emergente, cât și perspectivele pozitive, cum ar fi optimizarea eficienței operaționale și avansul în inovația în domeniul securității. Incorporarea noilor tehnologii prezintă atât provocări, cât și perspective favorabile în domeniul securității cibernetice, în contextul perspectivelor viitoare și al inovațiilor în digitalizarea proceselor de securitate. Este crucial să analizăm aceste potențiale pericole și beneficii pentru a elabora strategii și soluții corespunzătoare pentru securizarea

datelor și infrastructurii într-un mediu digital în perpetuă evoluție. Iată câteva dintre principalele riscuri și oportunități asociate cu noile tehnologii: [13]

- Amenințări cibernetice avansate
- Noile tehnologii, cum ar fi inteligența artificială și criptografia cuantică, ar putea fi exploatate de către atacatori pentru a genera amenințări cibernetice mai avansate și mai greu de identificat și contracarat.
- Vulnerabilități noi și necunoscute
- Odată cu integrarea tehnologiilor emergente, apar și noi slabiciuni și zone vulnerabile care pot fi exploatate de către atacatori. Adoptarea timpurie și implementarea acestor tehnologii poate prezenta riscuri neașteptate în ceea ce privește securitatea.
- Probleme de confidențialitate și etică
- Tehnologiile emergente, precum recunoașterea facială și analiza big data, generează îngrijorări în ceea ce privește confidențialitatea și drepturile individuale. Utilizarea acestor tehnologii poate implica colectarea și procesarea extensivă a datelor personale, având potențialul de a afecta intimitatea și libertatea individuală.
- Dependența de tehnologie
- Pe măsură ce organizațiile își intensifică utilizarea tehnologiilor emergente în operațiunile lor cheie, există posibilitatea unei dependențe excesive de aceste tehnologii și a unei vulnerabilități sporite în fața eventualelor defecțiuni sau atacuri cibernetice.
- Detectarea și prevenirea amenințărilor mai eficiente
- Tehnologiile emergente, precum inteligența artificială și analiza comportamentală, pot furniza funcționalități avansate pentru detectarea și prevenirea amenințărilor, facilitând identificarea și intervenția mai promptă în caz de atacuri cibernetice. Organizațiile trebuie să adopte o strategie echilibrată și proactivă în ceea ce privește securitatea cibernetică, pentru a profita de avantajele oferite de tehnologiile emergente și pentru a gestiona riscurile asociate. Acest lucru implică o evaluare atentă a beneficiilor și riscurilor fiecărei tehnologii, împreună cu implementarea măsurilor adecvate pentru protejarea datelor și infrastructurii într-un mediu digital în continuă schimbare.

Perspectivele viitoare și inovațiile în digitalizarea proceselor de securitate sunt esențiale într-un peisaj global din ce în ce mai interconectat și dependent de tehnologie. Într-un mediu digital într-o continuă schimbare, organizațiile se confruntă cu provocări și oportunități complexe în ceea ce privește protejarea datelor și infrastructurii lor împotriva amenințărilor cibernetice în continuă expansiune.

Capitolul 3. Studiu de caz

Într-o perioadă în care tehnologia continuă să avanseze rapid, interesul și relevanța votului electronic în cadrul democrației contemporane cresc constant. Această temă este subiectul unor dezbateri intense și extinse atât în cercurile politice, cât și printre experții în domeniul tehnologiei și membrii societății în ansamblu. Votul electronic are potențialul de a simplifica accesul la vot pentru diferite segmente de populație, inclusiv pentru cei care se confruntă cu dificultăți de mobilitate sau care locuiesc în afara țării. Implementarea acestei tehnologii ar putea stimula o mai mare implicare în procesul electoral și ar putea face exercitarea dreptului de vot mai comodă pentru alegători.

Autoritatea Electorală Permanentă este o entitate administrativă independentă, cu statut juridic propriu și cu competențe extinse în domeniul electoral. Misiunea sa este să garanteze planificarea și realizarea alegerilor și a referendumurilor, și să finanțeze partidele politice și campaniile electorale, respectând în întregime Constituția, legislația națională și standardele internaționale și europene în domeniu. Autoritatea Electorală Permanentă își desfășoară activitatea în conformitate cu principiile independenței, imparțialității, legalității, transparenței, eficienței, profesionalismului, responsabilității, sustenabilității, predictibilității și legitimității. [26]

Cadrul legal

De la înființarea sa prin Legea nr. 286/2003, atribuțiile Autorității Electorale Permanente s-au extins semnificativ prin intermediul unor acte normative ulterioare, cum ar fi Legea nr. 373/2004 privind alegerea Camerei Deputaților și a Senatului, Legea nr. 334/2006 referitoare la finanțarea partidelor politice și a campaniilor electorale, Legea nr. 33/2007 privind alegerile pentru Parlamentul European și Legea nr. 35/2008 pentru alegerea Camerei Deputaților și a Senatului, printre altele. De asemenea, atribuțiile au fost influențate de numeroase ordonanțe de urgență ale Guvernului și alte legi, inclusiv Legea nr. 208/2015 privind alegerile pentru Senat și Camera Deputaților și organizarea și funcționarea Autorității Electorale Permanente, precum și Legea nr. 115/2015 privind alegerile autorităților administrației publice locale și alte modificări legislative.

Scopul principal al Autorității Electorale Permanente este: [26]

- de a garanta și de a îmbunătăți în mod constant cadrul legal și organizatoric al alegerilor și a oricăror alte forme de consultare la nivel național sau local, inclusiv finanțarea partidelor politice, în conformitate cu instrumentele juridice internaționale, legislația comunitară și prevederile constituționale.
- se asigura ca dispozițiile legale din domeniul electoral și al finanțării partidelor politice sunt aplicate uniform în întreaga țară, și controlează îndeplinirea sarcinilor și atribuțiilor celorlalte autorități publice care au competențe în acest domeniu.
- are rolul de a instrui și informa atât electoratul, cât și ceilalți participanți la procesul electoral.
- reprezintă România în relațiile externe, evidențiind modul în care statul respectă principiile democratice, inclusiv exercitarea drepturilor electorale, egalitatea de șanse în competiția politică și transparența în finanțarea partidelor politice și a campaniilor electorale.

Obiective:

- Alegerile sunt organizate periodic, desfășurate în mod liber și corect, cu o gestionare eficientă și transparentă a resurselor umane, financiare și economice.
- Management electoral integrat.
- Partidele politice și campaniile electorale beneficiază de finanțare echitabilă și transparentă.

Funcţii:

Conform Legii nr. 208/2015 referitoare la alegerea Senatului și a Camerei Deputaților și la organizarea și funcționarea Autorității Electorale Permanente, AEP este responsabilă pentru următoarele aspecte:

- Dezvoltă sugestii privind furnizarea logistică necesară pentru desfășurarea alegerilor.
- Aceste sugestii sunt transmise Guvernului și autorităților administrației publice locale pentru a fi luate în considerare și implementate.
- AEP monitorizează modul în care aceste sugestii sunt puse în practică.

O noțiune ambiguă, „vot electronic” poate cuprinde diverse metode de exprimare a votului bazate pe tehnologie electronică. Prin urmare, este necesară o clarificare terminologică pentru a desemna specific tipurile de vot electronic și componentele implicate. În prezent, la nivel global, există patru categorii de sisteme de vot care implică cel puțin un aspect electronic. [27]

Numărarea electronică:

În acest sistem, componenta electronică se limitează la procesul de numărare a voturilor, în timp ce celelalte aspecte ale procesului electoral rămân tradiționale: alegătorul completează un

buletin de vot de hârtie în cabina de vot, indică opțiunea sa pe buletin și ulterior introduce buletinul în urnă. La sfârșitul procesului, rezultatele sunt procesate de un calculator pentru a determina câștigătorul alegerilor.

Mașini de vot electronice care funcționează cu hârtie:

Conform acestui sistem, procesul de votare efectiv ar fi realizat cu un dispozitiv electronic care ar genera un buletin de vot pe care ar fi înregistrată opțiunea exprimată de alegător. Alegătorul introduce buletinul de vot produs de dispozitivul de votare într-o urnă convențională, care colectează buletinele de vot până la încheierea scrutinului. Conținutul urnei este apoi numărat fie manual, în mod tradițional, fie automat, cu ajutorul unei alte componente electronice. Prin urmare, o variantă a acestui tip de sistem de vot utilizează scannere, cu grade variate de automatizare, pentru a scana buletinele de vot și a raporta rezultatele numărătorii, în timp ce buletinele de vot sunt păstrate pentru a fi verificate ulterior, dacă este necesar. [28]

Sistemele de vot electronic cu înregistrare directă (Direct-recording electronic - DRE voting machines):

Sistemul DRE a fost dezvoltat ca o evoluție a mașinilor de vot electronice tradiționale, diferența principală constând în capacitatea mașinii de a înregistra și număra electronic preferințele exprimate de alegători. Un beneficiu semnificativ al acestui sistem este eliminarea necesității utilizării urnelor și a generării buletinelor de vot. Sistemul DRE a fost dezvoltat ca o evoluție a mașinilor de vot electronice tradiționale, diferența principală constând în capacitatea mașinii de a înregistra și număra electronic preferințele exprimate de alegători. Un beneficiu semnificativ al acestui sistem este eliminarea necesității utilizării urnelor și a generării buletinelor de vot. În scopul asigurării corectitudinii înregistrării votului, atât pentru alegători cât și pentru organizatori, mașinile de vot DRE pot include un mecanism de verificare bazat pe o urmă de audit pe hârtie, cunoscut sub numele de voter verification paper audit trail (VVPAT).

Cu toate că există diverse modalități de implementare a sistemului VVPAT, toate se concentrează pe imprimarea pe hârtie a opțiunii exprimate de către alegător și pe stocarea acestei hârtii pentru a permite renumărarea ulterioară, dacă este necesar. Referitor la sistemul VVPAT, există preocupări legate de securitate [29]. Potrivit acestor preocupări, există riscul ca sistemul să fie infectat cu un virus care să modifice intenționat votul înregistrat, făcând dificilă distingerea între voturile valide și cele fraudate. În plus, acest sistem nu garantează secretul votului, ceea ce ridică, de asemenea, preocupări etice.

Vot la distanță online/pe Internet:

Această tehnologie reprezintă vârful evoluției sistemelor de vot electronic, deoarece oferă alegătorilor posibilitatea de a vota de oriunde în lume, utilizând doar un dispozitiv conectat la internet. Implementarea unui astfel de sistem în procesele electorale ar putea aduce beneficii considerabile, dar este în același timp un subiect controversat, fiind însoțit de întrebări majore privind securitatea.

Dacă este pus în aplicare cu atenție, sistemul de vot electronic poate eradica frauda, îmbunătăți procesarea rezultatelor, extinde accesibilitatea și poate face exercitarea votului mai convenabilă pentru cetățeni. În unele situații, utilizarea acestui sistem în diverse evenimente electorale ar putea duce la reducerea costurilor alegerilor și referendumurilor pe termen lung. Cu toate acestea, nu toate eforturile de digitalizare reușesc să atingă aceste obiective din cauza preocupărilor legate de securitatea tehnologiei actuale pe care se bazează aceste sisteme.

În unele situații, au apărut provocări atât legislative, cât și tehnice, iar în altele a fost exprimat scepticismul cu privire la faptul că sistemul de vot electronic nu este încă complet dezvoltat. E-votingul este adesea văzut ca o cale de progres în cadrul democrației, contribuind la consolidarea încrederii în managementul electoral și oferind credibilitate rezultatelor electorale, ceea ce poate îmbunătăți eficiența procesului electoral. O provocare majoră a sistemelor de acest

tip este menținerea secretului votului, motiv pentru care este crucial să se evite orice asociere între identitatea alegătorului și distribuția votului exprimat. Această practică este în contradicție cu principiile sistemelor care utilizează tehnologia informației (TIC), deoarece sistemele TIC sunt în mod intrinsec construite pentru a urmări și monitoriza tranzacțiile efectuate.

În plus, separarea completă între alegător și vot poate compromite integritatea unui sistem de vot electronic, deoarece nu poate fi garantată numărarea și înregistrarea corectă a fiecărui vot. Astfel, confirmarea indirectă a corectitudinii rezultatelor electronice prin intermediul auditului pe hârtie sau prin certificarea sistemelor, împreună cu o supraveghere atentă a calității și a procedurilor de securitate, devine de o importanță crucială pentru asigurarea integrității unui sistem de vot electronic. Fără aceste măsuri, există riscul ca rezultatele incorecte sau manipulate să rămână nedetectate. [28]

După cum se poate observa și în tabelul 1, la nivel global, stadiul adoptării diferitelor tipuri de sisteme de vot electronic este variabil. Perspectiva asupra acestei probleme și modul în care sunt compilate diversele statistici pot crea impresia că votul electronic este mai răspândit decât este în realitate. Această situație se datorează faptului că multe state au explorat ideea votului electronic, trecând de la discuții preliminare, prin diverse teste și soluții, până la adoptarea votului electronic doar pentru anumite grupuri de cetățeni sau la nivel local/regional.

	Utilizat în trecut	Utilizat parțial în trecut	Utilizare universală	**Total (în funcție de tip)**
Mașini bazate pe hârtie + numărare electronică sau mașini de vot cu înregistrare directă cu urmă de audit pe hârtie		1 (6.25%) Belgia		1 (6.25%)
Mașini de vot cu înregistrare directă fără urmă de audit pe hârtie	4 (25 %) Finlanda, Germania, Irlanda, Olanda		2 (12.5%) Brazilia, India	6 (37.5%)
Vot pe Internet	2 (12.5%) Norvegia, Suedia	1 (6.25%) Franța	1 (6.25%) Estonia	4 (25%)
Amestec de mai multe tipuri de sisteme de vot electronic		5 (31.25%) Australia, Canada, Elveția, Marea Britanie, Statele Unite ale Americii		5 (31.25%)
Total (în funcție de utilizare)	6 (37.5%)	7 (43.75%)	3 (18.75%)	

Figura 1. Statistica folosirii sistemelor de vot electronic în funcție de tipul de sistem folosit și de amploarea folosirii respectivelor sisteme de vot electronic.
Sursa: Victor Guzun, Kevin Tammearu, Ana-Maria Stancu, Alexandru Balmoș, Votul Online-Realitatea timpurilor noastre, București, 2020

În ceea ce privește funcționalitățile de bază, un sistem de vot electronic poate furniza: [28]

- Accesul la liste electorale electronice prin autentificarea alegătorilor.
- În cadrul unui sistem de vot digital, o componentă crucială poate fi lista electorală electronică, care poate acoperi o anumită zonă sau întreaga țară. Această listă poate fi

utilizată ca buletin de vot, iar alegătorul ar trebui doar să selecteze butonul corespunzător candidatului preferat.

- Platforma software destinată utilizării de către organizatorii din secțiile de votare.
- Aceste funcționalități includ adăugarea sau ștergerea de candidați, atribuirea de fotografii, stabilirea intervalului orar al scrutinului, precum și gestionarea datei și resetarea numărului de voturi.
- Interfața hardware variază în funcție de tipul de sistem utilizat, putând consta în ecrane tactile sau tablete, buletine de vot ce sunt scanate de un scanner, sau pagini web și software special pentru votul online.
- Platforme speciale pentru accesibilitatea persoanelor cu dizabilități.
- În acest context, interfața se referă la adaptarea procesului electoral pentru persoanele cu nevoi speciale, prin includerea sistemelor Braille sau audio pentru nevăzători și asigurarea accesului ușor pentru alegătorii cu dizabilități fizice.

Introducerea unor sisteme de vot electronic poate reprezenta o soluție pentru reducerea riscului de fraudă electorală și eliminarea posibilelor erori umane asociate cu procesul manual de numărare a voturilor. Cu toate acestea, este crucial să se garanteze că aceste sisteme sunt securizate și că asigură protecția confidențialității și integrității procesului electoral. AEN-ul trebuie să acorde o atenție deosebită aspectelor legate de securitatea cibernetică în timp ce examinează posibilitatea implementării votului electronic. [26]

Este de o importanță critică să se construiască sisteme de securitate puternice pentru a contracara eventualele amenințări cibernetice și pentru a garanta autenticitatea și verificabilitatea rezultatelor electorale. Deși votul electronic ar putea oferi avantaje semnificative, este esențial să se ia în considerare și necesitățile celor care nu au acces la tehnologie sau care nu se simt confortabil să folosească astfel de sisteme. AEN ar trebui să identifice modalități de a garanta că niciun alegător nu este marginalizat în procesul electoral din cauza lipsei de acces la tehnologie. Prin analiza meticuloasă și specializată a acestor chestiuni, AEN-ul poate să evalueze cu succes dacă implementarea votului electronic în sistemul electoral național este fezabilă și să exploreze potențialul său, garantând totodată integritatea și credibilitatea procesului electoral.

Categoriile de vot electronic

Pe măsură ce societatea avansează în era digitală, importanța votului electronic crește constant, iar există diverse metode prin care acesta poate fi introdus, fiecare prezentând avantaje și provocări unice. [30]

- Scanarea optică a buletinelor de vot.

Alegătorii se deplasează la secțiile de votare, completează buletinele de vot manual și apoi introduc buletinele într-un scaner optic care le înregistrează electronic. Scanerul examinează opțiunea exprimată de alegător și procesează datele pentru toți participanții la vot. Pentru alegători, această metodă nu reprezintă o schimbare semnificativă în comparație cu procedurile tradiționale de vot. Pentru membrii comisiei electorale, procedura de numărare și înregistrare a voturilor devine mult mai eficientă și mai rapidă.

În situația unor eventuale defecțiuni tehnice sau a necesității de a renumăra voturile, autoritățile electorale păstrează buletinele de vot pe hârtie ca o măsură de siguranță. SUA au fost prima țară care a implementat acest sistem în anul 1962.

- Aparate electronice cu înregistrare directă(DRE)

Aparatele DRE sunt dispozitive electronice avansate care nu necesită utilizarea unui buletin de vot pe hârtie. În loc să completeze un buletin de vot tradițional cu ajutorul unui pix sau al unei ștampile, alegătorii apasă butoane sau folosesc un ecran tactil pentru a-și selecta candidații

preferați. Primele dispozitive similare au fost lansate în Statele Unite în 1975. Eliminarea buletinelor de vot pe hârtie simplifică procesul electoral prin eliminarea necesității de a proiecta, tipări, stoca și transporta buletinele în timpul procesului electoral.

Echipamentele folosite în diferite țări variază, începând de la sistemele foarte simple și fiabile utilizate în India pentru aproape un miliard de alegători și continuând cu modele sofisticate care includ interferențe multilingve, dimensiuni variate ale fonturilor și chiar senzori de mișcare pentru persoanele cu dizabilități. Dispozitivele de vot electronic direct (DRE) sunt cele mai comune opțiuni de vot electronic utilizate la nivel global. Un aspect negativ semnificativ al metodei DRE este că nu există nicio dovadă fizică a votului înregistrat, ceea ce ridică îndoieli cu privire la securitatea și integritatea completă a procesului electoral. În încercarea de a soluționa această problemă, unele dispozitive de vot moderne sunt echipate pentru a imprima și a păstra opțiunile exprimate de alegători.

- Votul online

Această modalitate de exprimare a votului oferă posibilitatea alegătorilor de a vota de la distanță, de oriunde există o conexiune la internet, eliminând necesitatea de a se deplasa la o secție de votare. Toate etapele procesului electoral sunt desfășurate online, folosind metode și instrumente de identificare sigure. Această practică a fost implementată în mai multe țări, dar în prezent, doar Estonia o utilizează pentru toate tipurile de alegeri: locale, parlamentare și pentru Parlamentul European.

Similar cu orice formă de alegeri, standardele pentru votul electronic ar trebui să fie conforme cu Pactul internațional cu privire la drepturile civile și politice, adoptat de Organizația Națiunilor Unite în 1966 [31], care garantează principiile votului universal și egal, precum și secretul votului. În prezent, nu există standarde internaționale adoptate pentru votul electronic sau tehnologia asociată, iar acestea diferă de la o țară la alta.

În 2004, Consiliul Europei a emis o recomandare referitoare la standardele pentru votul electronic, care includ următoarele principii de bază: alegătorii trebuie să fie identificați, să aibă posibilitatea de a-și confirma votul înainte de a verifica ulterior corectitudinea exprimării acestuia și să fie anonimi; în plus, toate aspectele procesului electoral trebuie să fie complet transparente, ușor de înțeles și de utilizat. [32]

Beneficiile votului electronic

- Comoditate

Votul electronic este eficient, exact și se fundamentează pe liste electorale digitale extrem de precise, care sunt actualizate în mod prompt. Votul online oferă posibilitatea cetățenilor de a-și exprima votul din orice loc în care au acces la internet, făcându-l o metodă extrem de eficientă pentru comunitățile mari de expatriați, pentru cetățenii rezidenți permanent în străinătate și pentru cei care călătoresc, economisind astfel timp și resurse considerabile.

- Creșterea prezenței la vot

Votul electronic extinde accesul la vot pentru un număr mai mare de cetățeni. Având în vedere că procentul mediu al participării la alegeri este în scădere în întreaga lume, adoptarea votului electronic, în special a celui online, ar putea spori prezența la vot, conducând la rezultate electorale mai autentice și mai reprezentative. O problemă majoră pentru multe democrații este absența oportunităților de vot pentru milioane de cetățeni care trăiesc în străinătate. De exemplu, la alegerile prezidențiale din 1 noiembrie 2020 în Republica Moldova (primul tur), doar 48,54% din cetățenii cu drept de vot au participat, în comparație cu 50,95% în alegerile din 2016.

- Economie de bani și de resurse

În Estonia, costurile per persoană asociate votului online sunt de aproximativ zece ori mai mici decât cele ale votului tradițional cu buletine de vot. Această tranziție a economisit aproximativ 11.000 de zile lucrătoare în timpul alegerilor din 2017. După implementare, votul online devine o opțiune de vot convenabilă și economică, în special în țările care organizează scrutine și referendumuri frecvente. Această soluție este benefică având în vedere că mulți alegători ar trebui să parcurgă distanțe mari și ar avea nevoie de mult timp pentru a vota în ziua alegerilor.

- Înregistrarea alegătorilor.

Registrele electorale digitale sunt extrem de exacte și pot reflecta informațiile actualizate din registrele populației. Prin urmare, în cea mai mare parte a situațiilor, sunt eliminate persoanele decedate, se previne înregistrarea multiplă și se reduc șansele de fraudă electorală. În comparație, registrele electorale pe hârtie sunt mai vulnerabile la aceste riscuri și, prin urmare, sunt mai puțin fiabile. De asemenea, colectarea datelor biometrice de la cetățeni reduce riscul înregistrării incorecte a alegătorilor.

- Verificarea identității alegătorilor

Frauda electorală prin vot multiplu reprezintă o problemă serioasă în multe țări, iar soluțiile digitale pot ajuta la reducerea acestui fenomen. Prin utilizarea instrumentelor de identificare digitală securizate, lucrătorii electorali pot verifica în ziua alegerilor, folosind informațiile actualizate din evidența populației. În Estonia, identitatea este verificată de la distanță folosind cărțile de identitate electronice securizate și infrastructura corespunzătoare, disponibile pentru orice rezident înregistrat. În mai multe țări, sunt folosite date biometrice pentru a compara identitatea alegătorului cu registrul electoral.

- Exprimarea votului

Sistemul de vot electronic reprezintă o soluție eficientă pentru a rezolva numeroasele provocări asociate procesului de votare. În Estonia, întregul proces de votare este finalizat în câteva minute. Interfața este intuitivă și accesibilă, permițând alegătorilor să corecteze eventualele erori sau să-și schimbe preferințele de vot, în cazul în care este necesar, sau în situația în care votul lor a fost influențat în mod nepermis. În diverse state, analfabetismul reprezintă o problemă serioasă, iar dispozitivele de vot cu ecran tactil (DRE) facilitează procesul de vot pentru cetățeni. În același mod, votul electronic poate fi de ajutor pentru persoanele cu dizabilități, care nu pot să se deplaseze la secțiile de votare în ziua alegerilor sau care suferă de deficiențe de vedere.

- Numărarea voturilor

După încheierea votului, demarează procedura atentă de numărare a voturilor; procesul digital de numărare este extrem de rapid și precis, practic eliminând erorile umane și reducând semnificativ numărul de resurse umane necesare. Acest beneficiu este extrem de valoros în țări cu populații mari, cum ar fi India, Brazilia și Statele Unite ale Americii. În Estonia, procesul de numărare a rezultatelor votului online este aproape în totalitate automatizat și extrem de rapid.

- Transmiterea și înregistrarea rezultatelor.

În fiecare scrutin electoral, mii sau chiar milioane de secții de votare sunt deschise în toate țările. Colectarea rezultatelor de la toate aceste secții de votare și circumscripțiile electorale poate fi un proces extrem de complex și laborios, iar în unele situații, poate fi și destul de imprecis. Cu ajutorul instrumentelor digitale, datele pot fi transmise instantaneu în mod securizat, facilitând astfel înregistrarea și comunicarea rezultatelor într-un timp mai scurt.

Principalele preocupări privind votul electronic

- Încrederea

Principala preocupare a alegătorilor, instituțiilor de stat și partidelor politice în ceea ce privește votul electronic este înțelegerea și încrederea în funcționarea acestor sisteme. De multe ori, cetățenii și chiar liderii politici au dificultăți în înțelegerea modului în care funcționează sistemele electorale electronice, iar reacția lor inițială este să se opună utilizării acestor sisteme. Politicienii utilizează adesea afirmații referitoare la disfuncționalitățile sistemelor în diverse moduri și în scopuri variate. [30]

În numeroase țări, lipsa încrederii în sistemele electorale electronice a generat o rezistență serioasă și, ca rezultat, implementarea lor a fost oprită sau întârziată. Gradul de încredere în alegerile electronice este un proces gradual, influențat de nivelul general de încredere în instituțiile statului. Mai mulți experți recomandă că cea mai eficientă metodă de implementare a votului electronic ar fi prin etape treptate.

- Protecția împotriva fraudelor electorale

Procedura de vot electronic este una democratică, însă autoritățile naționale nepotrivite sau corupte ar putea să folosească soluțiile digitale pentru a influența rezultatele alegerilor, fie din greșeală, fie intenționat.

- Fiabilitatea, auditabilitatea și verificabilitatea

Autentificarea electronică nu este mereu precisă în totalitate, iar sistemele pot avea defecțiuni sau funcționa necorespunzător din când în când. De asemenea, probleme legate de conectivitatea la internet și defecțiuni hardware pot apărea frecvent, în special în țările în curs de dezvoltare. Dacă votul se va desfășura exclusiv în mediul digital, există o preocupare semnificativă cu privire la modalitățile de verificare ulterioară a preciziei, în situații de fraudă electorală, necesitatea renumărării voturilor sau apariția neîncrederii în rezultate. [28]

Pentru a soluționa această problemă, numeroase dispozitive de vot cu ecran tactil sunt concepute pentru a imprima o copie pe hârtie, denumită pista de audit pe hârtie verificabilă de către alegători (WPAT). Atunci când voturile sunt exprimate electronic, mulți alegători nu sunt conștienți de procesul prin care trec voturile lor în dispozitivele de vot, sau dacă acele voturi au fost înregistrate și numărate corect.

Sistemele de vot electronic cele mai recente oferă alegătorilor posibilitatea să-și verifice voturile folosind sistemul E2EVV (verificare a întregului proces de votare), prin care aceștia pot confirma dacă votul lor a fost exprimat, înregistrat și numărat corect. Din anul 2013, sistemul de vot la distanță din Estonia a oferit alegătorilor posibilitatea de a utiliza sistemul E2EVV.

- Testarea și certificarea

Preocupările legate de testare și certificare sunt prezente, deoarece sistemele care nu sunt supuse la teste și certificări adecvate tind să nu beneficieze de suficientă credibilitate. Pentru mulți cetățeni, cunoștințele despre tehnologiile de vot electronic și funcționalitățile lor sunt limitate, motiv pentru care testarea și certificarea acestora de către entități independente și credibile sunt esențiale. În anumite situații, entități independente au reușit să influențeze funcționarea diverselor sisteme, ceea ce a slăbit credibilitatea acestora.

- Costuri ridicate

În unele state, adoptarea tehnologiilor de vot electronic poate fi o investiție costisitoare. Dispozitivele DRE sunt complicate, costisit Dacă doresc să urmeze exemplul Estoniei și să elibereze cărți de identitate electronice pentru fiecare cetățean, unele țări ar trebui să actualizeze și să schimbe certificatele de identificare securizate.oare, necesită mentenanță dificilă și trebuie

păstrate adecvat între perioadele de alegeri. Echipamentele hardware, precum computerele de ultimă generație, și programele de competențe informatice pot fi, de asemenea, costisitoare.

eVoteNow-Detalii de implementare

În acest subcapitol, voi examina procesul de implementare a aplicației eVoteNow, inclusiv tehnologiile utilizate, nucleul sistemului, structura sa, cazurile de utilizare și un studiu de caz care evidențiază funcționalitățile și procedurile folosite în dezvoltarea sa. [28]

Baza de date

Baza aplicației prezentate în acest studiu are la bază o bază de date MySQL, care stochează informații despre utilizatori, administratori, candidați și configurarea sistemului. După cum se poate observa în Figura 1, baza de date este compusă din patru tabele distincte.

Tabel	Acțiune	Rânduri	Tip	Interclasare	Dimensiune
admin	Navigare Structură Caută Inserare Golește Aruncă	1	InnoDB	latin1_swedish_ci	16 KiO
candidati	Navigare Structură Caută Inserare Golește Aruncă	3	InnoDB	latin1_swedish_ci	16 KiO
setari	Navigare Structură Caută Inserare Golește Aruncă	1	InnoDB	latin1_swedish_ci	16 KiO
utilizatori	Navigare Structură Caută Inserare Golește Aruncă	12	InnoDB	latin1_swedish_ci	32 KiO
4 tabele	Sumă	17	InnoDB	latin1_swedish_ci	80 KiO

Figura 1. Structura bazei de date.
Sursa https://www.code4.ro/ro/blog/securitatea-sistemelor-de-vot-electronic

- În tabelul admin sunt înregistrate detalii referitoare la administratorul sistemului, inclusiv numele, prenumele, numele de utilizator și parola, cu un ID unic ca cheie primară. Din perspectiva tipului de date, aceste câmpuri conțin informații de tip VARCHAR, cu o lungime maximă de 50 de caractere, cu excepția cheii primare, care este de tip INT.

id	nume	prenume	username	passcode
1	Ionescu	Popescu	admin	21232f297a57a5a743894a0e4a801fc3

Figura 2.Tabelul cu administratori.
Sursa https://www.code4.ro/ro/blog/securitatea-sistemelor-de-vot-electronic

Din considerente de securitate, toate parolele din acest sistem sunt criptate folosind algoritmul MD5 (Message Digest Algorithm 5) sau SHA1 (Secure Hash Algorithm 1), astfel încât să nu poată fi văzute în clar.

- În tabelul candidați sunt stocate detalii importante despre aceștia, inclusiv nume, prenume, departament sau partid, funcție sau rol, mesaj sau slogan, imagine, precum și numărul de voturi obținute. Datorită flexibilității sistemului, câmpurile din acest tabel au fost definite într-un mod generic pentru a putea fi ajustate în funcție de schimbările necesare. Cheia primară rămâne un ID unic, generat automat cu funcția de autoincrementare, având tipul de date INT. Pentru a optimiza accesul la baza de date, s-a optat pentru stocarea locală a imaginilor asociate candidaților, în timp ce în tabel sunt salvate doar căile absolute către aceste imagini. Această abordare a permis îmbunătățirea vitezei de acces și reducerea traficului de date, contribuind la economisirea lățimii de bandă disponibile.

#	Nume	Tip	Interclasare	Proprietăți	Nul	Implicit	Extra
1	**id**	int(11)		UNSIGNED	Nu	*None*	AUTO_INCREMENT
2	**nume**	varchar(40)			Nu	*None*	
3	**prenume**	varchar(40)			Nu	*None*	
4	**departament**	varchar(20)			Da	*NULL*	
5	**imagine**	varchar(256)			Nu	*None*	
6	**voturi**	int(11)			Nu	*None*	
7	**mesaj**	varchar(255)			Nu	*None*	
8	**functie**	varchar(255)			Da	*NULL*	

Figura 3. Tabelul candidaților.
Sursa: Victor Guzun, Kevin Tammearu, Ana-Maria Stancu, Alexandru Balmoș, Votul Online-Realitatea timpurilor noastre, București, 2020

• În tabelul setări sunt stocate datele de configurare ale sistemului, inclusiv numele evenimentului pentru care se efectuează votul, tipul de vot (unic sau modificabil) și intervalul de timp alocat pentru votare. În contrast cu tabelele anterioare, tipul de date utilizat pentru stocarea intervalului de timp al votului este DATETIME. Folosind acest tip de date, este posibil să se stocheze atât data, cât și ora într-un singur câmp, contribuind la eficiența sistemului. De asemenea, pentru a îndeplini această cerință, s-a utilizat și tipul de date TINYINT pentru a stoca tipul de vot, care poate lua doar valorile 1 și 2 în această versiune a sistemului.

#	Nume	Tip	Interclasare	Proprietăți	Nul	Implicit	Extra
1	**id**	int(11)			Nu	*None*	AUTO_INCREMENT
2	**nume**	varchar(255)			Nu	*None*	
3	**tip**	tinyint(4)			Nu	*None*	
4	**data_inceput**	datetime			Nu	*None*	
5	**data_sfarsit**	datetime			Nu	*None*	

Figura 4.Tabelul de setări.
Sursa: Victor Guzun, Kevin Tammearu, Ana-Maria Stancu, Alexandru Balmoș, Votul Online-Realitatea timpurilor noastre, București, 2020

• Tabelul utilizatorilor este cel mai elaborat din acest sistem, deoarece utilizatorul constituie cea mai vitală componentă a acestuia. Pentru fiecare utilizator, sunt necesare înregistrarea numelui și prenumelui, a codului numeric personal, pentru a evita ambiguități, a adresei, a unui indicator care indică dacă utilizatorul a votat anterior, a opțiunii de vot exprimată, a unei parole de acces și, opțional, a datei angajării. Deși poate părea că încalcă confidențialitatea votului, înregistrarea opțiunii de vot în baza de date este esențială pentru a valida corectitudinea rezultatelor. Pentru a asigura integritatea, nici administratorul sistemului nu are acces la informația despre cine a votat pentru cine.

#	Nume	Tip	Interclasare	Proprietăți	Nul	Implicit	Extra
1	**id**	int(11)		UNSIGNED	Nu	*None*	AUTO_INCREMENT
2	**nume**	varchar(40)			Nu	*None*	
3	**prenume**	varchar(40)			Nu	*None*	
4	**cnp**	char(13)			Nu	*None*	
5	**tara**	varchar(20)			Nu	*None*	
6	**adresa**	varchar(50)			Nu	*None*	
7	**votat**	int(1)			Nu	*None*	
8	**vot**	int(11)			Nu	*None*	
9	**parola**	varchar(255)			Nu	*None*	
10	**data_ang**	datetime			Da	*NULL*	

Figura 5. Tabelul utilizatorilor.
Sursa: Victor Guzun, Kevin Tammearu, Ana-Maria Stancu, Alexandru Balmoș, Votul Online-Realitatea timpurilor noastre, București, 2020

Structura aplicației

Structura întregului sistem se bazează pe clase care includ atribute și metode, această abordare ajutând la depanarea și dezvoltarea ulterioară a codului, precum și la posibilitatea de a reutiliza porțiuni de cod. Pentru a evidenția importanța acestor clase, diagrama de clase UML (Unified Modeling Language) din Figura 13 ilustrează atât clasele principale, cât și relațiile dintre ele.

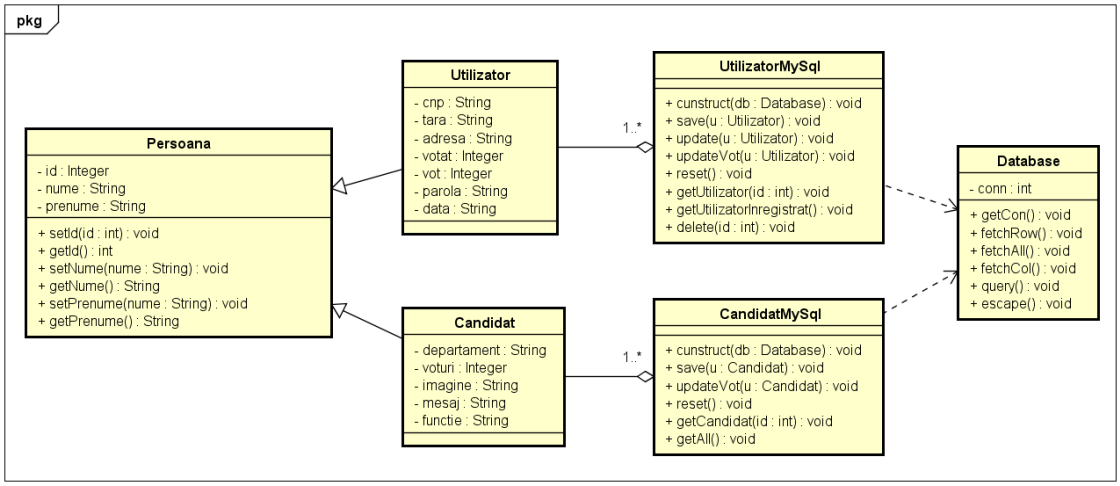

Figura 6.Diagrama de clase.
Sursa: https://www.freiheit.org/ro/romania-and-republic-moldova/votul-online-realitatea-timpurilor-noastre

- Clasa Persoană servește ca o clasă fundamentală, fiind clasa părinte pentru clasele Utilizator și Candidat. Plecând de la premisa că atât utilizatorii, cât și candidații sunt persoane, această clasă și metodele sale încorporează datele comune ale acestora, cum ar fi numele și prenumele. Această abordare a economisit timp și spațiu prin definirea acestor atribute într-un singur loc și utilizarea lor în mai multe contexte. Ca și atribute, clasa conține id, nume și prenume, toate fiind marcate cu modificatorul de acces protected, astfel încât să poată fi accesate din clasele copil.

Figura 7. Clasa persoană.
Sursa: Victor Guzun, Kevin Tammearu, Ana-Maria Stancu, Alexandru Balmoș, Votul Online-Realitatea timpurilor noastre, București, 2020

```
class Persoana
{
    protected $id;
    protected $nume;
    protected $prenume;
```

• Clasele Utilizator și Candidat preiau atributele și metodele definite cu modificatorul de acces protected în clasa părinte și definesc, la rândul lor, o serie de atribute și metode conform câmpurilor din baza de date.

• Clasele UtilizatorMySql și CandidatMySql includ un set de funcții care implementează interogările SQL (Structured Query Language), prin intermediul cărora clasele Utilizator și Candidat interacționează cu baza de date. Aceste clase permit efectuarea operațiilor CRUD (Create, Read, Update, Delete), precum și a altor funcții specifice. În principal, metodele acestor clase apelează metodele definite în clasa DbMySql, specializată în lucrul cu baze de date. Acestea includ metode care returnează fie un rând, fie o coloană, fie un obiect, așa cum este ilustrat în figurile de mai jos:

```
public function fetchRow($query)
{
    $result = mysqli_query($this->conn, $query);
    $roww = $result->fetch_assoc();
    return $roww;
}
```

Figura 8a. Clasele UtilizatorMySql și CandidatMySql.
Sursa: Victor Guzun, Kevin Tammearu, Ana-Maria Stancu, Alexandru Balmoș, Votul Online-Realitatea timpurilor noastre, București, 2020

```
public function fetchCol($query, $col = null)
{
    $result = mysqli_query($this->conn, $query);
    $arr = array();
    $col=(is_null($col))? 0:$col;
    while ($row = $result->fetch_array())
    {
        if (!isset($row[$col])) break;
        $arr[] = $row[$col];
    }
    return $arr;
}
```

Figura 8b. Clasele UtilizatorMySql și CandidatMySql.
Sursa: Victor Guzun, Kevin Tammearu, Ana-Maria Stancu, Alexandru Balmoș, Votul Online-Realitatea timpurilor noastre, București, 2020

• În cadrul clasei DbMySql, primul element este funcția de conectare la baza de date, implementată în constructorul clasei și prezentată mai jos. În această situație, fiecare apel al constructorului ar rezulta în instanțierea unui nou obiect al acestei clase, adică o nouă conexiune. Din această cauză, a fost necesară implementarea unui model singleton (Singleton Pattern), care restricționează crearea mai multor instanțe ale aceluiași obiect, menținând o singură conexiune activă. Apelul acestei funcții este realizat static, folosind operatorul de rezoluție:

```
$db=DbMySql::getInstance();
```

```php
public static function getInstance()
{
    if(!self::$instance)
        {
            self::$instance=new self;
        }
    return self::$instance;

}
```

Figura 9.Clasa Setări.
Sursa: Victor Guzun, Kevin Tammearu, Ana-Maria Stancu, Alexandru Balmoș, Votul Online-Realitatea timpurilor noastre, București, 2020

- Clasa Setări include următoarele atribute: nume, tip, dată_început și dată_sfârșit, care reprezintă elementele configurabile ale sistemului. Prin intermediul acestei clase se realizează particularizarea sistemului prin furnizarea acestor opțiuni de configurare.

Cazuri de utilizare și activități

Din perspectiva modului în care este folosită, aplicația poate fi utilizată de două tipuri de utilizatori: administratorul și utilizatorul obișnuit. Diagrama cazurilor de utilizare din figura 14 oferă o succintă prezentare a acțiunilor pe care acești actori le pot întreprinde, oferind astfel o înțelegere a funcționalităților sistemului.

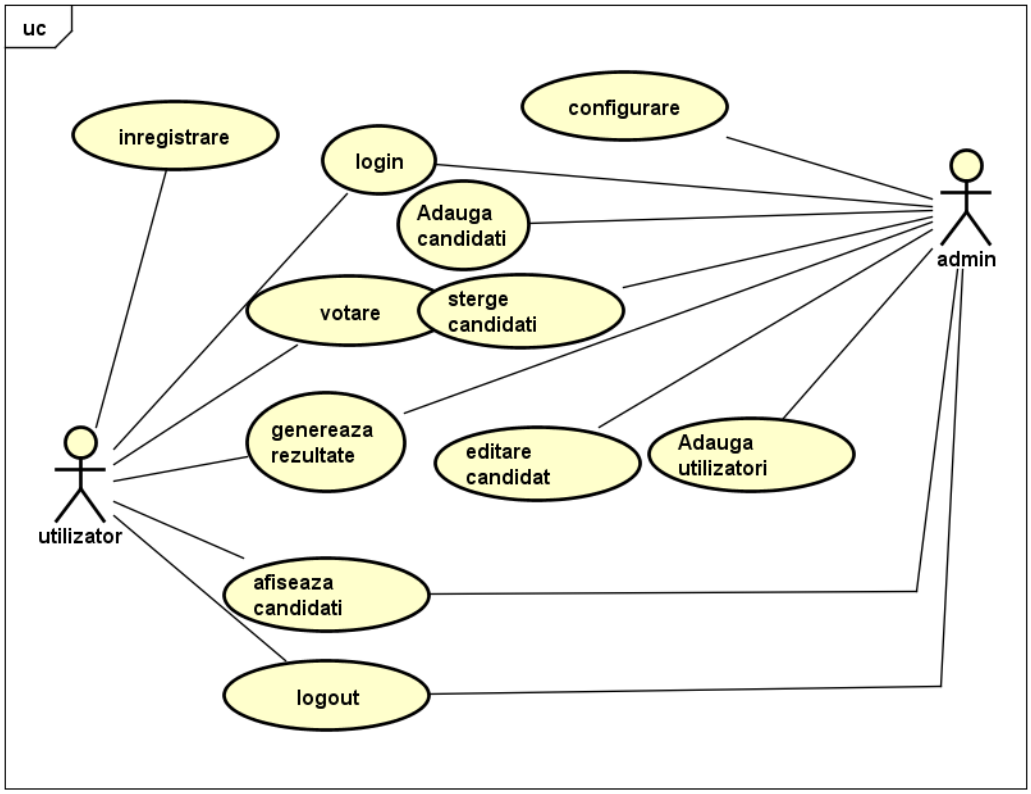

Figura 10. Diagrama Cazurilor de utilizare.
Sursa: https://www.freiheit.org/ro/romania-and-republic-moldova/votul-online-realitatea-timpurilor-noastre

Analizând diagrama, se poate deduce că utilizatorul nu trebuie să fie familiarizat cu operațiile complexe ale unui calculator, deoarece pașii necesari pentru a vota sunt simpli și ușor de înțeles. Acest grad de ușurință poate fi privit ca un avantaj semnificativ, deoarece permite utilizatorilor să-și exprime voturile rapid, reducând astfel riscul de supraîncărcare sau blocare a sistemului. Acțiunile pe care le întreprinde un utilizator în cadrul aplicației sunt influențate de durata intervalului de votare și de tipul de vot. În cazul în care intervalul este activ și sistemul o permite, utilizatorul are posibilitatea să-și modifice votul de câte ori dorește, cu condiția ca doar

ultima sa opțiune să fie reținută. Cu toate acestea, rezultatele finale nu sunt disponibile până când nu se încheie intervalul de timp alocat pentru votare.

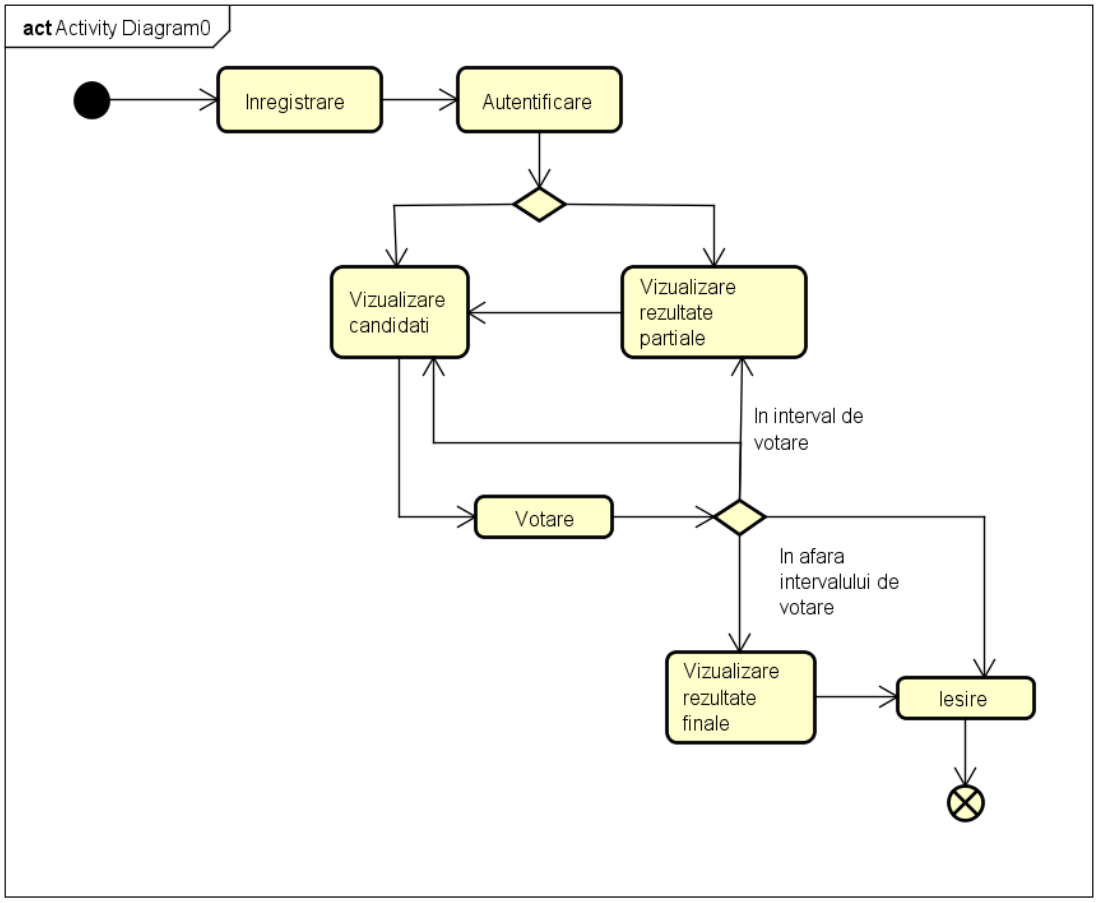

Figura 11. Diagrama de activități pentru utilizator.
Sursa: https://www.freiheit.org/ro/romania-and-republic-moldova/votul-online-realitatea-timpurilor-noastre

Pentru ca această aplicație să funcționeze corespunzător, este esențial ca administratorul să o configureze corect. Pentru a realiza acest lucru, administratorul trebuie să urmeze acești pași:

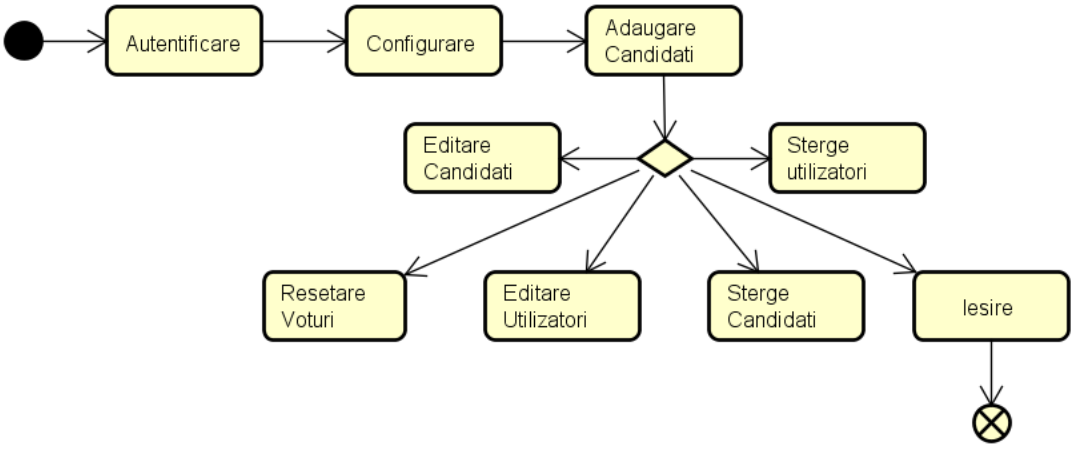

Figura 12. Diagrama de activități pentru administrator.
Sursa: https://www.freiheit.org/ro/romania-and-republic-moldova/votul-online-realitatea-timpurilor-noastre

Funcționalități și detalii de implementare

Pentru a accesa sistemul de vot electronic, este necesar ca utilizatorul să se înregistreze. Informațiile sale de identificare sunt apoi înregistrate într-o bază de date și vor fi utilizate pentru verificarea identității sale în momentul participării la vot. Interfața către baza de date este

implementată printr-o interfață grafică dezvoltată cu ajutorul PHP 5.6.19. Alegerea acestui limbaj de programare s-a datorat faptului că este orientat pe obiecte și nu necesită un compilator, ceea ce permite modificări în timp real la codul sursă al aplicației.

```
public function getUtilizatorInregistrat()
 {
     $myusername = $this->db->escape($_POST['username']);
     $mypassword = $this->db->escape($_POST['password']);
     $query = "SELECT * FROM utilizatori WHERE nume = '".$myusername."' AND prenume ='" .$mypassword. "' LIMIT 1";
     $row = $this->db->fetchRow($query);
     if ($row) {
      $utilizator = new Utilizator();
      $utilizator->setNume($row['nume'])->setPrenume($row['prenume'])->setCnp($row['cnp'])->setTara($row['tara'])
                 ->setAdresa($row['adresa'])->setVotat($row['votat'])->setVot($row['vot'])->setParola($row['parola'])
                 ->setId($row['id'])->setData($row['data_ang']);
        return $utilizator;}
      else return NULL;
 }
```

În situația în care utilizatorul nu are un cont, acesta este îndrumat să își creeze unul, după care este automat redirecționat către pagina de înregistrare. Procesul de autentificare se bazează pe numele și parola furnizate de utilizator, iar aceste date sunt trimise pentru verificare în baza de date. În situația în care verificarea este negativă, utilizatorul este notificat cu privire la incorectitudinea datelor furnizate, iar accesul său este restricționat până când acestea sunt corectate. Formularul de autentificare colectează informațiile introduse de utilizator și generează o interogare SQL prin intermediul funcției de mai jos.

Pentru a atribui valori variabilelor $myusername și $mypassword, s-a utilizat funcția escape(), care este o aliasă a funcției native PHP mysqli_real_escape_string(connection,String). Această funcție transformă șirul de caractere primit într-un șir securizat, care poate fi utilizat într-o interogare către baza de date. Această funcție elimină caracterele speciale care ar putea fi introduse de atacatori într-un șir de caractere, astfel menținând integritatea bazei de date. Acest tip de atac este cunoscut sub numele de SQL Injection.

În cazul în care datele de autentificare furnizate de utilizator sunt valide, funcția va crea un obiect de tip Utilizator. Apoi, folosind metodele din clasa corespunzătoare, va inițializa acest obiect cu valorile returnate de interogare. După aceasta, funcția va returna obiectul către pagina de autentificare și va solicita browserului să înceapă o sesiune care va rămâne activă până când utilizatorul se deconectează. Procedura de inițializare folosește un concept numit chaining (înlănțuire) pentru a simplifica scrierea codului. În caz contrar, dacă datele de autentificare sunt incorecte sau utilizatorul nu are un cont creat, interogarea va returna NULL, iar utilizatorul va primi un mesaj de eroare în consecință.

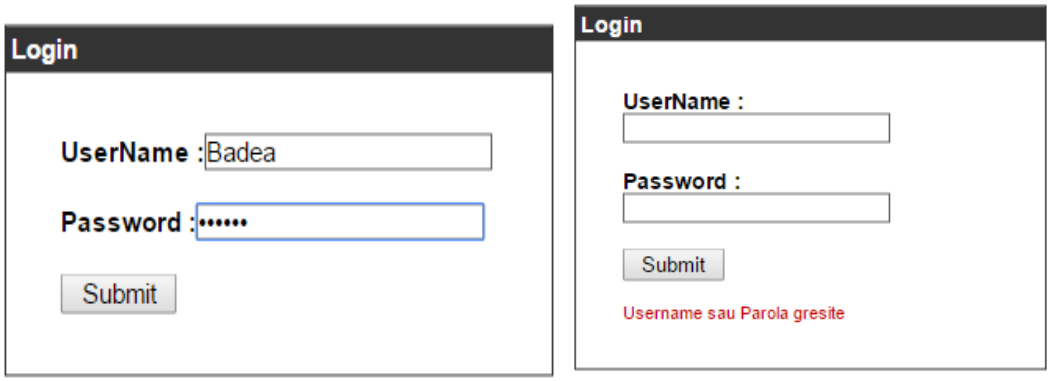

Figura 13. Formular de autentificare.
Sursa : https://elections.europa.eu/ro/how-to-vote/ro/

După autentificare, utilizatorul este redirecționat către pagina principală a aplicației. Această pagină conține un grafic cu rezultate parțiale, generat cu JavaScript și beneficiind de biblioteca JqueryUI. De asemenea, sunt afișate numele evenimentului setat de administrator, o numărătoare inversă care indică timpul rămas până la încheierea programului de vot și un meniu

de navigare. Meniul de navigare a fost dezvoltat separat, într-un alt script PHP, și este inclus în toate paginile accesibile utilizatorului. În plus, funcționarea meniului de navigare este influențată de numărătoarea inversă. Pe durata primirii voturilor, pagina cu rezultate finale nu poate fi accesată. Odată ce primirea voturilor încetează, pagina de vizualizare a candidaților va deveni indisponibilă.

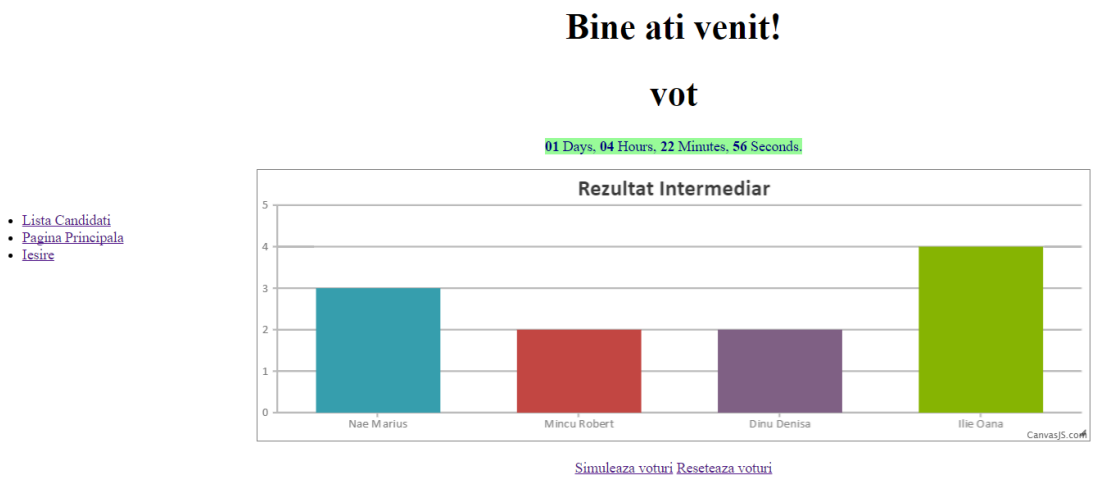

Figura 14. Pagina principală cu rezultate intermediare.
Sursa https://elections.europa.eu/ro/how-to-vote/ro/

Funcția canVote ia decizia pe baza informațiilor din baza de date, mai precis, preia un obiect de tipul Setări și determină dacă momentul curent se încadrează sau nu în intervalul specificat de la data de începere a evenimentului până la data de încheiere a evenimentului. Aceasta returnează o valoare booleană, adevărat sau fals, în funcție de rezultatul verificării. Conform secvenței de cod următoare, compararea acestor date se realizează prin intermediul funcției strtotime(). Această funcție convertește datele în numărul de secunde care au trecut de la 1 Ianuarie 1970.

```
public function canVote(){
    return (strtotime($this->data_inc) < time() && strtotime($this->data_sf) > time()) ? true : false;
}
```

Graficul cu rezultate intermediare ar trebui să fie actualizat automat la fiecare interval de o oră, însă trebuie oprit cu câteva ore înainte de încheierea procesului de votare pentru a evita influențarea rezultatului final. Scopul graficului este să asiste utilizatorul în procesul de luare a deciziilor referitoare la candidatul preferat. Pentru a ilustra evoluția acestui grafic, au fost integrate o funcție pentru generarea aleatoare a voturilor și una pentru resetarea acestora.
Prin funcția de generare a voturilor, sunt selectați aleator utilizatorii care vor vota și opțiunile lor de vot. Acest proces a fost implementat prin introducerea într-un vector a tuturor ID-urilor utilizatorilor care nu au votat încă.

```
$sql="SELECT id FROM utilizatori WHERE votat=0";
$arrUtilizatori = $db->fetchCol($sql,'id');
$nrUtilizatori = count($arrUtilizatori);
```

Următorul pas implică determinarea lungimii acestui vector, care va fi utilizată ca număr total de utilizatori. Apoi, într-o buclă repetitivă, este generat un număr aleatoriu la fiecare iterație, cu valori între 0 și numărul total de utilizatori. Utilizatorul corespunzător poziției generate aleator este adăugat într-un alt vector, care reprezintă 20% din lungimea primului vector și conține utilizatorii care vor vota în acel moment.

```
$nrUtilizatoriDeVotat =$nrUtilizatori * $procent / 100;
$arrUtilizatoriCareVorVotaAcum = array();
while (count($arrUtilizatoriCareVorVotaAcum) <= $nrUtilizatoriDeVotat) {
    $pozitie = mt_rand(0, $nrUtilizatori-1);
    if (isset($arrUtilizatoriCareVorVotaAcum[$pozitie])) {
        continue;
    }
    $arrUtilizatoriCareVorVotaAcum[$pozitie] = $arrUtilizatori[$pozitie];
}
```

În continuare, pentru a determina candidații pentru care vor vota acești utilizatori, se aplică un proces similar. Se realizează o interogare a bazei de date pentru a obține ID-urile tuturor candidaților și se stochează într-un vector. Pentru fiecare utilizator care votează în acel moment, se generează un număr aleator care indică poziția candidatului în vectorul de candidați. Apoi, tabelele din baza de date sunt actualizate cu noile valori conform secvenței de cod de mai jos:

```
foreach($arrUtilizatoriCareVorVotaAcum as $idUtilizator)
 {
        $pozitie = mt_rand(0, $nrCandidati-1);
        $utilizator = new Utilizator();
        $utilizator->setId($idUtilizator)
                   ->setVotat(1)
                   ->setVot($arrCandidati[$pozitie]);
        $userSQL->updateVot($utilizator);

        $candidatOBJ = $candSQL->getCandidat($arrCandidati[$pozitie]);
        $candidatOBJ->setVoturi($candidatOBJ->getVoturi()+1);
    $candSQL->updateVot($candidatOBJ);
 }
```

```
foreach ( $candidati as $candidat )
{ ?>
   <div class="lista-candidat" id="candidat_'<?php echo $candidat->getId();?>">
      <img src="<?php echo $candidat->getImagine();?>" width="200" height="200"  />
      <p><?php echo $candidat->getFullName();?></p>
      <p><?php echo $candidat->getFunctie();?></p>
      <button title="test">Mesaj</button>
      <div class="mesaje" style="display:none;" id="msj_candidat_' . $candidat->getId() . '">
        <?php echo $candidat->getMesaj();?>
      </div>
      <p><a href="vote.php?id=<?php echo $candidat->getId()?>">Voteaza</a></p>
   </div>
```

Funcția de resetare are rolul de a restabili toate câmpurile care țin de numărarea voturilor din tabelele de utilizatori și candidați, inițializându-le cu valoarea zero. În continuare, utilizatorul va naviga către pagina de listare a candidaților, unde va avea acces la mesajele de campanie ale acestora, precum și la imaginile lor, pentru a-i identifica mai ușor. Utilizatorul poate vizualiza sloganul unui candidat făcând clic pe butonul "Mesaj", iar textul va fi afișat sub acesta. Prin reapăsarea butonului, mesajul va fi ascuns din nou. Funcționalitatea grafică este realizată cu ajutorul funcției slideToggle din biblioteca JavaScript, JqueryUI, așa cum este prezentat în secvența de cod de mai jos.
Pentru a-și înregistra votul, alegătorul trebuie să apese butonul "Votează" situat sub candidatul preferat. Acesta este ultimul pas necesar pentru a vota online.

Figura 15. Lista de candidați.
Sursa https://elections.europa.eu/ro/how-to-vote/ro/

În funcție de setările tipului de vot, alegătorul poate acorda un vot unic sau unul convertibil. Verificarea se realizează în funcție de câmpul de semnalizare stocat în baza de date înregistrată

pentru fiecare utilizator. Acest semnalizator poate avea valori de zero sau unu (FALSE sau TRUE). În cazul în care semnalizatorul este setat pe zero, aplicația înregistrează opțiunea alegătorului, afișează mesajul din figura 22 și actualizează semnalizatorul la valoarea 1. În cazul în care semnalizatorul are deja valoarea 1, se verifică tipul de vot selectat pentru acel eveniment și se ia o decizie în consecință. Pentru votul convertibil, sistemul ignoră semnalizatorul și reține ultimul vot selectat de utilizator, însă se asigură că se scade un vot de la candidatul anterior votat. În cazul în care tipul de vot este vot unic și semnalizatorul este deja setat pe 1, aplicația nu va înregistra noua preferință a utilizatorului și va genera mesajul următor.

La încheierea perioadei de votare, sistemul permite accesul la pagina de rezultate finale. Astfel, alegătorul poate vizualiza rezultatele imediat după încheierea votului, fără a fi necesară o așteptare suplimentară pentru numărătoare. Această abordare sporește eficiența aplicației. Pe pagina de rezultate finale, se găsește un grafic similar cu cel pentru rezultatele intermediare, însă acesta include toate voturile și afișează procentajul obținut de fiecare candidat. Procentajul este relevant în situațiile în care votul se bazează pe o metodă proporțională care implică selecția mai multor învingători.

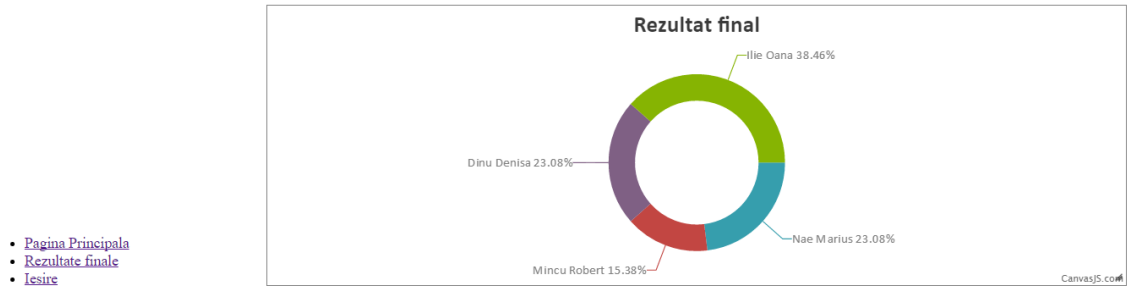

Figura 16. Grafic rezultat final.
Sursa https://elections.europa.eu/ro/how-to-vote/ro/

Interfața grafică servește atât utilizatorului, prin funcțiile descrise anterior, cât și administratorului, prin opțiunile de configurare. În plus, un alt rol al interfeței grafice pentru administrator constă în restricționarea accesului acestuia la datele personale ale utilizatorilor, contribuind la transparență și integritatea sistemului. În faza de administrare, se implică introducerea informațiilor referitoare la organizarea votului, inclusiv numele evenimentului, tipul de vot acceptat și intervalul de timp în care acesta are loc. Administratorul joacă un rol central în această etapă, având acces la diverse funcționalități precum ștergerea, editarea sau adăugarea de utilizatori și candidați, contribuind astfel la buna funcționare a sistemului.

Pasul inițial pe care trebuie să-l efectueze un administrator constă în configurarea sistemului, care poate fi realizată prin accesarea paginii de Setări din interfața de administrare. După cum se poate observa și în figura 23, pagina de configurare include un formular prin care informațiile sunt transmise pentru a fi stocate în baza de date. Pentru a ușura introducerea datei și orei specificate în formatul DATETIME al bazei de date, a fost utilizată funcția datePicker() din biblioteca JQueryUI. Dorind să ofere o experiență plăcută în utilizarea sistemului, s-a implementat și funcția tooltip(), care furnizează o descriere a câmpurilor respective atunci când utilizatorul își poziționează cursorul deasupra lor.

Figura 17 a și b. Pagina de configurare.
Sursa : https://elections.europa.eu/ro/how-to-vote/ro/

Pagina principală servește ca loc în care administratorul poate vizualiza lista inițială de candidați, care este inițial goală. Prin intermediul meniului de administrare situat în partea stângă a paginii, acesta poate accesa pagina de adăugare a candidaților, permițându-i să populeze lista de pe pagina principală.

Figura 18. Pagina de configurare.
Sursa : https://elections.europa.eu/ro/how-to-vote/ro/

În pagina de adăugare a candidaților, administratorul poate încărca fotografia fiecărui candidat. Funcția care gestionează acest proces nu stochează imaginea în baza de date, ci o transferă în directorul /images din cadrul proiectului, apoi salvează în baza de date calea absolută către respectivul fișier. Pe lista recent populată cu ajutorul paginii de adăugare a candidaților, utilizatorul poate efectua acțiuni de modificare sau ștergere a candidaților. Pentru a șterge un candidat din această listă, se utilizează un apel AJAX (Asynchronous JavaScript And XML), facilitând astfel actualizarea tabelului fără a fi necesară reîncărcarea întregii pagini. Apelul AJAX din secvența de cod de mai jos oferă avantajul comunicării asincrone cu serverul și nu blochează firul principal de execuție al aplicației.

```
<script type = "text/javascript" language = "javascript">
    $(document).ready(function() {
        $('a.ajax-sterge').click(function(event) {
            event.preventDefault();
            var candidatID = $(this).data('id');
            $.ajax(this.href, {
            dataType: 'json',
            success: function(data) {
                console.log(data);
                if (data.result) {
                    $('#candidat_' + candidatID).remove();
                } else if (data.message) {
                    alert(data.message);
                } else {
                    alert('Eroare generala');
                }
            },
            error: function() {
                alert('O eroare de conexiune');
```

Aplicația de administrare poate efectua aceleași operațiuni și pe lista de utilizatori, care este prezentată în continuare sub formă de tabel. De această dată, însă, voturile utilizatorilor nu sunt afișate pentru a garanta caracterul secret al acestora.

Figura 19.Pagina de listare utilizatori.
Sursa: https://elections.europa.eu/ro/how-to-vote/ro/

eVoteNow este o platformă eficace și ușor de folosit pentru coordonarea și monitorizarea votului online. Cu o interfață intuitivă, atât utilizatorii cât și administratorii pot interacționa cu sistemul fără dificultăți, beneficiind de o experiență plăcută și sigură. Prin introducerea unor caracteristici esențiale cum ar fi administrarea utilizatorilor și candidaților, setarea evenimentelor de votare și prezentarea rezultatelor, eVoteNow furnizează o gestiune cuprinzătoare a întregului proces electoral. În ansamblu, eVoteNow este o platformă solidă și cuprinzătoare pentru votul online, oferind avantaje semnificative în ceea ce privește accesibilitatea, performanța și siguranța.

Concluzii

Această analiză evidențiază relevanța protejării informațiilor sensibile și a datelor în cadrul instituțiilor și agențiilor guvernamentale. Se subliniază faptul că securitatea informațiilor este crucială pentru a menține integritatea, confidențialitatea și accesibilitatea datelor în mediul guvernamental. În cadrul acestei lucrări sunt examinate diversele pericole și provocări cu care se confruntă securitatea informațiilor în Administrația Publică, printre care se numără atacurile cibernetice, riscul de pierdere a datelor și accesul neautorizat la informațiile cu caracter sensibil. Se subliniază importanța de a fi conștienți și de a gestiona aceste riscuri într-un mod proactiv. În plus, sunt propuse și examinate politici și măsuri specifice menite să asigure protecția informațiilor în cadrul Administrației Publice.

Acestea ar putea implica introducerea standardelor de securitate, criptarea informațiilor, autentificarea utilizatorilor și implementarea unor mecanisme de control al accesului. Se recunoaște importanța factorului uman în protejarea securității informațiilor și se subliniază importanța formării și sensibilizării personalului în ceea ce privește măsurile de securitate și riscurile implicate. Pornind de la evaluarea și analiza situației prezente, lucrarea propune sugestii concrete pentru îmbunătățirea securității informațiilor în cadrul Administrației Publice. Aceste recomandări ar putea cuprinde revizuirea și actualizarea politicilor și procedurilor de securitate, investiții în tehnologii de securitate de vârf și consolidarea cooperării între diversele agenții guvernamentale.

Prin intermediul acestei lucrări se poate dezvolta o înțelegere temeinică a importanței protejării datelor și a informațiilor critice ale instituțiilor guvernamentale împotriva intruziunilor neautorizate și a atacurilor cibernetice. Prin identificarea și evaluarea riscurilor legate de securitatea informațiilor, lucrarea poate evidenția necesitatea păstrării integrității și confidențialității datelor în cadrul Administrației Publice, cu scopul de a descuraja orice încercare de alterare sau acces neautorizat. O atitudine riguroasă și eficientă în gestionarea securității informațiilor poate consolida încrederea publicului în capacitatea administrației publice de a proteja datele și informațiile personale ale acestora, consolidând astfel legitimitatea și autoritatea instituțiilor guvernamentale.

Descoperirea și punerea în aplicare a unor politici și măsuri corespunzătoare de securitate a informațiilor pot ajuta la minimizarea riscurilor de expunere la amenințări și la scăderea costurilor implicate în abordarea incidentelor de securitate. Prin garantarea integrității și accesibilității datelor, lucrarea poate evidenția necesitatea asigurării unei funcționări eficiente a instituțiilor guvernamentale, permițându-le să își desfășoare activitățile fără a fi perturbate de incidentele de securitate. Prin explorarea acestor elemente, lucrare de licență poate sublinia importanța esențială a securității informațiilor în cadrul Administrației Publice și poate juca un rol important în îmbunătățirea politicilor și practicilor din acest domeniu.

Relevanța lucrării de licență referitoare la securitatea informațiilor în Administrația Publică devine evidentă în lumina creșterii dependenței continue a instituțiilor guvernamentale de tehnologia informației și comunicațiilor (TIC), împreună cu amenințările din ce în ce mai complexe la adresa securității cibernetice. În epoca digitală, administrațiile publice acumulează, analizează și reține o cantitate semnificativă de informații sensibile, iar asigurarea securității acestor date este esențială pentru funcționarea eficientă a statului și pentru protejarea intereselor cetățenilor.

În adiție la progresele tehnologice, noile directive legislative și regulamente în domeniul protecției datelor personale, precum Regulamentul General privind Protecția Datelor (GDPR) în Uniunea Europeană, cer o atenție crescută asupra securității informațiilor în cadrul Administrației Publice. În plus, evenimentele de securitate cibernetică care afectează instituțiile guvernamentale au evidențiat fragilitatea și repercusiunile negative ale unor astfel de atacuri asupra serviciilor publice, integrității datelor și încrederii cetățenilor. Astfel, într-un mediu caracterizat de progresul rapid al tehnologiei și de amenințările în creștere din domeniul securității cibernetice, o lucrare de licență axată pe securitatea informațiilor în Administrația Publică rămâne relevantă și semnificativă, oferind posibilitatea de a analiza și de a sugera soluții pentru provocările în evoluție din acest domeniu.

Aplicația eVoteNow, destinată votului electronic, prezintă versatilitate în diversele sale utilizări: fie pentru organizarea de alegeri electorale (mai ales după optimizări), fie pentru integrarea în cadrul companiilor sau grupurilor sociale. Aceasta poate fi configurată pentru a permite votarea într-o gamă largă de domenii de interes, adaptându-se la nevoile specifice ale fiecărui context.
Prin intermediul eVoteNow, utilizatorii beneficiază de posibilitatea de a vota rapid și convenabil, indiferent de locație, necesitând doar două minute și acces la internet.

Deși necesită îmbunătățiri, aplicația a fost optimizată pentru a accesa baza de date prin implementarea unui model "Singleton", care limitează crearea mai multor instanțe ale aceleiași conexiuni. În plus, s-au implementat proceduri pentru filtrarea datelor de autentificare, astfel încât să se elimine caracterele speciale introduse de posibili atacatori. În cazul utilizării pentru procese electorale, unul dintre aspectele ce necesită îmbunătățire este securitatea. Dat fiind mediul în care operează, aplicația poate prezenta vulnerabilități în ceea ce privește transmiterea datelor către centralizare.

În afară de optimizările la nivel operațional, există oportunitatea de a extinde gama de funcționalități oferite. În prezent, eVoteNow include doar funcționalitățile de bază ale unei astfel de aplicații, fără adăugarea unor opțiuni avansate. Cred că progresul rapid al tehnologiei va influența semnificativ stilul de viață al oamenilor. În era digitală actuală, schimbările sunt evidente și sugerează că în viitorul apropiat, astfel de sisteme vor deveni din ce în ce mai relevante și mai căutate. Având aceste aspecte în vedere, cred că eVoteNow reprezintă o primă etapă către un sistem de vot modern, civilizat și, mai presus de toate, de încredere și sigur.

Referințe bibliografice

[1] Manda Cezar Corneliu, Smart Cities, București: Editura Universitară, 2021.

[2] Ștefanescu Alexandra, „Code for Romania," 22 Decembrie 2020. [Interactiv]. Available: https://www.code4.ro/ro/blog/securitatea-sistemelor-de-vot-electronic. [Accesat 16 Ianuarie 2024].

[3] Popa Sorin Eugen, „SECURITATEA SISTEMELOR INFORMATICE," 2007. [Interactiv]. Available: https://cadredidactice.ub.ro/sorinpopa/files/2011/10/Curs_Securit_Sist_Inf.pdf. [Accesat 24 februarie 2024].

[4] Popa Sorin Eugen, Securitatea Sistemelor Informatice, 2007.

[5] Secretarul General(A/62/659-S/2008/39), „Asigurarea păcii și securității. Rolul Națiunilor unite în susținerea reformei sectorului de securitate," 2008.

[6] Guvernul, „Strategia națională de dezvoltare a societății informaționale".

[7] Sebastiao, „Integrating Physical and Logical Security," Dubai, 2017.

[8] „securitatea informatică," [Interactiv]. Available: http://www.securitatea-informatica.ro. [Accesat 03 Martie 2024].

[9] „Fundamental security Concepts," [Interactiv]. Available: http://cryptome.org/. [Accesat 03 Martie 2024].

[10] Baltac Vasile, Tehnologiile Informației- Noțiuni de bază, București: Andreco Educațional, 2011.

[11] Oscarson Petter, Information security fundamentals, orebro, sweden: Kluwer Academic Publisher Norwell, 2013.

[12] Țigănoaia Bogdan Dumitru, Asigurarea securității informațiilor in organizații, București: INSTITUTUL EUROPEAN, 2013.

[13] Vrabie Cătălin, Elemente de IT pentru administrație publică, București: Editura Pro Universitaria, 2023.

[14] Profiroiu Alina Georgiana, Bazele administratiei publice, București: Economică, 2010.

[15] „Pagina Oficială a Camerei Deputaților," 2023. [Interactiv]. Available: http://www.cdep.ro/,. [Accesat 05 Martie 2024].

[16] Ploeșteanu Nicolae Dragoș, Farcaș Darius Lăcătușu Vlad, Protecția datelor cu caracter personal și viața privată, București: UNIVERSUL JURIDIC, 2018.

[17] Trifan Georgiana, Grecu Elena, Comănescu Raluca, GDPR pentru afaceri. Un ghid eficient pentru companii, București: UNIVERSUL JURIDIC, 2021.

[18] Șandru Daniel Mihail, „Pandectele Române," february 2019.

[19] Irina Alexe, Legislatia privind protectia datelor in Romania, București: ROSETTI, 2018.

[20] [Interactiv]. Available: Smartcitymagazine.ro. [Accesat 18 Martie 2024].

[21] [Interactiv]. Available: https://www.certsign.ro/ro/semnatura-electronica-la-distanta-certsign-solutia-e-citizen-pentru-digitalizarea-primariei-oradea. [Accesat 19 Martie 2024].

[22] [Interactiv]. Available: https://dnsc.ro/vezi/document/cybersecurity-provocari-perspective-educatie. [Accesat 21 Martie 2024].

[23] Ion Alexandru, Securitatea cibernetică, București: Ideea Europeana, 2023.

[24] [Interactiv]. Available: Contributors.ro. [Accesat 23 Martie 2024].

[25] Alina Nechita Vingan, Comunicarea digitală. Provocări și perspective, București: EIKON, 2014.

[26] [Interactiv]. Available: https://www.roaep.ro/prezentare/despre-noi/. [Accesat 05 Aprilie 2024].

[27] [Interactiv]. Available: http://apti.ro/votul-electronic-in-lume/. [Accesat 09 Aprilie 2024].

[28] [Interactiv]. Available: https://www.freiheit.org/ro/romania-and-republic-moldova/votul-online-realitatea-timpurilor-noastre. [Accesat 21 Aprilie 2024].

[29] [Interactiv]. Available: http://estonia.eu/about-estonia/economy-a-it/e-voting.html/. [Accesat 12 Aprilie 2024].

[30] Tammearu Kevin, Stancu Ana-Maria, Balmoș Alexandru, Guzun Victor, Votul Online-Realitatea timpurilor noastre, București, 2020.

[31] [Interactiv]. Available: http://www.ucl.ac.uk/~ucahhwi/dhondt.pdf/. [Accesat 16 Aprilie 2024].

[32] Schifreen Robert, How to create Web sites and applications with HTML, CSS, Javascript, PHP and MySQL, UK: Oakworth Business Publishing Ltd , 2009.

[33] Vrabie Cătălin, „Artificial Intelligence Promises to Public Organizations and Smart Cities.," *Digital Transformation. Lecture Notes in Business Information Processing,* vol. 465, 8 12 2022.

[34] Baltac Vasile, „Smart cities—A view of societal aspects," *Smart Cities,* vol. 2, nr. 4, 2019.

[35] Vrabie Cătălin, „E-Government 3.0: An AI Model to Use for Enhanced Local Democracies," *Sustainability,* 2023.

[36] Tegmark Max, Life 3.0: Being Human in the Age of Artificial Intelligence, Penguin books, 2017.

[37] [Interactiv]. Available: http://www.securitatea-informatica.ro.

[38] [Interactiv]. Available: https://www.roaep.ro/prezentare/despre-noi/. [Accesat 20 04 2024].

[39] Tammearu Kevin, Stancu Ana-Maria, Balmoș Alexandru, Guzun Victor, Votul Online-Realitatea timpurilor noastre, București, 2020.