Școala Națională de Studii Politice și Administrative
Facultatea de Administrație Publică

Securitatea cibernetică în administrația publică din România: Provocări și măsuri de protecție în contextul digitalizări

- lucrare de licență, Facultatea de Administrație Publică -

Coordonator

Conf. Univ. Dr. Cătălin VRABIE

Absolventă

Ciucă Mara Teodora

București
2025

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 declarația anti-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

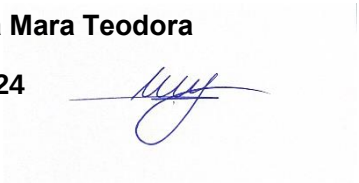
1. Cunosc că plagiatul este o formă de furt intelectual și declar pe proprie răspundere că această lucrare este rezultatul propriului meu efort intelectual și creativ și că am citat corect și complet toate informațiile preluate din alte surse bibliografice (de ex: cărți, articole, clipuri audio-video,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

2. Declar că nu am permis și nu voi permite nimănui 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: Ciucă Mara Teodora

Data și semnătura: 23.12.2024



Cuprins

Abstract

Digitalizarea administrației publice din România scoate la iveală în prim-plan amenințările legate de securitatea cibernetică, în special în cazul unor instituții centrale precum Parlamentul României. Această lucrare analizează vulnerabilitățile cibernetice specifice în acest context, evidențiind importanța unei infrastructuri IT moderne și a unor măsuri adecvate de protecție. În contextual actual, lipsa educației digitale a personalului și resursele insuficiente de securitate sunt factorii decisivi atunci când vine vorba de funcționarea optimă a instituției. Utilizând o combinație de metode, printre care analiza documentară a legislației, studii de caz si analiza datelor colectate de la funționarii publici care activează în domeniu, putem obține rezultate care subliniază necesitatea implementării unor soluții avansate, precum sisteme moderne de detecție și programe de formare continuă pentru personal. Totodată, lucrarea propune modernizarea cadrului legislativ pentru a sprijini o abordare integrată a securității cibernetice, adaptată nevoilor specifice ale Parlamentului României. Datorită analizei aprofundate a provocărilor și soluțiilor identificate, această lucrare oferă o contribuție semnificativă la înțelegerea și gestionarea riscurilor cibernetice din administrația publică. În plus, subliniază importanța capacității de adaptare digitală pentru protecția infrastructurilor critice ale statului și pentru îmbunătățirea interacțiunii dintre instituții și cetățeni. Lucrarea sprijină dezvoltarea unui cadru teoretic și practic de valoare, adresat atât factorilor de decizie, cât și specialiștilor în securitate informațională. Se evidențiază necesitatea unei colaborări între sectorul public și cel privat pentru implementarea unor măsuri eficiente de securitate. Investițiile în educație digitală și conștientizarea publicului cu privire la amenințările cibernetice reprezintă pași esențiali pentru asigurarea unei tranziții line spre digitalizarea completa a administrației publice..

Cuvinte cheie: atacuri cibernetice, Securitate IT în România, protecția datelor în sectorul public, riscuri cibernetice, inovație digitală în guvernare.

Introducere

Într-o lume dominată de interconectivitate digitală și dependență de tehnologie, administrația publică din România se confruntă cu o provocare majoră: protejarea infrastructurilor digitale esențiale împotriva amenințărilor cibernetice tot mai complexe. Procesul accelerat de transformare digitală, impulsionat de nevoia de modernizare a serviciilor publice și de optimizarea proceselor administrative, a amplificat riscurile la care sunt expuse sistemele informatice guvernamentale. Aceste vulnerabilități nu sunt doar ipotetice, ci pot genera consecințe grave, precum întreruperea funcționării instituțiilor, erodarea încrederii cetățenilor și compromiterea securității naționale [1]. Adoptarea tehnologiilor avansate, cum ar fi platformele online pentru interacțiunea cu cetățenii, stocarea în cloud sau soluțiile bazate pe inteligență artificială, introduce noi puncte slabe care pot fi exploatate de actori rău-intenționați, de la hackeri independenți la organizații infracționale sau entități statale ostile [2], [3].

Atacurile cibernetice îndreptate împotriva sectorului public pot varia de la tentative simple, precum e-mailurile de tip phishing, la operațiuni sofisticate care vizează furtul de date confidențiale, blocarea serviciilor esențiale sau compromiterea infrastructurilor critice, cum ar fi rețelele de energie, transport sau sănătate [4]. Un astfel de atac asupra unei rețele critice ar putea perturba funcționarea spitalelor, a sistemelor de transport public sau a comunicațiilor, generând efecte în lanț cu impact semnificativ asupra societății și economiei [9]. Studiile evidențiază că un incident cibernetic major poate provoca pierderi financiare substanțiale, scurgeri de date personale și scăderea încrederii în instituțiile publice, subliniind necesitatea unor măsuri de protecție eficiente [1]. Dezvoltarea unor strategii proactive, bazate pe detectarea timpurie a amenințărilor, formarea continuă a personalului și implementarea unor politici de securitate robuste, este indispensabilă pentru consolidarea rezilienței digitale a administrației publice [5].

Această cercetare își demonstrează relevanța prin identificarea soluțiilor necesare pentru prevenirea și gestionarea incidentelor de securitate cibernetică. Investițiile în educația digitală a funcționarilor publici, în special în administrațiile locale unde competențele digitale sunt adesea limitate, sunt cruciale pentru reducerea erorilor umane, care reprezintă o cauză frecventă a breșelor de securitate [2]. Colaborarea cu sectorul privat poate facilita accesul la tehnologii de ultimă generație și expertiză specializată, îmbunătățind capacitatea de răspuns rapid la incidente cibernetice [6]. De asemenea, alinierea la standardele europene, cum ar fi Directiva NIS 2, oferă un cadru clar pentru monitorizarea și protejarea infrastructurilor critice, contribuind la

armonizarea eforturilor naționale [7]. Aceste măsuri sunt esențiale pentru a preveni efectele devastatoare ale atacurilor cibernetice și pentru a asigura continuitatea serviciilor publice.

Din perspectiva instituțiilor publice, această analiză propune o evaluare detaliată a riscurilor cibernetice și soluții practice pentru depășirea acestora. Identificarea vulnerabilităților sistemelor IT, implementarea mecanismelor proactive de apărare și elaborarea unor politici de securitate bine structurate permit administrației publice să devină mai rezilientă în fața provocărilor digitale [8]. Modernizarea infrastructurii IT și formarea continuă a personalului în domeniul securității cibernetice pot reduce semnificativ riscul incidentelor, în timp ce colaborarea intersectorială și adoptarea standardelor internaționale contribuie la crearea unui ecosistem digital guvernamental mai sigur [9]. Prin aceste măsuri, administrația publică poate răspunde eficient amenințărilor digitale, protejând atât interesele cetățenilor, cât și stabilitatea instituțională.

Scopul acestei cercetări este de a oferi un cadru cuprinzător pentru înțelegerea și abordarea provocărilor securității cibernetice în contextul transformării digitale a administrației publice din România. Prin analiza riscurilor actuale, identificarea lacunelor din infrastructura IT și propunerea unor soluții adaptate, studiul contribuie la dezvoltarea unor politici publice care să asigure protecția datelor și funcționarea neîntreruptă a serviciilor esențiale [6]. Într-un peisaj global în care atacurile cibernetice devin tot mai sofisticate și implică actori diverși, de la infractori cibernetici la entități statale, securitatea cibernetică reprezintă o prioritate strategică pentru România. Protejarea infrastructurilor critice devine o responsabilitate fundamentală a administrației publice, esențială pentru stabilitatea socio-economică și pentru construirea unei societăți digitale sigure, capabile să facă față provocărilor viitorului [5], [7].

Ipotezele de cercetare

- Digitalizarea administrației publice facilitează creșterea eficienței operaționale, însă amplifică riscurile asociate securității cibernetice. Se consideră că, deși digitalizarea generează avantaje semnificative în funcționarea instituțiilor, ea implică și vulnerabilități sporite, al căror nivel depinde de măsurile de protecție implementate de fiecare autoritate publică.
- Educația și conștientizarea în materie de securitate cibernetică reduc vulnerabilitățile din cadrul organizațiilor. Implementarea unor programe de formare continuă pentru angajații instituțiilor publice contribuie în mod semnificativ la diminuarea riscurilor asociate comportamentului uman în mediul digital.
- Adoptarea tehnologiilor inovatoare și a soluțiilor bazate pe inteligență artificială asigură o protecție cibernetică completă în administrația publică. Se consideră că tehnologiile de ultimă generație pot elimina cele mai multe vulnerabilități cibernetice. Totuși, cercetările vor demonstra dacă această ipoteză este realistă sau dacă, în anumite situații, inovația tehnologică este insuficientă pentru a contracara atacurile avansate

Obiective

- Evaluarea principalelor amenințări cibernetice cu care se confruntă administrația publică.
- Identificarea vulnerabilităților din infrastructura IT utilizată în sectorul public.
- Analiza tipologiei și frecvenței atacurilor cibernetice îndreptate asupra instituțiilor publice.
- Investigarea impactului acestor amenințări asupra funcționării serviciilor publice esențiale.
- Determinarea nivelului de conformitate a sistemelor IT cu standardele internaționale de securitate cibernetică.

Metodologia de cercetare

Pentru a oferi o analiză detaliată și bine fundamentată asupra problematicii și soluțiilor din domeniul securității cibernetice în administrația publică din România, am utilizat o metodologie mixtă, combinând abordări teoretice cu investigații empirice. Această strategie a permis explorarea aprofundată a fundamentelor conceptuale și legislative, precum și obținerea de date

primare relevante din practica instituțiilor publice și din percepțiile populației, oferind astfel o perspectivă integrată asupra subiectului.

Cercetarea a început cu o analiză teoretică menită să clarifice conceptele esențiale și să contureze contextul securității cibernetice. Au fost definite noțiuni precum „securitate cibernetică", „amenințări cibernetice", „vulnerabilități" și „măsuri de protecție", stabilind un cadru clar de referință. Pentru aceasta, am consultat surse variate, incluzând studii și articole academice naționale și internaționale care abordează securitatea cibernetică în sectorul public, cu accent pe provocările specifice administrației. Au fost analizate rapoarte emise de organizații precum ENISA, CERT-RO sau companii private din domeniul IT, precum și acte normative relevante, cum ar fi Legea nr. 362/2018, care transpune Directiva NIS a Uniunii Europene, și alte reglementări europene, precum GDPR. De asemenea, am studiat strategiile și politicile de securitate cibernetică implementate de state membre ale UE, precum Estonia, Germania sau Finlanda, pentru a identifica modele de succes aplicabile în contextul românesc. Această etapă a permis înțelegerea contextului teoretic și evidențierea principalelor riscuri cibernetice, cum ar fi atacurile de tip phishing, ransomware, breșele de date sau lipsa pregătirii adecvate a personalului.

Pe lângă analiza teoretică, cercetarea empirică a avut rolul de a colecta și interpreta date primare, reflectând atât realitatea din teren, cât și percepțiile cetățenilor. Pentru aceasta, am utilizat două chestionare structurate, distribuite prin platforma Google Forms. Primul chestionar a fost adresat populației generale, având scopul de a evalua viziunea cetățenilor asupra digitalizării administrației publice și nivelul de încredere în securitatea cibernetică a instituțiilor. Acesta a inclus întrebări despre gradul de utilizare a serviciilor digitale publice, percepția asupra riscurilor cibernetice și încrederea în capacitatea instituțiilor de a proteja datele personale. Al doilea chestionar a fost adresat funcționarilor publici și responsabililor din departamentele IT sau de management al securității cibernetice din instituțiile publice românești. Acest chestionar a evaluat nivelul de pregătire profesională a personalului, inclusiv cursurile de formare urmate și competențele digitale, expunerea la riscuri cibernetice, tipurile de amenințări întâlnite, precum malware sau atacuri DDoS, și frecvența acestora. De asemenea, a investigat măsurile de protecție implementate, cum ar fi utilizarea de firewall-uri, soluții antivirus, politici de backup sau protocoale de răspuns la incidente, resursele alocate securității cibernetice, precum bugetul dedicat sau numărul de specialiști angajați, și experiențele cu incidente cibernetice, inclusiv natura acestora, impactul asupra activității instituționale și timpul de răspuns. Ambele chestionare au fost distribuite unui eșantion reprezentativ, primul către cetățeni din diverse categorii socio-demografice, iar al doilea către funcționari din ministere, primării sau agenții guvernamentale, utilizând platforma Google Forms și, în unele cazuri, interviuri directe pentru răspunsuri mai detaliate.

Pentru a ilustra impactul concret al amenințărilor cibernetice, au fost analizate studii de caz bazate pe incidente recente din administrația publică românească, selectate din surse publice, cum ar fi rapoartele CERT-RO, comunicatele de presă ale instituțiilor afectate sau documente interne publicate ulterior. Fiecare studiu de caz a examinat contextul incidentului, tipul de atac, impactul asupra instituției, cum ar fi pierderi financiare sau întreruperea serviciilor publice, răspunsul instituțional, inclusiv timpul de reacție și măsurile de remediere, precum și lecțiile învățate pentru prevenirea viitoarelor incidente. Un exemplu ar putea fi un atac ransomware asupra unui spital public, evidențiind vulnerabilitățile sistemului IT, efectele asupra pacienților și măsurile luate ulterior.

Datele colectate prin cele două chestionare au fost procesate exclusiv prin Google Forms, utilizând funcționalitățile platformei pentru a genera diagrame care să ilustreze răspunsurile. Aceste diagrame, de tip bară sau circular, au permis sintetizarea datelor, evidențiind, de exemplu, procentul cetățenilor care au încredere în securitatea serviciilor digitale publice sau procentul instituțiilor care alocă un buget redus pentru securitate cibernetică. Analiza a inclus statistici descriptive pentru a sumariza răspunsurile, precum procentaje și frecvențe, și a facilitat identificarea tiparelor, cum ar fi relația dintre pregătirea personalului și vulnerabilitatea la atacuri

cibernetice sau percepția publicului asupra digitalizării. De asemenea, au fost realizate comparații între practicile din România și cele din alte state membre UE, pentru a evidenția decalaje și oportunități de îmbunătățire.

Prin integrarea analizelor teoretice și empirice, cercetarea a oferit o imagine de ansamblu asupra stării securității cibernetice în administrația publică românească, completată de perspectiva cetățenilor asupra digitalizării. Pe baza rezultatelor, au fost formulate recomandări practice, precum intensificarea investițiilor în formarea profesională a funcționarilor, implementarea unor politici naționale coerente, adoptarea de tehnologii moderne pentru detectarea amenințărilor în timp real, consolidarea colaborării între instituțiile publice și sectorul privat din domeniul IT și creșterea încrederii cetățenilor prin campanii de informare privind securitatea datelor. Această metodologie mixtă a asigurat o abordare echilibrată, combinând rigoarea academică cu relevanța practică, și a oferit o bază solidă pentru înțelegerea și abordarea provocărilor din acest domeniu.

Capitolul 1. Introducere în digitalizarea administrației publice

Digitalizarea administrației publice reprezintă un pas crucial în modernizarea și eficientizarea proceselor administrative, având un impact profund asupra accesibilității, transparenței și calității serviciilor oferite cetățenilor. La nivel internațional, transformarea digitală a devenit o prioritate strategică, reflectată în inițiative care vizează reducerea birocrației, optimizarea interacțiunii dintre cetățeni și instituții, și consolidarea responsabilității autorităților publice. În România, adoptarea tehnologiilor digitale este esențială pentru a răspunde cerințelor Uniunii Europene și pentru a susține dezvoltarea unui sector public modern, capabil să ofere servicii eficiente și accesibile [9]. Programe precum GovITHub, lansat pentru a accelera digitalizarea administrației publice, și Strategia Națională privind Agenda Digitală pentru România subliniază angajamentul țării pentru modernizarea sistemului administrativ [10], [11]. Digitalizarea facilitează nu doar optimizarea proceselor interne, ci și crearea unui mediu propice pentru dezvoltarea orașelor inteligente, prin integrarea tehnologiilor emergente și îmbunătățirea relației cu cetățenii [12], Acest proces contribuie la alinierea României la standardele europene, promovând o administrație mai incluzivă și mai receptivă la nevoile societății .

Cu toate acestea, tranziția către o administrație digitalizată implică provocări semnificative, în special în ceea ce privește securitatea cibernetică. Infrastructurile IT ale instituțiilor publice sunt expuse constant riscurilor cibernetice, care includ atacuri de tip phishing, ransomware, breșe de date sau atacuri DDoS. Aceste amenințări pot genera consecințe grave, precum pierderi financiare, compromiterea datelor sensibile ale cetățenilor și scăderea încrederii publice în capacitatea statului de a gestiona servicii digitale sigure. De exemplu, rapoarte recente ale CERT-RO și articole din presă au evidențiat o creștere a frecvenței și sofisticării atacurilor cibernetice asupra instituțiilor publice din România, cum ar fi atacurile ransomware asupra sistemelor medicale sau atacurile asupra platformelor guvernamentale . În acest context, autoritățile române au început să prioritizeze investițiile în soluții avansate de securitate, cum ar fi sistemele de monitorizare în timp real, soluțiile de backup și restaurare, și măsurile de protecție fizică a infrastructurilor IT . De asemenea, colaborarea cu sectorul privat a devenit esențială pentru consolidarea rezilienței cibernetice, așa cum subliniază inițiativele de parteneriat public-privat în domeniul securității cibernetice [5]. Astfel, digitalizarea, deși indispensabilă pentru modernizarea administrației publice, impune o responsabilitate majoră în asigurarea securității infrastructurilor IT și a datelor, aspecte fundamentale pentru menținerea încrederii cetățenilor și pentru garantarea continuității serviciilor publice [9].

1.1. Definiții și termeni relevanți

Această secțiune definește conceptele fundamentale utilizate în procesul de digitalizare a administrației publice și în domeniul securității cibernetice. Acești termeni sunt indispensabili

pentru înțelegerea modului în care instituțiile publice adoptă tehnologiile moderne și pentru clarificarea provocărilor asociate cu protejarea datelor și a infrastructurilor digitale.

Din perspectiva administrației publice, terminologia specifică include noțiuni referitoare la modernizarea serviciilor publice, simplificarea interacțiunii dintre cetățeni și instituții și optimizarea proceselor administrative prin soluții digitale. În ceea ce privește securitatea cibernetică, conceptele cheie se axează pe măsurile destinate protejării sistemelor digitale, asigurând confidențialitatea, integritatea și disponibilitatea informațiilor gestionate de autoritățile publice.

Astfel, prezentarea acestor definiții va oferi un cadru clar și structurat pentru înțelegerea aspectelor fundamentale ale digitalizării și securității cibernetice în administrația publică, facilitând o analiză detaliată a impactului tehnologiilor emergente în acest domeniu

- Administrația publică - Sistemul de instituții și structuri guvernamentale care au rolul de a implementa politicile și legile statului, gestionând resursele publice și oferind servicii cetățenilor.
- Digitalizarea administrației publice - Transformarea proceselor administrative prin utilizarea tehnologiilor moderne pentru a îmbunătăți eficiența, transparența și accesibilitatea serviciilor guvernamentale.
- Servicii guvernamentale - Activitățile desfășurate de autoritățile publice pentru a satisface nevoile cetățenilor, precum educația, sănătatea, transportul și alte domenii de interes public.
- Birocrație - Sistemul de reguli și proceduri administrative care, adesea, poate crea întârzieri și complexitate în livrarea serviciilor publice.
- Infrastructura IT guvernamentală - Rețeaua de sisteme informatice și echipamente tehnologice care susțin activitățile guvernamentale, asigurând gestionarea și protecția datelor publice.
- Securitate cibernetică – Reprezintă totalitatea măsurilor, tehnologiilor și strategiilor utilizate pentru protejarea sistemelor informatice, a rețelelor și a datelor împotriva atacurilor, accesului neautorizat sau altor amenințări digitale. Scopul său principal este prevenirea, detectarea și răspunsul la incidente de securitate.
- Atac cibernetic – O acțiune intenționată desfășurată de o persoană sau grup de atacatori care vizează compromiterea, accesarea neautorizată, manipularea sau distrugerea datelor și sistemelor informatice. Atacurile pot varia de la phishing și ransomware la atacuri avansate asupra infrastructurilor critice.
- Vulnerabilitate cibernetică – Orice slăbiciune sau punct slab în software, hardware sau în procesele de securitate care ar putea fi exploatată de un atacator pentru a obține acces neautorizat la un sistem sau la date sensibile.
- Phishing – O tehnică frauduloasă utilizată pentru a păcăli utilizatorii să divulge informații confidențiale, cum ar fi parole sau date bancare, prin mesaje false care par autentice. Aceste atacuri sunt realizate de obicei prin e-mailuri sau site-uri web false.
- Ransomware – Un tip de atac cibernetic în care datele victimei sunt criptate de un software malițios, iar atacatorul solicită o sumă de bani (răscumpărare) pentru a debloca informațiile.
- Protecția datelor – Se referă la măsurile și politicile implementate pentru a asigura confidențialitatea, integritatea și disponibilitatea informațiilor sensibile. Aceasta include criptarea, controlul accesului și monitorizarea activităților suspecte.
- AI (Artificial Intelligence) – Inteligență Artificială: Tehnologia care permite calculatoarelor și sistemelor informatice să analizeze date, să învețe modele și să ia decizii bazate pe algoritmi avansați. În securitatea cibernetică, AI este folosită pentru detectarea amenințărilor și automatizarea răspunsurilor.
- E-guvernare – Procesul de digitalizare a serviciilor guvernamentale, prin care cetățenii și companiile pot accesa și interacționa cu administrația publică prin intermediul platformelor online. Scopul principal este creșterea eficienței, transparenței și accesibilității serviciilor publice.

- Infrastructură critică – Rețele, sisteme și servicii esențiale pentru funcționarea unui stat, cum ar fi transportul, energia, sănătatea și administrația publică. Protecția acestora împotriva atacurilor cibernetice este o prioritate națională.
- Identitate digitală – Reprezintă un set de informații digitale care identifică un individ sau o organizație în mediul online. Este utilizată pentru autentificarea și accesul securizat la servicii publice și private.
- GDRP (General Data Protection Regulation) – Regulamentul General privind Protecția Datelor: Lege adoptată de Uniunea Europeană care stabilește norme stricte privind colectarea, stocarea și prelucrarea datelor cu caracter personal.
- Zero Trust – Model de securitate cibernetică care presupune că niciun utilizator sau dispozitiv, din interiorul sau din afara rețelei, nu este de încredere în mod implicit. Accesul se acordă doar după verificări stricte și continue, indiferent de locație.
- SOC (Security Operations Center) – Centru operațional de securitate, responsabil cu monitorizarea, detectarea, analizarea și răspunsul la incidentele de securitate cibernetică într-o organizație.
- Incident de securitate cibernetică – Eveniment care afectează negativ confidențialitatea, integritatea sau disponibilitatea datelor sau sistemelor informatice, precum atacuri, scurgeri de date sau acces neautorizat.
- Threat Intelligence – Informații despre amenințările cibernetice actuale și potențiale, utilizate pentru a anticipa, preveni și răspunde la atacuri. Include tactici, tehnici și proceduri (TTPs) ale atacatorilor.
- Criptografie – Domeniu al informaticii care se ocupă cu protejarea informațiilor prin transformarea lor într-un format ininteligibil pentru persoanele neautorizate, utilizând algoritmi matematici (ex: criptare și decriptare).
- Autentificare multifactor (MFA) – Mecanism de securitate care solicită utilizatorului două sau mai multe metode de verificare a identității, de obicei o parolă și un cod primit pe telefon sau o amprentă digitală.
- Backdoor (ușă din spate) – Metodă ascunsă prin care un atacator sau un program poate ocoli procedurile obișnuite de autentificare pentru a accesa un sistem informatic fără permisiune.
- Politici de securitate – Set de reguli și proceduri implementate de o organizație pentru a asigura protecția informațiilor și a infrastructurii informatice împotriva amenințărilor cibernetice.
- Audit de securitate – Proces formal prin care se evaluează starea securității unei organizații, identificând punctele slabe, vulnerabilitățile și nivelul de conformitate cu politicile și standardele de securitate.
- Reziliență cibernetică – Capacitatea unui sistem, organizații sau infrastructuri de a rezista, răspunde și a se recupera rapid în urma unui atac cibernetic sau a unui incident de securitate.
- Cloud computing – Tehnologie care permite accesul la resurse IT (servere, stocare, aplicații) prin internet, fără a fi nevoie de infrastructură locală. Implică riscuri și măsuri specifice de securitate.
- Ciberhigienă – Practici de bază și rutine zilnice menite să protejeze utilizatorii și organizațiile de amenințările cibernetice, precum actualizarea software-ului, utilizarea de parole complexe și evitarea site-urilor suspecte.
- CERT (Computer Emergency Response Team) – Echipă specializată în răspunsul la incidente de securitate informatică, care oferă suport, coordonare și analiză în cazul unor atacuri sau probleme majore.
- DNSC (Directoratul Național de Securitate Cibernetică) – Autoritate națională din România responsabilă cu coordonarea și implementarea politicilor de securitate cibernetică, monitorizarea amenințărilor și sprijinirea instituțiilor publice și private.
- Politica de acces (Access Control Policy) – Document care definește cine are voie să acceseze ce resurse informatice și în ce condiții, pentru a preveni accesul neautorizat și scurgerile de informații.

1.2. Digitalizarea în România și transformarea administrației publice

Digitalizarea reprezintă o prioritate strategică pentru dezvoltarea durabilă a României, având ca scop modernizarea economiei, eficientizarea instituțiilor publice și îmbunătățirea calității vieții cetățenilor. Aceasta presupune integrarea tehnologiilor informaționale în toate domeniile societății – educație, sănătate, economie și administrație publică – pentru optimizarea proceselor, reducerea birocrației și facilitarea accesului la servicii. Digitalizarea nu se limitează la adoptarea tehnologiilor, ci implică și o schimbare a modului în care instituțiile și cetățenii interacționează, promovând transparența, accesibilitatea și eficiența [2], [13].

România a realizat progrese semnificative în ceea ce privește conectivitatea la internet și digitalizarea sectorului privat, însă serviciile publice digitale sunt încă într-o fază incipientă. Disparitățile regionale și lipsa unei implementări coerente a politicilor digitale reprezintă obstacole majore. Zonele rurale și orașele mici sunt adesea dezavantajate comparativ cu marile centre urbane, ceea ce accentuează decalajul digital [11],. Date recente indică faptul că fragmentarea sistemelor digitale și lipsa interoperabilității între instituții limitează eficiența serviciilor publice [8].

Pentru a aborda aceste provocări, România a elaborat strategii de transformare digitală, susținute de fonduri europene pentru perioada 2021–2027. Aceste strategii vizează crearea unei societăți digitale bazate pe inovație, interoperabilitate și incluziune socială. Planul Național de Acțiune pentru Implementarea Strategiei Naționale de Digitalizare a Administrației Publice subliniază necesitatea unei infrastructuri digitale integrate și a unor servicii accesibile pentru toți cetățenii. Obiectivul este construirea unui ecosistem digital care să răspundă nevoilor cetățenilor, indiferent de locație sau nivelul de competențe digitale.

Digitalizarea administrației publice este esențială, deoarece eficiența serviciilor guvernamentale influențează direct încrederea cetățenilor în instituții. Transformarea digitală a administrației implică utilizarea tehnologiilor IT în procesele interne (cum ar fi gestionarea documentelor sau comunicarea interinstituțională) și externe (interacțiunea cu cetățenii), pentru a simplifica procedurile, a crește transparența și a reduce timpul de răspuns. Platforme precum ghișeul.ro, care facilitează plata online a taxelor, sau Spațiul Privat Virtual (SPV), pentru depunerea electronică a documentelor, reprezintă pași importanți spre o administrație modernă. Cu toate acestea, dependența de procese manuale și lipsa integrării sistemelor informatice între instituții încetinesc progresul [14].

O provocare majoră o reprezintă lipsa competențelor digitale în rândul funcționarilor publici și rezistența la schimbare a culturii organizaționale. Aceste aspecte limitează adoptarea tehnologiilor avansate, precum cloud computing, automatizarea robotică a proceselor (RPA) sau inteligența artificială (AI), care ar putea optimiza analiza datelor, luarea deciziilor administrative și gestionarea resurselor [51]. De exemplu, AI poate anticipa blocajele administrative, poate optimiza fluxurile de lucru sau poate personaliza serviciile publice în funcție de nevoile cetățenilor.

România se situează în continuare în coada clasamentelor europene privind furnizarea de servicii publice digitale, din cauza lipsei interoperabilității și a fragmentării soluțiilor digitale existente [10],. Pentru a accelera tranziția spre o administrație digitală eficientă, este necesară o abordare integrată, care să includă:

- Standardizarea tehnică și legislativă: Crearea unui cadru unitar pentru compatibilitatea sistemelor IT ale instituțiilor publice, facilitând schimbul de date în timp real [8],.
- Dezvoltarea unei infrastructuri digitale unificate: Investițiile în centre de date moderne și soluții cloud pot asigura securitatea și accesibilitatea datelor [11],.

- Formarea continuă a funcționarilor publici: Programele de instruire axate pe competențe digitale sunt esențiale pentru a crește capacitatea instituțiilor de a utiliza tehnologiile moderne.
- Promovarea unei culturi organizaționale orientate spre inovație: Încurajarea adoptării noilor tehnologii și reducerea rezistenței la schimbare sunt cruciale pentru succesul digitalizării [14].

În plus, utilizarea inteligenței artificiale și a analizei predictive poate transforma administrația publică, permițând identificarea proactivă a blocajelor și alocarea eficientă a resurselor. Securitatea cibernetică este, de asemenea, o prioritate, având în vedere creșterea atacurilor asupra infrastructurilor publice, [15]. Implementarea unor soluții robuste de securitate, conforme cu Directiva NIS2 a Uniunii Europene, este esențială pentru protejarea datelor și menținerea încrederii cetățenilor. Prin valorificarea oportunităților oferite de tehnologiile moderne și prin soluționarea provocărilor actuale, România poate construi o administrație publică eficientă, transparentă și centrată pe cetățean, contribuind astfel la dezvoltarea sustenabilă a societății [13].

Modernizarea administrației publice din România prin digitalizare este esențială pentru creșterea eficienței și accesibilității serviciilor, însă întâmpină provocări precum infrastructura tehnologică limitată și lipsa competențelor digitale adecvate. Coordonată de Ministerul Cercetării, Inovării și Digitalizării (MCID), Strategia Națională de Cercetare, Inovare și Specializare Inteligentă (SNCISI) facilitează adoptarea tehnologiilor digitale prin colaborarea între instituțiile publice și sectorul privat, adresând nevoile economice și sociale ale țării. MCID gestionează fondurile pentru cercetare și inovare, susținând proiecte digitale prin inițiative precum Programul Operațional de Creștere Inteligentă, Digitalizare și Instrumente Financiare 2022-2027. La nivel local, Agențiile pentru Dezvoltare Regională (ADR) contribuie prin strategii de specializare inteligentă (RIS3), care planifică dezvoltarea regională și alocă resurse pentru integrarea tehnologiilor în administrațiile publice.

Din 2016, România a intensificat eforturile de digitalizare, concentrându-se pe integrarea inteligenței artificiale (AI) în procesele administrative [16]. Strategia Națională pentru Dezvoltarea Centrelor de Inovare Digitală (SNDCIDR) 2024-2027, elaborată de MCID în parteneriat cu Universitatea Tehnică din Cluj-Napoca, promovează crearea unei rețele de Centre de Inovare Digitală (CID) pentru a sprijini modernizarea instituțiilor publice și a sectorului industrial [17]. Aceste centre sunt vitale pentru a contracara poziția slabă a României în clasamentele globale ale digitalizării, evidențiată în timpul pandemiei prin dificultățile tranziției către învățământul online, care au afectat în special comunitățile defavorizate [18]. Colaborarea între autoritățile centrale și locale este crucială pentru a depăși aceste obstacole [19].

Strategia Națională privind Agenda Digitală pentru România 2020 stabilește direcții prioritare, precum e-guvernarea, securitatea cibernetică, tehnologiile cloud, educația digitală, sănătatea, incluziunea socială și extinderea infrastructurii de internet de mare viteză [13]. Aceste inițiative urmăresc reducerea birocrației, optimizarea costurilor și accesul facil al cetățenilor la servicii online, cum ar fi plata taxelor, depunerea cererilor sau obținerea documentelor oficiale [20]. Digitalizarea internă a instituțiilor, prin sisteme de arhivare electronică și monitorizare automată, permite decizii mai informate și fluxuri administrative mai eficiente [20]. Aceste măsuri contribuie la o administrație publică mai transparentă și mai orientată către nevoile cetățenilor [19].

Adoptarea tehnologiilor digitale la nivel local facilitează modernizarea serviciilor, precum gestionarea inteligentă a deșeurilor, iluminatul public automatizat sau parcările digitalizate, îmbunătățind calitatea vieții [18]. Publicarea informațiilor de interes public în format digital și crearea unor platforme accesibile reduc eforturile administrative și întăresc încrederea cetățenilor în instituții [19]. Formarea continuă a funcționarilor publici în competențe digitale și dezvoltarea sistemelor de identificare electronică sunt esențiale pentru succesul digitalizării [18]. Investițiile necesare, estimate la peste 3,9 miliarde de euro, ar putea crește PIB-ul cu 13%, genera 11% mai

multe locuri de muncă și reduce costurile administrative cu 12%, conform proiecțiilor bazate pe modele internaționale [13].

Obiectivul acestor strategii este de a transforma administrația publică românească într-un sistem modern, eficient și accesibil, adaptat cerințelor societății digitale [19]. Prin investiții în infrastructură IT, cercetare în AI și consolidarea rețelei CID, România își propune să diminueze decalajul digital și să promoveze dezvoltarea sustenabilă [16]. Realizarea acestor obiective necesită o colaborare intensă între autoritățile centrale, locale și sectorul privat, alături de programe susținute de educație digitală, pentru a poziționa administrația publică ca un catalizator al progresului național [20].

1.3. Importanța securității cibernetice în administrația publică

Securitatea cibernetică reprezintă un element esențial pentru protecția infrastructurilor digitale ale administrației publice, având un impact semnificativ asupra funcționării guvernelor și încrederii cetățenilor. Atacurile cibernetice pot duce la pierderi economice substanțiale și la daune reputaționale considerabile pentru instituțiile guvernamentale. De exemplu, atacurile de tip ransomware au devenit tot mai frecvente și complexe în ultimele decenii, ceea ce a determinat guvernele să investească masiv în soluții de protecție și recuperare rapidă a datelor [3].

În România, securitatea cibernetică trebuie să devină o prioritate strategică, având în vedere provocările actuale în domeniul tehnologic. Printre măsurile necesare pentru protejarea infrastructurilor IT se numără implementarea unor soluții avansate de detecție a amenințărilor. Acestea pot preveni accesul neautorizat la date sensibile și pot facilita identificarea rapidă a potențialelor atacuri, contribuind astfel la reducerea riscurilor [6].

De asemenea, crearea unor echipe de răspuns rapid la incidente cibernetice este crucială pentru gestionarea eficientă a situațiilor de urgență. În cazul unui atac, aceste echipe pot interveni prompt pentru a minimiza daunele și pentru a restabili serviciile esențiale [3]. În paralel, dezvoltarea unui cadru legislativ care să răspundă noilor provocări digitale este vitală pentru a asigura protecția datelor și respectarea reglementărilor internaționale [5].

Un alt aspect esențial este educația digitală și conștientizarea angajaților asupra riscurilor cibernetice. Mulți dintre angajații administrației publice nu dispun de suficientă pregătire în ceea ce privește utilizarea tehnologiilor de protecție și recunoașterea amenințărilor digitale. Investițiile în formarea acestora pot reduce semnificativ riscurile legate de atacurile de tip phishing, malware sau inginerie socială [3].

În acest context, se evidențiază importanța aplicării inteligenței artificiale (AI) pentru supravegherea și prevenirea atacurilor cibernetice, subliniind rolul esențial al acesteia în protejarea sistemelor informatice. AI are capacitatea de a detecta amenințările într-un stadiu incipient și de a răspunde rapid în caz de atac, asigurând astfel o protecție mult mai eficientă față de soluțiile tradiționale [6]. Prin implementarea acestei tehnologii, instituțiile guvernamentale pot asigura o securitate îmbunătățită, reducând în același timp costurile de operare și riscurile asociate cu incidentele cibernetice. Aceste măsuri proactive sunt esențiale pentru dezvoltarea unei administrații publice sigure, eficiente și reziliente în fața amenințărilor cibernetice tot mai sofisticate.

1.3.1. Dimensiuni complementare ale securității cibernetice în administrația publică

Securitatea cibernetică reprezintă un pilon esențial în modernizarea și eficientizarea administrației publice, mai ales în contextul transformării digitale accelerate. Pentru a răspunde provocărilor actuale, este necesară o abordare multidimensională care să integreze pregătirea umană, adoptarea

tehnologiilor avansate, colaborarea intersectorială și protejarea infrastructurilor critice. Un factor-cheie în asigurarea securității cibernetice este formarea continuă a personalului din administrația publică. Lipsa competențelor digitale rămâne o problemă semnificativă, în special în cadrul autorităților locale, unde cunoștințele despre protecția datelor, gestionarea platformelor digitale și prevenirea atacurilor informatice sunt adesea limitate. Angajații trebuie să fie instruiți periodic pentru a înțelege și aplica principiile de igienă digitală, cum ar fi utilizarea parolelor sigure, recunoașterea e-mailurilor de tip phishing și gestionarea corectă a datelor sensibile. Programele de formare trebuie să includă module dedicate identificării și contracarării amenințărilor cibernetice, precum ransomware-ul sau atacurile de tip „inginerie socială". Prin investiții în educația digitală a angajaților, instituțiile publice pot reduce vulnerabilitățile cauzate de erori umane, care reprezintă una dintre principalele cauze ale incidentelor de securitate [21].

În paralel, inteligența artificială (AI) joacă un rol tot mai important în optimizarea proceselor administrative și în consolidarea securității cibernetice. Tehnologiile bazate pe AI, precum sistemele de automatizare a procesării cererilor, analiza predictivă a datelor și detectarea automată a anomaliilor, permit instituțiilor publice să își crească eficiența operațională și să identifice rapid riscurile cibernetice. De exemplu, algoritmii de învățare automată pot detecta tentative de fraudă sau atacuri informatice prin analiza în timp real a tiparelor de comportament. Totuși, utilizarea AI în administrația publică necesită o guvernanță riguroasă pentru a asigura transparența deciziilor automate și responsabilitatea în gestionarea datelor. Lipsa unor politici clare poate duce la riscuri etice, precum discriminarea algoritmică sau utilizarea necorespunzătoare a datelor personale. Astfel, implementarea AI trebuie să fie însoțită de mecanisme de control și de standarde etice bine definite [22]

Colaborarea dintre sectorul public și cel privat reprezintă o altă dimensiune esențială pentru întărirea securității cibernetice. Parteneriatele public–private, demonstrate ca fiind eficiente în statele membre ale Uniunii Europene, facilitează accesul instituțiilor publice la expertiză tehnică, tehnologii avansate și resurse umane specializate din sectorul privat. În România, dezvoltarea unor astfel de parteneriate ar putea sprijini funcționarea eficientă a centrelor de răspuns la incidente de securitate cibernetică (CERT), prin accesul la infrastructură modernă și la soluții inovatoare. Companiile private pot oferi tehnologii de ultimă generație pentru monitorizarea rețelelor sau pentru gestionarea crizelor cauzate de atacuri cibernetice, contribuind la schimbul de bune practici și la alinierea la standardele internaționale [23].

Nu în ultimul rând, infrastructurile critice, precum rețelele energetice, sistemele de transport, comunicațiile sau serviciile de sănătate, reprezintă ținte prioritare pentru atacurile cibernetice datorită interconectivității lor și impactului major pe care o breșă l-ar putea avea asupra societății și economiei. O singură vulnerabilitate într-un sistem critic poate genera efecte în lanț, perturbând funcționarea altor sectoare vitale. De exemplu, un atac asupra rețelei energetice ar putea afecta spitalele, transportul public sau sistemele de comunicații. Pentru a preveni astfel de scenarii, este necesară o strategie națională integrată care să includă standarde stricte de securitate, monitorizare continuă și planuri de răspuns rapid la incidente. Alinierea la reglementările și recomandările europene, cum ar fi Directiva NIS 2, este crucială pentru armonizarea eforturilor de protejare a infrastructurilor critice și pentru consolidarea rezilienței naționale [19].

Securitatea cibernetică în administrația publică necesită, așadar, o abordare holistică, care să combine pregătirea umană, utilizarea responsabilă a tehnologiilor avansate, colaborarea intersectorială și protejarea infrastructurilor critice. Prin investiții în educația digitală a angajaților, adoptarea tehnologiilor AI cu o guvernanță adecvată, dezvoltarea parteneriatelor public–private și securizarea sistemelor esențiale, administrația publică din România poate răspunde mai eficient provocărilor cibernetice actuale, contribuind la crearea unui mediu administrativ mai sigur și mai rezilient.

1.4. *Studii de caz privind atacurile cibernetice asupra administrației publice*

Pentru a înțelege mai bine impactul atacurilor cibernetice asupra administrației publice, este util să analizăm câteva cazuri relevante la nivel internațional și național. Studierea acestor exemple oferă o perspectivă concretă asupra vulnerabilităților infrastructurilor digitale utilizate de instituțiile guvernamentale, precum și asupra consecințelor pe care astfel de incidente le pot avea asupra funcționării serviciilor publice.

Analiza atacurilor cibernetice la nivel internațional evidențiază modul în care diverse guverne au fost afectate de breșe de securitate, atacuri de tip ransomware sau acces neautorizat la date sensibile. Aceste cazuri demonstrează necesitatea implementării unor măsuri proactive de protecție, cum ar fi sisteme avansate de detecție a amenințărilor, politici de securitate riguroase și instruirea personalului pentru a recunoaște și preveni riscurile cibernetice.

Pe plan național, incidentele de securitate cibernetică pot afecta stabilitatea infrastructurilor critice și încrederea cetățenilor în instituțiile publice. Atacurile care vizează bazele de date guvernamentale, sistemele de plăți electronice sau platformele online de servicii publice pot perturba activitățile administrației și pot avea implicații majore asupra protecției informațiilor personale.

Prin examinarea unor astfel de situații, se pot identifica cele mai frecvente tipuri de atacuri, strategiile utilizate de atacatori și lecțiile învățate de administrațiile afectate. Aceste studii de caz contribuie la dezvoltarea unor măsuri eficiente de prevenție și răspuns, consolidând securitatea cibernetică a sectorului public într-un context digital tot mai complex.

1.4.1. *Atacuri asupra instituțiilor guvernamentale din Uniunea Europeană*

Un caz semnificativ a avut loc într-un stat membru al Uniunii Europene, unde un atac de tip phishing a compromis datele de autentificare ale angajaților unei agenții guvernamentale, permițând hackerilor să acceseze informații sensibile și să întrerupă temporar serviciile esențiale. Impactul acestui atac a fost considerabil, afectând milioane de cetățeni și aducând costuri semnificative pentru restaurarea securității [6].

Un exemplu semnificativ este atacul cibernetic din 2018 asupra Ministerului Afacerilor Externe al Germaniei (Auswärtiges Amt), atribuit grupului APT28. Printr-un atac de tip spear-phishing, atacatorii au obținut acces la rețeaua IT, compromițând comunicațiile diplomatice timp de peste un an [24]. Lipsa unui sistem robust de detecție a intruziunilor a permis persistența atacului, generând costuri estimate la milioane de euro pentru remediere. Ca răspuns, Germania a implementat măsuri conforme cu Directiva NIS2, inclusiv monitorizarea continuă a rețelelor și instruirea personalului.

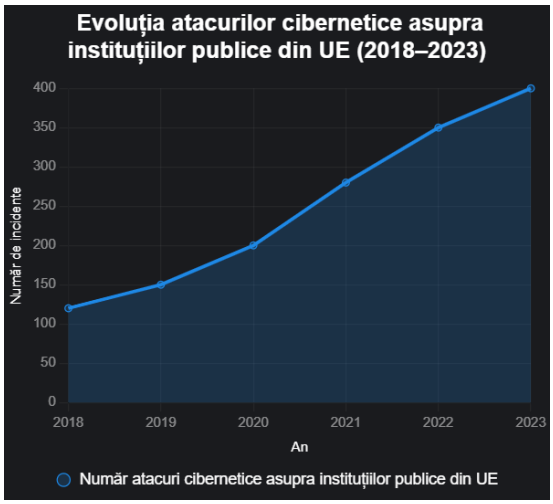


Fig. 1. Evoluția atacurilor cibernetice
Sursa: https://grok.com/

Un alt caz relevant este atacul ransomware din 2022 asupra municipalității din Antwerpen, Belgia, care a paralizat servicii digitale esențiale, precum emiterea documentelor de identitate și gestionarea plăților online. Acest incident a evidențiat necesitatea backup-urilor regulate și a planurilor de continuitate, care ar fi redus impactul asupra cetățenilor. Aceste cazuri subliniază importanța alinierii la standardele europene de securitate cibernetică, precum Directiva NIS2, și a colaborării transfrontaliere pentru partajarea informațiilor despre amenințări [25].

Tabel 1. Exemple de atacuri cibernetice asupra instituțiilor guvernamentale din UE

Țara	Instituția Vizată	Tipul Atacului	Date Compromise	Impact
Germania	Afacerilor Externe (Auswärtiges Amt)	Phishing prin e-mail	Date de autentificare ale angajaților	Acces neautorizat la informații sensibile, compromiterea securității interne
România	Apărării Naționale (MApN)	Phishing prin e-mail	Date de autentificare ale angajaților	Acces neautorizat la informații sensibile, expunerea datelor clasificate
Franța	Agenția Națională de Securitate a Sistemelor de Informații (ANSSI)	Phishing, malware	Detalii financiare, acces la sisteme interne	Compromiterea infrastructurilor critice, pierderi financiare
Italia	Agenția Națională pentru Securitatea Cibernetică	Phishing, Ransomware	Conturi de e-mail ale angajatilo	Întârzieri în operarea instituției, pierderi de date critice

Sursa: https://therecord.media/ / https://www.bitdefender.com / https://www.ssi.gouv.fr

1.4.2. Vulnerabilități în sistemele IT ale administrației publice din România

În România, un exemplu notabil este atacul ransomware din 2022 asupra Spitalului Clinic de Boli Infecțioase „Victor Babeș” din București, care a criptat datele pacienților, blocând accesul la fișele medicale și întârziind tratamentele critice [15]. Lipsa unui sistem de backup actualizat și a protecției adecvate împotriva malware-ului a amplificat impactul, generând costuri semnificative de remediere și pierderea temporară a datelor esențiale. Un alt incident relevant este atacul DDoD din 2022 asupra site-urilor guvernamentale românești, inclusiv al Parlamentului și al Ministerului Apărării, orchestrat de grupul Killnet ca reacție la poziționările geopolitice ale României. Acest atac a evidențiat vulnerabilitățile infrastructurilor web neprotejate și lipsa mecanismelor eficiente de filtrare a traficului. Pentru a preveni astfel de incidente, autoritățile române pot implementa soluții precum autentificarea multifactorială (MFA) [26], criptarea bazelor de date folosind tehnologii blockchain [27], și platforme de monitorizare bazate pe inteligență artificială, precum Darktrace, care detectează anomaliile în timp real [6]. Colaborarea public-privată cu companii precum Bitdefender poate facilita accesul la expertiză și tehnologii avansate, contribuind la consolidarea securității cibernetice [25].

Atacurile cibernetice asupra instituțiilor publice din România au devenit din ce în ce mai frecvente, iar un exemplu semnificativ a fost compromiterea unei baze de date guvernamentale care a dus la expunerea informațiilor sensibile ale cetățenilor. Aceste incidente pun în evidență vulnerabilitățile din sistemele IT ale administrației publice, mai ales în fața unor atacuri sofisticate, cum ar fi cele de tip SQL injection. Lipsa unor măsuri de protecție adecvate împotriva acestui tip de atac, combinată cu gestionarea defectuoasă a accesului la date sensibile, facilitează exploatarea vulnerabilităților. De asemenea, actualizarea infrastructurii IT rămâne o provocare constantă pentru prevenirea vulnerabilităților și asigurarea integrității și securității datelor.

Măsurile insuficiente de protecție cibernetică, precum și absența unui cadru legislativ adaptat noilor riscuri, pot contribui la amplificarea impactului unui atac. De exemplu, vulnerabilitățile în implementarea criptării și a autentificării multifactor pot lăsa deschise porți pentru accesul neautorizat.

Pentru a combate aceste riscuri, este esențial ca autoritățile publice să adopte politici mai stricte de control al accesului și să implementeze soluții avansate de monitorizare a traficului IT. În acest sens, colaborarea între sectorul public și cel privat joacă un rol crucial. Parteneriatele public-private pot contribui la dezvoltarea unor soluții inovative și eficiente, care să asigure nu doar protecția infrastructurilor critice, dar și prevenirea incidentelor cibernetice. De asemenea, integrarea unor soluții de inteligență artificială pentru detectarea și prevenirea atacurilor poate spori semnificativ capacitatea de reacție a administrației publice în fața amenințărilor digitale [7] [24].

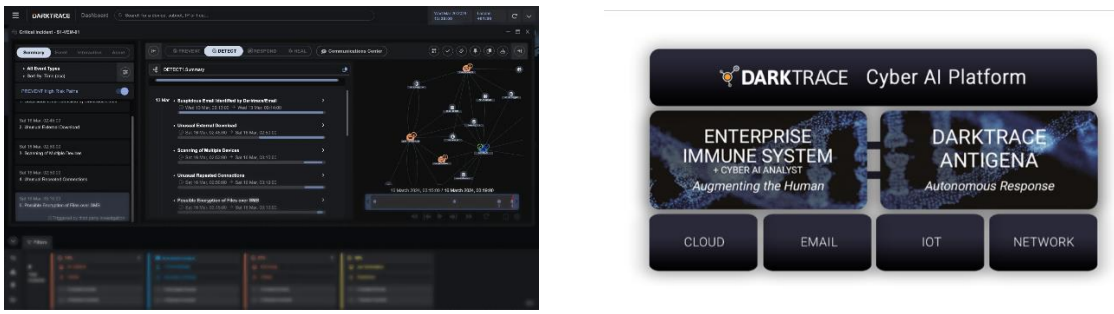


Fig. 2. Aplicație pentru monitorizarea securității cibernetice
Sursa: https://www.darktrace.com/

Aceste măsuri vor contribui la dezvoltarea unei administrații publice mai sigure și mai reziliente, în care cetățenii să aibă încredere, iar instituțiile să își îndeplinească rolul esențial de furnizor de servicii publice sigure și eficiente.

1.5. Strategii și soluții pentru îmbunătățirea securității cibernetice

Pentru a asigura protecția infrastructurilor IT ale administrației publice, guvernele trebuie să adopte strategii eficiente de securitate cibernetică. Printre cele mai importante măsuri se numără:

1.5.1. Implementarea inteligenței artificiale pentru detecția atacurilor

Într-un mediu digital caracterizat de o complexitate în creștere și de amenințări cibernetice tot mai rafinate, inteligența artificială (AI) s-a impus ca o tehnologie indispensabilă pentru protejarea infrastructurilor digitale. Datorită capacității sale de a procesa și analiza volume uriașe de date în timp real, AI permite identificarea rapidă a anomaliilor și tiparelor asociate atacurilor cibernetice, care adesea scapă metodelor tradiționale de securitate. Această tehnologie joacă un rol crucial nu doar în detectarea și prevenirea amenințărilor, ci și în optimizarea răspunsului la incidente, contribuind la consolidarea rezilienței cibernetice a instituțiilor publice.

Un avantaj major al inteligenței artificiale este capacitatea sa de a recunoaște comportamente anormale în rețelele și sistemele informatice. Prin utilizarea algoritmilor de învățare automată (machine learning), AI poate detecta semnele timpurii ale unor atacuri precum malware, ransomware sau phishing, analizând deviațiile de la modelele obișnuite de activitate. De exemplu, platforme precum Darktrace folosesc AI pentru a monitoriza în timp real traficul de rețea, identificând activități suspecte, cum ar fi transferurile neautorizate de date sau tentativele de exploatare a vulnerabilităților [6]. În contextul românesc, astfel de soluții ar putea fi integrate în infrastructurile critice, precum cele din sănătate sau energie, pentru a preveni incidente similare atacului ransomware din 2022 asupra Spitalului „Victor Babeș” din București [15].

Un alt beneficiu semnificativ al AI este capacitatea sa de învățare continuă. Algoritmii de AI se adaptează pe măsură ce procesează noi date, devenind din ce în ce mai eficienți în detectarea amenințărilor emergente. Această caracteristică este esențială într-un peisaj cibernetic în care atacatorii dezvoltă constant noi tehnici, cum ar fi atacurile de tip zero-day sau campanii de phishing sofisticate [28]. În plus, AI poate anticipa vulnerabilități prin analiza predictivă, sugerând măsuri proactive, precum actualizarea software-ului sau implementarea autentificării multifactoriale (MFA) [26]. În România, adoptarea unor astfel de soluții ar putea fi susținută prin Strategia Națională în domeniul Inteligenței Artificiale 2024–2027 [16], care promovează integrarea AI în administrația publică.

Integrarea inteligenței artificiale cu platformele existente de gestionare a incidentelor cibernetice, cum ar fi cele utilizate de CERT-RO, sporește eficiența răspunsului la amenințări [29]. De exemplu, AI poate prioritiza alertele de securitate, reducând timpul necesar pentru investigarea incidentelor și permițând echipelor de securitate să se concentreze pe amenințările critice. Aceasta este deosebit de relevantă pentru instituțiile publice românești, unde resursele umane specializate sunt adesea limitate [7]. Prin automatizarea proceselor repetitive, AI contribuie la reducerea costurilor operaționale și la îmbunătățirea coordonării între departamente, aliniindu-se cu cerințele Directivei NIS2 privind raportarea rapidă a incidentelor.

Cu toate acestea, implementarea AI în securitatea cibernetică nu este lipsită de provocări. Una dintre principalele dificultăți este necesitatea unor seturi de date de calitate pentru antrenarea algoritmilor, care pot fi greu de obținut în sectorul public din cauza restricțiilor de confidențialitate impuse de GDPR [26]. De asemenea, riscurile etice, cum ar fi deciziile automate eronate sau utilizarea abuzivă a AI, trebuie gestionate prin politici clare, așa cum se subliniază în studiile

privind etica în guvernanță. În România, aceste provocări pot fi abordate prin parteneriate public-private, precum cele cu companii de securitate cibernetică (ex. Bitdefender) [25], și prin investiții în formarea personalului, conform Programului EASI.

Pe termen lung, inteligența artificială poate transforma securitatea cibernetică a administrației publice, oferind o protecție dinamică și adaptivă împotriva amenințărilor în evoluție. Pentru a maximiza beneficiile, România trebuie să accelereze adoptarea AI în conformitate cu strategiile naționale de digitalizare [13] și să integreze aceste soluții cu tehnologii complementare, cum ar fi blockchain-ul pentru securizarea datelor. Aceste eforturi, corelate cu bunele practici, vor consolida reziliența cibernetică a instituțiilor publice, contribuind la o administrație mai sigură și mai eficientă [30].

1.5.2. Consolidarea legislației privind securitatea cibernetică

În contextul evoluției rapide a tehnologiilor și al proliferării atacurilor cibernetice, dezvoltarea unui cadru legislativ puternic și coerent este crucială pentru protecția infrastructurilor digitale. Uniunea Europeană a recunoscut importanța acestui aspect și a adoptat Directiva NIS2, care impune un nivel comun ridicat de securitate cibernetică în întreaga Uniune Europeană. Această directivă actualizează și extinde reglementările din directiva anterioară NIS, stabilind standarde mai stricte privind gestionarea riscurilor, protecția infrastructurilor critice și raportarea incidentelor cibernetice. Conform acestei directive, statele membre sunt obligate să implementeze măsuri care vizează protejarea rețelelor și sistemelor informatice esențiale pentru funcționarea economică și socială, precum cele din domeniul energiei, transporturilor, sănătății sau finanțelor.

În cazul României, transpunerea corectă a Directivei NIS2 în legislația națională este esențială pentru creșterea rezilienței cibernetice și pentru conformarea cu cerințele europene. România a făcut pași importanți în acest sens prin Strategia Națională de Creștere a Rezilienței Cibernetice [10], care stabilește obiective aliniate la cerințele europene, inclusiv desemnarea operatorilor de servicii esențiale și întărirea capacităților Centrului Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO) [29]. Cu toate acestea, provocările persistă, cum ar fi lipsa resurselor financiare și umane adecvate pentru implementarea standardelor stricte impuse de NIS2, precum și necesitatea armonizării legislației naționale cu cea europeană [7].

Directiva NIS2 introduce obligații specifice, precum raportarea incidentelor cibernetice în termen de 24 de ore de la detectare și adoptarea unor planuri de gestionare a riscurilor bazate pe standarde internaționale, cum ar fi ISO/IEC 27001 [31]. Aceste măsuri sporesc transparența și responsabilitatea instituțiilor publice, dar necesită investiții semnificative în infrastructura IT și în formarea personalului. În România, implementarea acestor cerințe poate fi susținută prin fonduri europene, cum ar fi cele disponibile prin Programul EASI, care promovează dezvoltarea competențelor de securitate cibernetică.

Mai mult, Directiva NIS2 încurajează cooperarea transfrontalieră prin crearea unei rețele de echipe de răspuns la incidente de securitate cibernetică (CSIRTs) și prin schimbul de informații despre amenințări. Pentru România, această colaborare este crucială, având în vedere atacurile recente, precum cele DDoS atribuite grupului Killnet în 2022. Parteneriatele strategice, cum ar fi cel coordonat de Agenția Națională a Funcționarilor Publici [32], pot facilita alinierea la aceste cerințe, dar necesită o coordonare mai eficientă între instituțiile naționale și partenerii europeni.

Aplicarea noilor reglementări va asigura nu doar protecția infrastructurilor digitale, ci și creșterea transparenței în gestionarea securității cibernetice la nivel național. Totodată, va consolida reziliența sectorului public românesc, reducând riscurile asociate cu atacurile cibernetice asupra infrastructurilor critice. Pentru a maximiza impactul Directivei NIS2, România trebuie să accelereze digitalizarea administrației publice, așa cum este prevăzut în Strategia Națională privind Agenda Digitală [13], și să integreze soluții tehnologice avansate, precum cele bazate pe

inteligență artificială sau blockchain [27]. Aceste eforturi, corelate cu bunele practici vor contribui la o administrație publică mai sigură și mai rezilientă în fața amenințărilor cibernetice [30].

1.5.3. Formarea continuă a angajaților din administrația publică

În peisajul securității cibernetice, factorul uman reprezintă adesea veriga cea mai slabă, deoarece greșelile neintenționate ale angajaților pot deschide porți pentru atacuri cibernetice devastatoare. Comportamente precum utilizarea unor parole ușor de ghicit, accesarea linkurilor din e-mailuri de tip phishing sau ignorarea actualizărilor de securitate sunt frecvent exploatate de atacatori pentru a compromite sistemele instituțiilor publice [28]. Prin urmare, educația continuă a personalului din administrația publică devine un pilon esențial pentru minimizarea riscurilor și cultivarea unei conștientizări sporite privind securitatea digitală.

Programele de formare regulată au rolul de a echipa angajații cu cunoștințele și abilitățile necesare pentru a preveni și gestiona amenințările cibernetice. Aceste inițiative ar trebui să includă module practice, cum ar fi identificarea tentativelor de phishing, crearea parolelor robuste și utilizarea autentificării multifactoriale (MFA), conform standardelor recomandate de GDPR [26]. De exemplu, exercițiile de simulare a atacurilor, precum cele dezvoltate în colaborare cu companii de securitate precum Bitdefender [25], permit testarea reacțiilor angajaților și evidențierea punctelor slabe în pregătirea lor. În România, astfel de programe ar putea fi implementate sub coordonarea Agenției Naționale a Funcționarilor Publici (ANFP), care promovează parteneriate strategice pentru securitatea cibernetică [32], și integrate în Proiectul DNSC pentru dezvoltarea competențelor [29].

Evaluarea periodică a cunoștințelor prin teste și scenarii realiste este crucială pentru a asigura eficacitatea instruirii. Aceste metode permit nu doar măsurarea progresului, ci și încurajarea unei abordări proactive în gestionarea riscurilor cibernetice. De pildă, în contextul atacurilor DDoS din 2022 asupra site-urilor guvernamentale românești, atribuite grupului Killnet, o pregătire mai riguroasă a angajaților ar fi putut facilita detectarea timpurie a anomaliilor și raportarea rapidă către CERT-RO, reducând impactul asupra serviciilor publice [29]. Formarea trebuie personalizată în funcție de rolurile angajaților și de specificul instituțiilor, ținând cont de vulnerabilitățile identificate în sistemele IT [7].

Directiva NIS2, adoptată de Uniunea Europeană, impune statelor membre să prioritizeze educația continuă a personalului din sectorul public pentru a îndeplini standardele de securitate cibernetică. În România, transpunerea acestei directive necesită alocarea de fonduri pentru organizarea de cursuri, posibile prin programe europene precum EASI. Aceste cursuri ar putea include certificări recunoscute, bazate pe standardul ISO/IEC 27001 [31], și platforme de e-learning care să permită accesul facil al angajaților din administrațiile locale. Astfel de inițiative ar spori nu doar competențele tehnice, ci și responsabilitatea individuală în protejarea datelor sensibile.

Formarea continuă contribuie la dezvoltarea unei culturi organizaționale centrate pe securitatea digitală, esențială în contextul transformării digitale a administrației publice românești, așa cum este prevăzut în Strategia Națională privind Agenda Digitală [13]. Această cultură reduce probabilitatea erorilor umane și creează un mediu în care angajații devin prima linie de apărare împotriva amenințărilor cibernetice. De exemplu, campaniile de conștientizare pot preveni incidente precum accesarea neautorizată a datelor, care au afectat instituții publice în trecut [28]. Integrarea formării cu tehnologii precum inteligența artificială și blockchain amplifică eficiența strategiilor de securitate, consolidând reziliența instituțiilor publice.

În concluzie, investițiile în educația continuă a angajaților din administrația publică sunt indispensabile pentru transformarea factorului uman dintr-o vulnerabilitate într-un atu strategic. Prin programe bine structurate, susținute de politici naționale și parteneriate cu sectorul privat,

România poate alinia pregătirea personalului la standardele europene, reducând riscurile cibernetice și protejând interesele cetățenilor [30].

1.5.4. Crearea unui centru național de răspuns la incidente cibernetice

În fața creșterii constante a atacurilor cibernetice și a complexității acestora, multe țări au înființat centre specializate în răspunsul la incidentele de securitate cibernetică (CSIRT). Aceste centre sunt responsabile cu monitorizarea în timp real a amenințărilor, coordonarea intervențiilor și asigurarea unei reacții rapide în cazul unui atac. În acest context, România ar trebui să dezvolte o structură națională consolidată, capabilă să răspundă în mod eficient atacurilor cibernetice și să colaboreze activ cu partenerii internaționali și sectorul privat [29].

În prezent, în România există centre precum CERT-RO și Cyberint, care joacă un rol esențial în securizarea infrastructurilor critice ale statului și ale sectorului privat. CERT-RO se ocupă cu monitorizarea și gestionarea incidentelor de securitate cibernetică, având în responsabilitate protejarea unor sectoare sensibile, cum ar fi cel energetic, financiar, al sănătății și al transporturilor [29]. Aceste structuri sunt interconectate și cu agențiile internaționale de securitate cibernetică, precum ENISA și Europol, pentru a asigura un răspuns coordonat și eficient în fața atacurilor transnaționale [29].

Cu toate acestea, având în vedere evoluția rapidă a tehnologiilor și atacurilor informatice, este esențial ca România să își consolideze aceste centre și să le extindă capabilitățile. Crearea unui centru național de răspuns consolidat ar trebui să includă nu doar monitorizarea și detectarea amenințărilor, ci și dezvoltarea de mecanisme de prevenire și anticipare a atacurilor cibernetice. Acesta ar trebui să fie dotat cu tehnologii avansate de analiză a datelor și să dispună de resurse suficiente pentru a interveni rapid în cazul unor incidente majore [29].

Un alt aspect esențial ar fi organizarea de exerciții de securitate cibernetică, cum ar fi cele deja realizate de CERT-RO, pentru a antrena autoritățile și instituțiile publice în răspunsul la atacuri. De exemplu, exercițiile „CyDEx" au rolul de a simula scenarii de atac cibernetic și de a testa capacitatea de reacție a instituțiilor implicate [29]. Aceste activități sunt esențiale pentru îmbunătățirea răspunsului colectiv și pentru consolidarea unui sistem de apărare cibernetică național.

1.5.5. Adoptarea tehnologiilor emergente în administrația publică

În contextul digitalizării administrației publice, integrarea tehnologiilor emergente, cum ar fi Cloud Computing, joacă un rol crucial în modernizarea infrastructurilor guvernamentale. Aceste soluții nu doar că reduc costurile operaționale, dar permit și scalabilitatea necesară pentru gestionarea unui volum tot mai mare de date guvernamentale. Unul dintre cele mai semnificative avantaje ale utilizării cloud-ului în administrația publică este capacitatea de a facilita accesul rapid și securizat la informații. Prin implementarea unor măsuri avansate de criptare și politici de securitate strict monitorizate, datele guvernamentale sunt protejate împotriva atacurilor cibernetice și a accesului neautorizat [5].

În plus, soluțiile de cloud permit autorităților să îmbunătățească transparența proceselor administrative și să eficientizeze furnizarea serviciilor publice. Protejarea datelor sensibile ale cetățenilor reprezintă o prioritate majoră în contextul reglementărilor privind protecția datelor, cum ar fi Regulamentul General privind Protecția Datelor (GDPR). Cloud Computing oferă mecanisme robuste de protecție a datelor, incluzând backup-uri automate, controlul accesului bazat pe autentificare multifactorială și monitorizarea continuă a infrastructurii IT pentru a detecta și preveni eventualele amenințări [3] .

Adoptarea tehnologiilor emergente contribuie la creșterea eficienței operaționale a instituțiilor publice. Prin automatizarea proceselor administrative și optimizarea fluxurilor de lucru, se reduce timpul necesar pentru procesarea cererilor cetățenilor, iar serviciile publice devin mai accesibile și mai rapide. De asemenea, utilizarea soluțiilor de inteligență artificială integrate în infrastructura cloud permite analizarea volumelor mari de date pentru a identifica modele și tendințe relevante în guvernare [3]. În ciuda avantajelor evidente, adoptarea tehnologiilor emergente în administrația publică vine și cu provocări. Printre acestea se numără necesitatea unei infrastructuri IT adecvate, formarea personalului administrativ pentru utilizarea noilor tehnologii și asigurarea interoperabilității între diferitele platforme digitale utilizate de instituțiile guvernamentale. Totuși, investițiile continue în tehnologii emergente vor facilita trecerea către o administrație publică digitalizată, eficientă și sigură.

1.5.6. Transformarea digitală a relației cu cetățeanul

Digitalizarea administrației publice trebuie să se extindă dincolo de optimizarea proceselor interne, având în vedere nevoile cetățenilor. O administrație modernă trebuie să asigure nu doar eficiență operațională, ci și o interacțiune mai simplă, rapidă și sigură cu cetățenii. Platformele digitale pentru servicii guvernamentale trebuie să garanteze accesibilitatea, transparența și protecția datelor personale.

Un aspect esențial al transformării digitale este implementarea portalelor online care să permită cetățenilor acces rapid la servicii administrative. Aceste platforme oferă posibilitatea depunerii documentelor în format electronic, a efectuării plăților pentru taxe și impozite, a obținerii autorizațiilor și a accesului la diverse informații publice fără a fi necesară prezența fizică la ghișee. Reducerea birocrației prin digitalizare contribuie la creșterea eficienței instituțiilor publice și la îmbunătățirea experienței utilizatorilor.

Totuși, o astfel de schimbare implică și provocări semnificative în ceea ce privește securitatea cibernetică. Protejarea datelor cetățenilor este esențială, iar sistemele digitale trebuie să fie echipate cu soluții avansate de criptare, autentificare multifactorială și monitorizare continuă pentru prevenirea fraudelor și a accesului neautorizat. În plus, este necesară actualizarea constantă a infrastructurilor IT pentru a combate noile amenințări cibernetice și a asigura continuitatea serviciilor publice online [5, 6].

Dezvoltarea unui ecosistem digital centrat pe cetățean necesită și inițiative de educare și informare a utilizatorilor cu privire la noile tehnologii și beneficiile acestora. Campaniile de conștientizare asupra securității digitale, ghidurile de utilizare a platformelor online și suportul tehnic accesibil sunt elemente cheie pentru a încuraja adoptarea soluțiilor digitale de către populație.

Transformarea digitală a administrației publice nu este doar o soluție tehnologică, ci și un proces de adaptare continuă la cerințele unei societăți moderne. Investițiile în infrastructură, reglementările clare privind protecția datelor și colaborarea dintre sectorul public și privat sunt factori determinanți pentru succesul acestei tranziții. Prin digitalizare, administrația publică poate deveni mai eficientă, mai accesibilă și mai sigură, consolidând astfel încrederea cetățenilor în instituțiile statului.

1.5.7. Evaluarea riscurilor și planificarea continuității afacerii

Evaluarea riscurilor cibernetice și planificarea continuității afacerii (Business Continuity Planning - BCP) sunt piloni esențiali pentru asigurarea funcționării neîntrerupte a administrației publice în fața amenințărilor cibernetice. În contextul creșterii frecvenței și sofisticării atacurilor, cum ar fi cele ransomware sau DDoS, instituțiile publice trebuie să adopte o abordare sistematică și proactivă pentru a identifica vulnerabilitățile, a evalua impactul potențial al incidentelor și a implementa măsuri eficiente de mitigarea riscurilor. Aceste procese contribuie nu doar la

protejarea infrastructurilor critice, ci și la menținerea încrederii cetățenilor în capacitatea statului de a gestiona crizele digitale [30].

Evaluarea riscurilor cibernetice trebuie să se bazeze pe metodologii recunoscute la nivel internațional, cum ar fi ISO/IEC 27005 [31], care oferă un cadru structurat pentru identificarea, analiza și gestionarea riscurilor de securitate a informațiilor. Aceasta implică maparea activelor critice ale instituțiilor publice, evaluarea amenințărilor și vulnerabilităților asociate și estimarea impactului financiar, operațional și reputațional al unui posibil incident. De exemplu, un atac ransomware asupra unei instituții publice, precum cel din 2022 asupra Spitalului „Victor Babeș" [15], poate întrerupe furnizarea serviciilor esențiale, generând costuri semnificative și afectând încrederea publică.

În România, evaluarea riscurilor ar putea fi integrată în Strategia Națională de Creștere a Rezilienței Cibernetice [10], care subliniază necesitatea unei abordări proactive. Aceasta poate include utilizarea unor instrumente automate de scanare a vulnerabilităților, precum Nessus sau Qualys, combinate cu analiza predictivă bazată pe inteligență artificială, pentru a anticipa amenințările emergente, cum ar fi atacurile de tip zero-day. De asemenea, conform Directivei NIS2, instituțiile publice sunt obligate să efectueze evaluări periodice ale riscurilor și să raporteze rezultatele către autoritățile competente, cum ar fi CERT-RO [29]. Implementarea acestor cerințe necesită investiții în instrumente tehnologice și formarea personalului, susținute prin fonduri europene, precum Programul EASI.

Planurile de continuitate a afacerii (BCP) sunt esențiale pentru a asigura recuperarea rapidă a operațiunilor în cazul unui incident cibernetic. Acestea trebuie să includă proceduri clare pentru backup-ul și restaurarea datelor, gestionarea accesului în situații de criză și reluarea serviciilor critice. Standardul ISO 22301 [31] oferă un cadru pentru elaborarea BCP, punând accent pe testarea periodică a planurilor prin simulări și exerciții, cum ar fi cele organizate de CERT-RO în cadrul „CyDEx". În România, lipsa unor astfel de planuri bine definite a fost evidențiată în timpul atacurilor DDoS din 2022 atribuite grupului Killnet, care au afectat temporar accesul la site-urile guvernamentale.

Un aspect crucial al BCP este implementarea unor soluții de backup redundante, preferabil stocate în medii cloud securizate [12], care respectă reglementările GDPR [26]. De exemplu, platformele cloud guvernamentale, precum cele dezvoltate în cadrul Strategiei Naționale privind Agenda Digitală [13], pot facilita stocarea descentralizată a datelor, reducând riscul pierderii informațiilor critice. În plus, integrarea tehnologiilor blockchain [27] poate spori securitatea backup-urilor prin asigurarea integrității și autenticității datelor.

Simulările de atacuri cibernetice sunt esențiale pentru testarea eficacității planurilor de continuitate și pentru antrenarea personalului. Exercițiile „CyDEx" organizate de CERT-RO oferă un exemplu concret de bună practică, permițând instituțiilor publice să simuleze scenarii realiste, precum atacuri ransomware sau breșe de date, și să evalueze timpul de răspuns al echipelor. Aceste simulări ar trebui extinse la nivel local, unde multe administrații publice sunt vulnerabile din cauza resurselor limitate [7]. Parteneriatele public-private cu companii de securitate, precum Bitdefender [25], pot facilita accesul la expertiză și tehnologii avansate pentru organizarea acestor exerciții.

Simulările contribuie, de asemenea, la cultivarea unei culturi organizaționale axate pe securitate, complementând programele de formare continuă. De exemplu, antrenarea angajaților pentru a recunoaște și raporta rapid anomaliile poate reduce impactul unui atac, aliniindu-se cu cerințele Directivei NIS2 privind raportarea incidentelor în 24 de ore. În plus, colaborarea cu centre internaționale, precum ENISA [28], poate aduce expertiză suplimentară pentru simularea atacurilor transfrontaliere.

Un atac cibernetic poate afecta nu doar funcționarea sistemelor IT, ci și încrederea cetățenilor în instituțiile publice. Prin urmare, planurile de continuitate trebuie să includă strategii de comunicare în criză, care să asigure transparența și să informeze publicul despre măsurile luate. De exemplu, în cazul unei breșe de date, instituțiile trebuie să respecte obligațiile GDPR [26] de notificare a autorităților și a persoanelor afectate în termen de 72 de ore. În România, CERT-RO [29] poate coordona comunicarea în astfel de situații, dar este necesară o mai mare armonizare între instituții pentru a evita mesajele contradictorii.

Campaniile de conștientizare, integrate în transformarea digitală a relației cu cetățeanul, pot pregăti publicul pentru astfel de scenarii, reducând panica și dezinformarea. De asemenea, colaborarea cu sectorul privat, prin parteneriate strategice [32], poate oferi acces la experți în comunicare de criză, contribuind la gestionarea eficientă a impactului reputațional.

Evaluarea riscurilor și planificarea continuității afacerii trebuie să fie strâns corelate cu alte măsuri descrise în acest capitol, precum implementarea inteligenței artificiale, consolidarea legislației și formarea continuă a angajaților. De exemplu, AI poate fi utilizată pentru a automatiza procesele de evaluare a riscurilor, identificând vulnerabilități în timp real, în timp ce formarea angajaților reduce probabilitatea erorilor umane care pot amplifica impactul unui atac [28]. De asemenea, centrele naționale de răspuns la incidente, precum CERT-RO, joacă un rol crucial în coordonarea răspunsului la incidente, asigurând implementarea rapidă a planurilor de continuitate.

Pe termen lung, România poate valorifica fondurile europene disponibile prin Programul EASI pentru a investi în instrumente avansate de gestionare a riscurilor și pentru a dezvolta infrastructuri reziliente. Aceste eforturi, aliniate cu Strategia Națională de Creștere a Rezilienței Cibernetice [10] vor consolida capacitatea administrației publice de a face față amenințărilor cibernetice, protejând interesele cetățenilor și asigurând continuitatea serviciilor esențiale [30].

1.6. Concluzii

Digitalizarea administrației publice reprezintă un pas important în modernizarea serviciilor guvernamentale, facilitând accesul cetățenilor la informații și servicii, precum și îmbunătățirea eficienței instituțiilor publice. Totuși, acest proces implică și provocări semnificative în ceea ce privește securitatea cibernetică. În cadrul studiilor de caz analizate, s-a demonstrat că atacurile cibernetice asupra infrastructurilor guvernamentale pot avea efecte devastatoare, de la pierderi financiare și de date până la afectarea încrederii publice și riscuri pentru securitatea națională.

Pentru a proteja infrastructura IT a instituțiilor publice, este crucial să se adopte soluții avansate de securitate cibernetică. Aceste soluții trebuie să fie adaptive și capabile să răspundă rapid la noile amenințări. De asemenea, este necesar să existe un cadru legislativ care să alinieze reglementările românești la standardele internaționale, precum cele ale Uniunii Europene sau ale organizațiilor internaționale în domeniul securității cibernetice. Aceste măsuri legislative trebuie să se concentreze pe protecția datelor personale, pe implementarea unor protocoale de securitate clare și pe sancționarea adecvată a atacurilor cibernetice.

Un alt element esențial este investiția în educația digitală a angajaților din sectorul public. Formarea continuă a personalului în ceea ce privește riscurile cibernetice și bunele practici de securitate este fundamentală pentru reducerea vulnerabilităților. Angajații trebuie să fie pregătiți să identifice și să reacționeze corect la amenințările cibernetice, astfel încât să poată proteja atât infrastructura IT a instituțiilor publice, cât și datele sensibile ale cetățenilor.

În plus, tehnologiile emergente, cum ar fi inteligența artificială, pot fi un aliat puternic în combaterea atacurilor cibernetice. Utilizarea IA pentru detectarea automată a anomaliilor și pentru răspunsul rapid la incidente poate îmbunătăți semnificativ securitatea infrastructurilor IT publice. De asemenea, colaborarea strânsă între sectorul public și cel privat poate aduce beneficii

semnificative, având în vedere expertiza tehnologică și resursele pe care sectorul privat le poate oferi în combaterea amenințărilor cibernetice.

Această cercetare subliniază importanța unei abordări proactive în domeniul securității cibernetice, în care guvernele trebuie să investească în infrastructuri mai sigure, în educația continuă a angajaților și în dezvoltarea unui cadru legislativ adaptat noilor provocări tehnologice. Recomandările formulate oferă un ghid pentru îmbunătățirea securității digitale în administrația publică românească, punând un accent deosebit pe prevenire, educație și colaborare între sectoare.

Capitolul 2. Provocări și măsuri de protecție în administrația publică din România în contextul digitalizării

Digitalizarea administrației publice din România reprezintă un proces esențial pentru modernizarea serviciilor oferite cetățenilor și pentru creșterea eficienței instituțiilor publice. În ultimii ani, autoritățile române au implementat platforme online și baze de date digitale pentru a facilita accesul la informații și pentru a îmbunătăți transparența proceselor administrative. De asemenea, dezvoltarea infrastructurii cloud a permis stocarea și gestionarea eficientă a volumelor mari de date guvernamentale. [2]

Totuși, tranziția către mediul digital a adus și provocări semnificative în ceea ce privește securitatea cibernetică. Creșterea interconectivității și a complexității sistemelor informatice a expus instituțiile publice la riscuri cibernetice mai mari, care pot afecta integritatea, disponibilitatea și confidențialitatea informațiilor gestionate. Aceste riscuri pot proveni din diverse surse, precum atacuri cibernetice externe, erori umane sau deficiențe în infrastructura IT existentă [1]

Pentru a aborda aceste provocări, România a dezvoltat strategii și măsuri specifice, inclusiv:

- Strategia Națională privind Agenda Digitală pentru România 2020: Această strategie vizează creșterea eficienței administrației publice prin implementarea de soluții TIC moderne, promovând interoperabilitatea și securitatea cibernetică. [13]
- Programul GovITHub: Inițiat pentru a sprijini dezvoltarea de platforme și servicii publice online, acest program contribuie la reducerea birocrației și la îmbunătățirea accesului cetățenilor la serviciile publice. [11]
- Planul Național de Acțiune pentru Implementarea Strategiei Naționale de Digitalizare a Administrației Publice: Acest plan detaliază măsurile specifice pentru dezvoltarea infrastructurii digitale și pentru asigurarea securității cibernetice în sectorul public.

Digitalizarea administrației publice din România a adus beneficii semnificative în termeni de eficiență și transparență. Cu toate acestea, este esențial ca autoritățile să continue să investească în măsuri de securitate cibernetică și în dezvoltarea infrastructurii digitale pentru a proteja datele sensibile și pentru a menține încrederea cetățenilor în serviciile publice. [7]

2.1. Amenințări cibernetice actuale asupra administrației publice

Instituțiile publice din România se confruntă cu o gamă tot mai variată de amenințări cibernetice:

- Atacurile de tip ransomware, care criptează datele instituțiilor și solicită recompense în schimbul deblocării acestora;
- Phishing-ul și spear phishing-ul, direcționate către funcționari publici pentru a obține acces neautorizat la sisteme sau date sensibile;
- Atacurile de tip DDoS (Distributed Denial of Service), care au ca scop blocarea accesului la servicii publice online;
- Exploatarea vulnerabilităților software sau a lipsei de actualizări de securitate în infrastructura digitală a administrației;
- Atacurile interne (insider threats), cauzate de angajați neglijenți sau rău-intenționați.

În anul 2021, mai multe instituții publice din România au fost ținta unor atacuri cibernetice de tip ransomware, care au dus la întreruperea temporară a activității și pierderi de date. De exemplu, în noiembrie 2021, doi bărbați din Constanța au fost arestați preventiv sub acuzația că au aderat la grupările de hackeri Sodinokibi/Revil și GandCrab. Aceste grupări au lansat atacuri ransomware asupra unor entități din întreaga lume, inclusiv companii, municipalități, spitale, forțe de ordine, servicii de urgență, unități școlare și universități, cu câștiguri ilicite estimate la miliarde de dolari.

Tot în aprilie 2022, site-urile mai multor autorități naționale și instituții financiar-bancare din România au fost afectate de un atac cibernetic de tip Distributed-Denial-of-Service (DDoS). Atacul a determinat indisponibilizarea site-urilor respective pentru mai multe ore. Investigațiile au arătat că atacatorii au utilizat echipamente de rețea din afacerea României, preluând controlul asupra acestora prin exploatarea unor vulnerabilități de securitate cibernetică. Atacul a fost revendicat de gruparea KILLNET, specializată în atacuri DDoS.

2.1.1. Atacul ransomware din 2021

În noiembrie 2021, mai multe primării și instituții publice din România au fost vizate de atacuri ransomware. Aceasta este o formă de atac cibernetic în care datele sunt criptate de atacatori, iar victimele sunt obligate să plătească o răscumpărare pentru a le recupera. Grupările de hackeri, precum Sodinokibi/Revil și GandCrab, au fost responsabile de astfel de atacuri pe scară largă, vizând atât organizații private, cât și instituții guvernamentale.

Cauzele principale ale atacului:

- Lipsa unor măsuri de securitate corespunzătoare: Multe dintre instituțiile atacate nu aveau măsuri de securitate cibernetică implementate la nivelul corespunzător. Aceste instituții nu dispun de infrastructuri robuste pentru prevenirea și detectarea atacurilor cibernetice, iar personalul nu era suficient de pregătit să gestioneze amenințările emergente.
- Vulnerabilități în infrastructura IT: Instituțiile guvernamentale din România nu aveau toate actualizările de securitate aplicate la timp. Această întârziere în patching-ul sistemelor a permis exploatarea vulnerabilităților de securitate de către atacatori, care au folosit software-ul dăunător pentru a pătrunde în rețelele guvernamentale.
- Atacuri de phishing: În multe cazuri, atacurile ransomware sunt declanșate prin e-mailuri de phishing care conțin linkuri malițioase sau atașamente periculoase. Aceste mesaje sunt adesea destinate angajaților neatenți, care pot deschide aceste mesaje fără a verifica sursa lor.

Cum ar fi putut fi prevenit acest atac:

- Îmbunătățirea educației și a instruirii personalului: Instituțiile guvernamentale ar fi trebuit să implementeze programe regulate de formare pentru angajați, pentru a le crește conștientizarea riscurilor cibernetice și pentru a le învăța cum să identifice e-mailurile de phishing și alte forme de atacuri.
- Măsuri de securitate proactive: Aplicarea regulată a actualizărilor de securitate și a patch-urilor pentru toate sistemele și software-urile utilizate de instituțiile publice ar fi ajutat la eliminarea vulnerabilităților exploatabile de hackeri.
- Implementarea unei infrastructuri IT robuste: Instituțiile ar fi trebuit să adopte soluții de securitate mai avansate, cum ar fi criptarea datelor, firewall-uri avansate și monitorizarea continuă a rețelelor, pentru a detecta activități suspecte în timp real.
- Planuri de recuperare în caz de dezastru: Ar fi fost esențial ca aceste instituții să dispună de planuri bine puse la punct pentru a recupera rapid datele afectate de ransomware, inclusiv backup-uri regulate și securizate ale datelor critice.

2.1.2. Atacul DDoS din 2022

În aprilie 2022, mai multe site-uri ale autorităților naționale și instituțiilor financiar-bancare din România au fost afectate de un atac cibernetic de tip Distributed-Denial-of-Service (DDoS) [33]. Atacurile DDoS au fost revendicate de gruparea cibernetică KILLNET, un grup cu legături susținute cu activități de tip hacktivism. Atacurile DDoS sunt concepute pentru a copleși serverele țintă cu un volum mare de trafic, făcându-le inaccesibile pentru utilizatori.

Cauzele principale ale atacului:

- Lipsa protecției împotriva atacurilor DDoS: În cazul acestui atac, instituțiile vizate nu aveau infrastructuri capabile să gestioneze volumele mari de trafic generate de un atac DDoS. Aceste atacuri sunt adesea ușor de realizat, dar greu de prevenit fără măsuri speciale de protecție.
- Dependința de infrastructuri vulnerabile: Multe dintre site-urile guvernamentale și instituțiile financiar-bancare nu aveau soluții de protecție eficiente, cum ar fi serviciile de mitigare DDoS, care sunt capabile să filtreze traficul malițios înainte ca acesta să ajungă la serverele instituțiilor.
- Lipsa unui plan de răspuns rapid: Chiar și în cazul în care aceste atacuri pot fi detectate rapid, multe organizații nu aveau un plan de răspuns rapid pentru a reduce impactul acestor atacuri asupra serviciilor lor online [33].

Cum ar fi putut fi prevenit acest atac:

- Implementarea unei protecții DDoS dedicate: Instituțiile ar fi trebuit să adopte soluții de protecție avansate împotriva atacurilor DDoS, cum ar fi utilizarea unor firewall-uri robuste și a unor platforme de protecție cloud care pot detecta și bloca traficul DDoS înainte ca acesta să afecteze infrastructura internă a rețelei.
- Scalabilitate și redundanță: Pentru a face față volumului mare de trafic generat de un atac DDoS, ar fi fost important ca instituțiile vizate să aibă infrastructuri scalabile, cu servere distribuite și backup-uri de date care să poată prelua sarcina în cazul în care serverele primare sunt afectate.
- Planuri de continuitate a activității: Instituțiile publice ar fi trebuit să dezvolte și să implementeze planuri de continuitate a activității pentru a asigura disponibilitatea site-urilor lor chiar și în timpul unui atac DDoS, astfel încât cetățenii și utilizatorii să poată accesa în continuare serviciile esențiale.

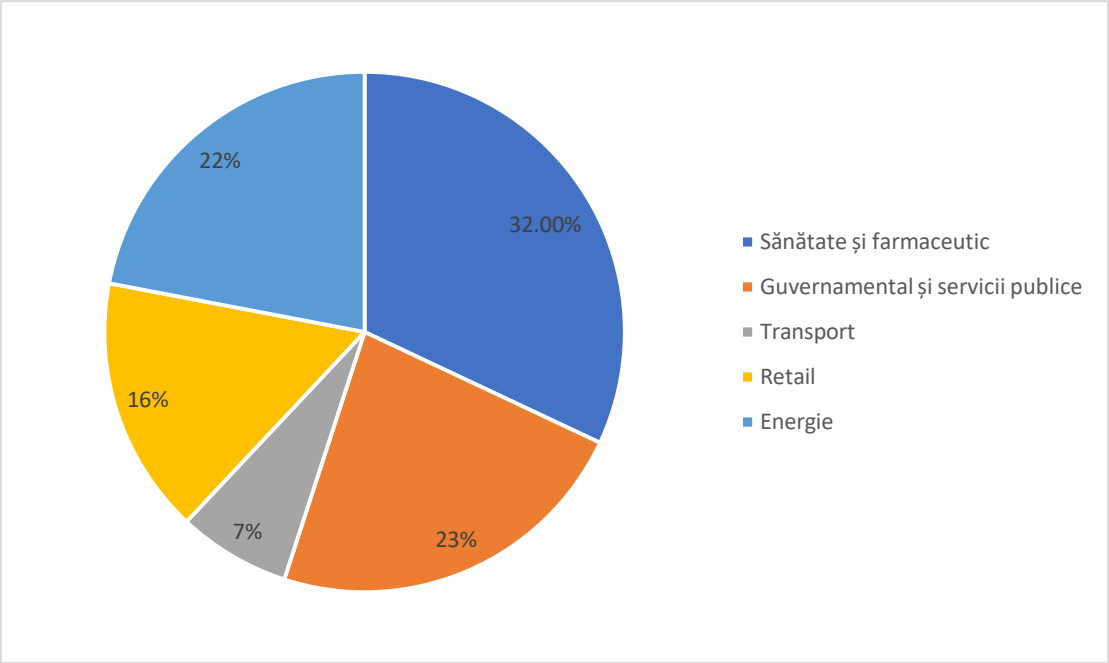


Fig. 3.a. Distribuția atacurilor cibernetice pe sectoare

Atacurile cibernetice afectează tot mai multe domenii de activitate, odată cu intensificarea proceselor de digitalizare. Conform datelor recente, cele mai vizate sectoare sunt sănătatea și industria farmaceutică, unde 32% dintre atacuri au avut loc, urmate de instituțiile guvernamentale și serviciile publice (23%), sectorul energetic (22%), retail (16%) și transporturi (7%). Această distribuție relevă faptul că atacatorii cibernetici vizează în special infrastructuri critice și domenii care gestionează volume mari de date sensibile sau au un impact major asupra funcționării societății. Sectoarele precum sănătatea și guvernarea sunt deosebit de vulnerabile din cauza complexității sistemelor informatice și a presiunii constante de a funcționa fără întreruperi, ceea ce poate duce la compromisuri în securitate. Prin urmare, este esențial ca aceste domenii să investească în măsuri avansate de protecție cibernetică și în politici eficiente de prevenire a incidentelor.

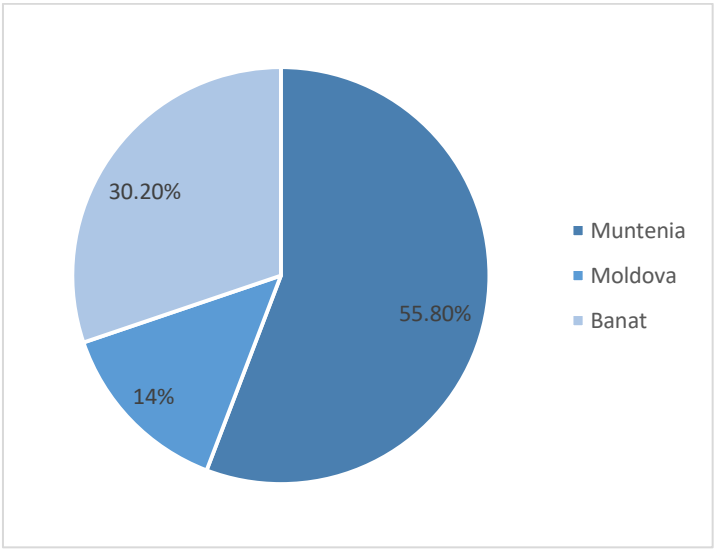


Fig. 3.b. Distribuția atacurilor cibernetice pe sectoare

Muntenia se află pe primul loc, cu aproape 55,8% din totalul atacurilor cibernetice, ceea ce subliniază faptul că această regiune include Capitala București și cele mai multe instituții

guvernamentale și infrastructuri critice. Bucureștiul, ca centru administrativ și economic al țării, constituie un punct de atracție major pentru atacatorii cibernetici.

Concentrarea instituțiilor guvernamentale și infrastructurilor critice: Bucureștiul găzduiește majoritatea ministerelor și agențiilor guvernamentale, iar atacurile asupra acestora pot avea un impact direct asupra securității naționale și a funcționării administrației publice.

Volume mari de date sensibile: Muntenia gestionează o cantitate considerabilă de date sensibile, ceea ce atrage hackerii, în special din domeniul sănătății, administrației publice și al infrastructurilor critice.

Banatul reprezintă 30,2% din totalul atacurilor cibernetice, ceea ce o plasează pe locul al doilea în clasament. Deși este o regiune mai puțin dens populată și cu un număr mai mic de instituții publice comparativ cu Muntenia, Banatul rămâne o țintă importantă din cauza infrastructurii sale critice și a industriei de energie.

Banatul reprezintă 30,2% din totalul atacurilor cibernetice, ceea ce o plasează pe locul al doilea în clasament. Deși este o regiune mai puțin dens populată și cu un număr mai mic de instituții publice comparativ cu Muntenia, Banatul rămâne o țintă importantă din cauza infrastructurii sale critice și a industriei de energie.

Moldova este responsabilă pentru aproximativ 14% din atacurile cibernetice din România. Regiunea, în general, nu a beneficiat de aceleași investiții în securitate cibernetică ca alte zone mai dezvoltate ale țării, ceea ce o face o țintă vulnerabilă pentru atacuri, în special în contextul digitalizării.

2.2. Cultura securității cibernetice

Una dintre dificultățile esențiale în procesul de digitalizare a administrației publice din România constă în absența unui mediu instituțional care să promoveze securitatea informatică ca prioritate. Multe organizații publice nu oferă instruiri regulate angajaților privind riscurile digitale, iar politicile de protecție sunt adesea vagi sau aplicate inconsecvent. În lipsa unor măsuri clare și a unei conduite unitare, sistemele informatice rămân expuse unor amenințări reale și frecvente.

Soluționarea provocărilor legate de lipsa unei culturi organizaționale de securitate cibernetică presupune implementarea unor strategii clare de formare profesională, promovarea leadershipului digital și crearea unor proceduri uniforme de prevenție și reacție la incidente. Este esențial ca angajații să fie familiarizați cu bunele practici în domeniu, iar instituțiile să adopte politici coerente și actualizate, aliniate standardelor europene. Astfel, digitalizarea poate fi realizată în mod sigur, fără a compromite integritatea datelor sau funcționarea serviciilor publice.

2.2.1. Strategia națională de creștere a rezilienței cibernetice

Strategia Națională de Creștere a Rezilienței Cibernetice [10] are ca obiectiv principal protejarea infrastructurilor și sistemelor informatice esențiale pentru funcționarea statului și a economiei, în fața riscurilor și atacurilor cibernetice. Adoptată în anul 2022, prin Hotărârea Guvernului nr. 1.321, această strategie pune accent pe dezvoltarea unui cadru normativ și instituțional robust, capabil să răspundă provocărilor în continuă schimbare din domeniul securității cibernetice.

Printre prioritățile acestei strategii se numără consolidarea mecanismelor de reacție în fața incidentelor cibernetice, formarea personalului specializat și crearea unor centre de răspuns rapid. De asemenea, se pune un accent deosebit pe educația și formarea continuă în domeniul securității cibernetice, pentru a crește gradul de conștientizare și competență în rândul cetățenilor și al profesioniștilor din sectorul public și privat. Un alt obiectiv important este promovarea unei

cooperări mai strânse între sectorul public și cel privat, dar și între țările membre ale Uniunii Europene, având în vedere natura globală a amenințărilor cibernetice.

Această strategie reprezintă un pilon esențial în securizarea mediului digital din România, susținând tranziția către o societate și o economie digitală mai sigure și mai reziliente. Pentru a atinge aceste obiective, strategia include măsuri concrete, precum consolidarea rolului Centrului Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO) și înființarea unor centre regionale de răspuns rapid, capabile să gestioneze incidentele în timp real [29]. De exemplu, în urma atacurilor DDoS din 2022 atribuite grupului Killnet, CERT-RO a coordonat răspunsul instituțiilor afectate, evidențiind nevoia unor mecanisme mai eficiente. Formarea personalului este susținută prin programe precum Proiectul DNSC, care oferă cursuri de conștientizare și certificări bazate pe standardul ISO/IEC 27001 [29], [31].

Strategia promovează parteneriate public-private, cum ar fi colaborările cu companii de securitate precum Bitdefender [25], pentru a facilita transferul de expertiză și tehnologie. La nivel european, România participă în rețeaua CSIRTs, conform Directivei NIS2, pentru schimbul de informații despre amenințări transfrontaliere. De asemenea, campaniile de informare vizează creșterea alfabetizării digitale a cetățenilor, în special pentru categoriile vulnerabile. Aceste inițiative sunt esențiale pentru protejarea platformelor digitale, cum ar fi „ghișeul.ro” [30].

Implementarea strategiei întâmpină însă provocări, precum lipsa resurselor financiare și a personalului calificat [7]. Armonizarea legislației naționale cu cerințele europene, necesită o coordonare interinstituțională sporită. De asemenea, conștientizarea limitată a cetățenilor poate încetini adoptarea practicilor sigure [34]. Prin alocarea de fonduri europene, precum cele din Programul EASI, și integrarea tehnologiilor emergente, cum ar fi inteligența artificială și blockchain-ul [27], strategia poate consolida reziliența digitală a României, reducând vulnerabilitățile infrastructurilor critice.

2.2.2. Dezvoltarea competențelor: proiectul DNSC

Pentru a răspunde provocărilor crescânde din mediul digital, România a consolidat rolul Directoratului Național de Securitate Cibernetică (DNSC), autoritate centrală în arhitectura națională de securitate cibernetică. DNSC are responsabilități-cheie în coordonarea și monitorizarea măsurilor de protecție a infrastructurilor critice, în conformitate cu cerințele Directivei UE NIS 2, transpusă prin OUG nr. 155/2024 [35].

DNSC desemnează și supraveghează operatorii de servicii esențiale (OSE) și entitățile critice din domenii precum sănătatea, energia, transporturile și administrația publică, evaluând riscurile, verificând conformitatea cu standardele de securitate și sprijinind organizațiile în prevenirea și gestionarea incidentelor cibernetice. În sectorul sănătății, Casa Națională de Asigurări de Sănătate, clasificată ca entitate esențială, trebuie să respecte obligații stricte de raportare, audit și conformitate, sub coordonarea DNSC [35].

Pentru a facilita adaptarea la noile cerințe, DNSC elaborează ghiduri, modele de audit și metodologii de evaluare a riscurilor, promovând totodată campanii de conștientizare, formare profesională și colaborare interinstituțională. Aceste inițiative vizează consolidarea culturii de securitate informațională, punând accent pe prevenție, monitorizare continuă și răspuns rapid, în linie cu standardele europene [35].

De asemenea, DNSC susține modernizarea platformelor informatice critice, cum ar fi cele din e-Sănătate (SIUI, CEAS, DES și viitoare sisteme integrate), esențiale pentru alinierea la normele europene de securitate și pentru reducerea vulnerabilităților în fața atacurilor cibernetice tot mai complexe [35].

Pe fondul transformării digitale accelerate, al creșterii volumului de date sensibile și al intensificării amenințărilor cibernetice, DNSC joacă un rol crucial în sporirea rezilienței cibernetice naționale. Prin reglementare și coordonare, instituția asigură continuitatea serviciilor esențiale și protejează drepturile cetățenilor într-un mediu digital sigur și eficient [35].

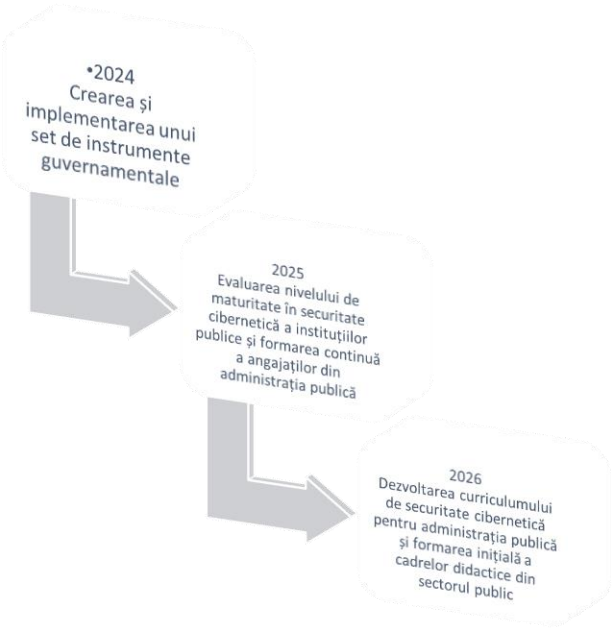


Fig. 4. Piramida activităților pentru securitatea cibernetică în administrația publică

2.3. Protecția și criptarea datelor sensibile în administrația publică

Protecția și criptarea datelor sensibile reprezintă un element fundamental al securității cibernetice, în special în contextul administrației publice, care gestionează frecvent informații de o mare valoare și sensibilitate, precum datele personale, financiare, medicale sau de securitate națională. Aceste informații trebuie protejate eficient pentru a preveni accesul neautorizat sau pierderea acestora, ceea ce face ca criptarea să fie o metodă esențială în protejarea datelor sensibile. Criptarea datelor presupune utilizarea unor algoritmi matematici care transformă informațiile într-un format inaccesibil pentru persoanele neautorizate. Astfel, criptarea poate fi aplicată în mai multe forme, în funcție de nevoile instituțiilor și de mediul în care sunt stocate sau transferate datele sensibile.

Una dintre tehnicile de criptare este criptarea datelor în tranzit, care protejează informațiile pe parcursul transmiterii lor între locații, cum ar fi rețelele de comunicație (internet sau rețele interne). Protocolul SSL/TLS este utilizat pentru criptarea conexiunilor între servere și utilizatori, în timp ce VPN-ul criptă datele transmise între rețele [36]. De asemenea, criptarea datelor în repaus protejează informațiile stocate pe dispozitive de stocare, precum servere sau hard diskuri, chiar și atunci când acestea nu sunt active. Algoritmul AES (Advanced Encryption Standard) este adesea folosit pentru a asigura criptarea datelor stocate, iar Full Disk Encryption (FDE) criptează întregul disk al unui dispozitiv, protejând astfel toate datele stocate [31].

Criptarea fișierelor individuale și a bazelor de date reprezintă alte soluții eficiente pentru protejarea datelor sensibile. GPG (GNU Privacy Guard) sau PGP (Pretty Good Privacy) sunt folosite pentru criptarea fișierelor individuale, iar Transparent Data Encryption (TDE) este aplicat

pentru criptarea datelor din bazele de date fără a afecta performanța aplicațiilor [35]. Aceste tehnici de criptare ajută la prevenirea accesului neautorizat la datele sensibile și contribuie la protecția informațiilor critice.

Pe lângă criptare, protejarea datelor sensibile necesită și implementarea unor măsuri complementare. Unul dintre principiile fundamentale în protecția datelor este controlul accesului, care presupune limitarea accesului angajaților doar la acele date de care au nevoie pentru îndeplinirea sarcinilor lor. În acest sens, autentificarea multifactorială (MFA) este o măsură esențială pentru asigurarea unui acces securizat la sistemele care stochează date sensibile. De asemenea, este recomandată utilizarea unor soluții de Single Sign-On (SSO), care permit gestionarea mai eficientă a accesului la multiple aplicații și sisteme, asigurându-se astfel că doar persoanele autorizate pot accesa informațiile critice [37].

Politicile și procedurile de protecție a datelor trebuie să fie clare și să includă norme privind stocarea, transferul și distrugerea datelor sensibile. De asemenea, protecția datelor în cloud reprezintă un aspect important, iar instituțiile publice trebuie să adopte soluții de criptare a datelor înainte de a le stoca în cloud, respectând reglementările legale și de securitate specifice, cum ar fi GDPR-ul [26]. Utilizarea unor soluții de cloud private sau hibride este preferabilă pentru a reduce riscurile asociate cu stocarea datelor sensibile în medii publice.

Monitorizarea și auditul accesului la date sunt, de asemenea, măsuri esențiale. Implementarea unor soluții de monitorizare care să țină evidența accesului la date sensibile ajută la detectarea rapidă a activităților suspecte sau a tentativelor de acces neautorizat. De asemenea, auditul periodic al logurilor și al activităților contribuie la identificarea vulnerabilităților și a potențialelor breșe de securitate.

În ceea ce privește ștergerea datelor sensibile, aceasta trebuie realizată într-un mod sigur, astfel încât informațiile să nu poată fi recuperate după ce au fost eliminate din sistem. Standardele precum DoD 5220.22-M sau NIST SP 800-88 oferă ghiduri pentru distrugerea completă a datelor stocate pe dispozitive externe [31].

Deși criptarea datelor poate avea un impact asupra performanței și poate implica costuri suplimentare, beneficiile de securitate sunt mult mai mari decât aceste provocări. Instituțiile trebuie să aloce resurse corespunzătoare pentru implementarea și gestionarea soluțiilor de criptare, asigurându-se astfel că datele sensibile sunt protejate în mod adecvat [36].

În contextul e-guvernării, protecția și criptarea datelor sensibile sunt fundamentale pentru securizarea informațiilor gestionate de administrațiile publice. Un exemplu concret este inițiativa Primăriei Brașov, descrisă de Vrabie [30], care a implementat un dispecerat tehnic integrat și un portal web pentru servicii electronice, incluzând plăți online și gestionarea datelor personale. Dispeceratul tehnic utilizează un geoportal interactiv prin care cetățenii raportează probleme, generând date sensibile, precum localizări geografice și sesizări. Aceste date necesită criptare pentru a preveni accesul neautorizată [30], iar sistemul de arhivare electronică al primăriei, dotat cu backup și redundanță, protejează datele în repaus, aliniindu-se cu soluțiile recomandate pentru prevenirea pierderii datelor. Transferul datelor între cetățeni, primărie și instituții partenere implică criptarea în tranzit, probabil prin protocoale securizate, esențiale pentru conformitatea cu standardele europene [24].

Portalul web al Brașovului, care facilitează plăți electronice și acces la informații personale, subliniază [30], necesitatea confidențialității și securității tranzacțiilor. Plățile online necesită criptare robustă pentru a proteja datele financiare, o practică aliniată cu cerințele de securitate cibernetică în administrația publică [7]. Accesul la bazele de date prin call center-ul automatizat implică stocarea datelor sensibile, care trebuie protejate prin metode precum criptarea bazelor de date, conform standardelor internaționale [38]. Implementarea autentificării multifactoriale

(MFA) și a controlului accesului este probabil utilizată pentru a limita accesul neautorizat, așa cum se recomandă în [33].

Un alt exemplu relevant este platforma poliției din Amsterdam [30], care permite cetățenilor să raporteze infracțiuni printr-un portal web, gestionând date de identificare confidențiale. Aceste date necesită criptare în repaus și în tranzit, respectând reglementările GDPR [26]. Autentificarea securizată prin username reduce riscul de abuz, dar necesită mecanisme suplimentare, precum MFA, pentru a preveni accesul neautorizat [33]. Aceste inițiative ilustrează importanța adoptării soluțiilor de criptare și a măsurilor de control al accesului în e-guvernare, contribuind la reziliența cibernetică a administrațiilor publice [29], [23].

2.4. Controlul accesului și gestionarea identităților în administrația publică

Controlul accesului presupune implementarea unor mecanisme care permit limitarea și monitorizarea accesului la resursele IT ale instituțiilor publice, inclusiv la datele sensibile. În general, controlul accesului poate fi realizat prin mai multe metode, detaliate mai jos:

Principiul celui mai mic privilegiu presupune că utilizatorii ar trebui să aibă acces doar la acele resurse sau informații de care au nevoie pentru a-și îndeplini sarcinile de serviciu. Implementarea acestui principiu minimizează riscurile de acces neautorizat la datele sensibile, reducând potențialele breșe de securitate [39].

Autentificarea multifactorială (MFA) adaugă un strat suplimentar de securitate, solicitând utilizatorilor să se autentifice folosind două sau mai multe metode de validare. Aceste metode pot include combinații de parole, dispozitive fizice (de exemplu, token-uri de securitate) sau biometrie (cum ar fi amprentele digitale sau scanările faciale). În administrațiile publice, MFA este esențială pentru protejarea accesului la informațiile sensibile, mai ales atunci când sunt utilizate rețele externe sau conexiuni prin VPN [40].

RBAC este o metodă de control al accesului care atribuie drepturi de acces în funcție de rolul utilizatorului în organizație. Aceasta ajută la simplificarea administrării accesului și asigură că utilizatorii au acces doar la datele necesare funcției lor. În cadrul administrației publice, utilizatorii pot fi împărțiți în categorii, iar accesul la informațiile sensibile va fi reglementat de aceste roluri [41].

PBAC se referă la utilizarea unor politici care reglementează accesul la datele sensibile, pe baza unor factori variabili, precum timpul zilei, locația utilizatorului sau statutul rețelei. Într-un context guvernamental, PBAC poate asigura că datele sensibile sunt accesibile doar în anumite condiții, cum ar fi utilizarea unei rețele securizate sau accesul într-un interval de timp specific [31].

2.4.1. Gestionarea identităților în administrația publică

Gestionarea identităților este procesul prin care instituțiile publice identifică, autentifică și autorizează utilizatorii, asigurându-se că doar persoanele corecte au acces la datele sensibile. Gestionarea identităților implică mai multe procese și tehnologii care lucrează împreună pentru a garanta securitatea datelor.

Un sistem IAM este un ansamblu de politici, procese și tehnologie care permite administrațiilor publice să gestioneze identitățile utilizatorilor și accesul acestora la resursele interne. Aceste sisteme pot include funcționalități de autentificare, autorizare, audit și raportare. În cadrul administrației publice, IAM ajută la automatizarea gestionării identităților utilizatorilor, reducând riscurile și erorile umane [40].

Single Sign-On (SSO) permite utilizatorilor să se autentifice o singură dată pentru a accesa mai multe aplicații și resurse fără a fi necesar să-și reintroducă datele de autentificare. Acest sistem este extrem de util în administrația publică, unde angajații trebuie să acceseze mai multe sisteme interne. SSO îmbunătățește eficiența, dar și securitatea, deoarece reduce riscurile asociate cu gestionarea mai multor parole și conturi [41].

În unele cazuri, autentificarea bazată pe certificare digitală este folosită pentru a confirma identitatea utilizatorilor, în special atunci când aceștia au acces la informații foarte sensibile sau sunt implicați în tranzacții legale sau financiare. Acest sistem utilizează chei publice și private pentru a asigura autenticitatea identității unui utilizator [39].

Monitorizarea activității utilizatorilor și realizarea de audituri regulate sunt esențiale pentru a detecta accesul neautorizat și eventualele abuzuri ale privilegiilor. Astfel de audite permit instituțiilor să identifice utilizatorii care accesează informații sau sisteme pentru care nu au permisiunea necesară și să ia măsurile corecte înainte ca datele sensibile să fie compromise [31].

Gestionarea corectă a parolelor este un alt aspect important în gestionarea identităților. Politicile de securitate a parolelor trebuie să includă reguli clare privind complexitatea și schimbarea periodică a parolelor, pentru a reduce riscurile de acces neautorizat.

2.4.2. Beneficiile controlului accesului și gestionării identităților

Implementarea unor măsuri adecvate de control al accesului și gestionare a identităților aduce multiple beneficii în administrația publică:

- Protecția datelor sensibile: Asigură că doar persoanele autorizate au acces la informațiile critice, protejând datele sensibile de accesul neautorizat.
- Conformitate cu reglementările: Respectă reglementările de protecție a datelor, cum ar fi GDPR, care impun politici clare de acces și protecție a datelor personale.
- Reducerea riscurilor de securitate: Implementarea unor soluții eficiente de control al accesului și gestionare a identităților ajută la prevenirea atacurilor de tip phishing, furtișaguri de identitate sau atacuri interne.
- Eficiență operațională: Automatizarea proceselor de autentificare și autorizare reduce încărcătura administrativă și îmbunătățește eficiența în gestionarea accesului la resursele publice [40].

2.5. AI și modernizarea administrației publice

Inteligența artificială (AI) reprezintă un domeniu al științei informatice axat pe dezvoltarea de sisteme capabile să execute sarcini care, în mod tradițional, necesită inteligență umană, precum recunoașterea vorbirii, luarea deciziilor, analiza imaginilor sau învățarea automată [19]. Scopul principal al AI este de a crea algoritmi și modele care să permită sistemelor informatice să înțeleagă și să prelucreze informații într-un mod cât mai apropiat de gândirea umană.

AI este implementată într-o varietate de domenii, de la educație și sănătate, până la administrație publică și mobilitate urbană. În aceste contexte, AI contribuie la automatizarea proceselor, la reducerea timpului necesar pentru procesarea datelor și la sprijinirea deciziilor strategice bazate pe analiză predictivă [3]. Un alt avantaj esențial este capacitatea sistemelor AI de a învăța din experiență și de a se adapta la noi situații, ceea ce le face utile într-un mediu digital în continuă schimbare.

În administrația publică, AI este deja folosită pentru a digitaliza serviciile și a le personaliza, astfel încât cetățenii să beneficieze de răspunsuri rapide, automatizate și corecte. Mai mult, AI joacă un rol important în orașele inteligente, unde contribuie la optimizarea resurselor, managementul traficului, protejarea mediului și securizarea infrastructurilor critice [19].

2.5.1. *Implementarea inteligenței artificiale (AI) în administrația publică*

Implementarea inteligenței artificiale (AI) în administrația publică reprezintă un pas esențial către transformarea digitală a serviciilor publice, având potențialul de a îmbunătăți semnificativ eficiența, transparența și calitatea acestora. Într-o eră în care volumul de date crește exponențial și cerințele cetățenilor pentru servicii publice mai rapide și mai eficiente sunt tot mai mari, AI oferă soluții inovative pentru a face față acestor provocări. Integrarea AI în diverse domenii ale administrației publice poate conduce la optimizarea resurselor, reducerea costurilor operaționale și îmbunătățirea serviciilor către cetățeni, toate contribuind astfel la dezvoltarea unei administrații mai inteligente și mai responsabile [3].

Unul dintre cele mai importante beneficii ale implementării AI în administrația publică este automatizarea proceselor administrative. Multe dintre activitățile repetitive, cum ar fi procesarea cererilor, completarea formularelor sau gestionarea documentelor, pot fi preluate de sistemele AI, economisind timp prețios pentru angajații instituțiilor publice și reducând riscul de erori umane. De exemplu, utilizarea algoritmilor de procesare a limbajului natural (NLP) poate permite automatizarea răspunsurilor la întrebările frecvente sau gestionarea cererilor de informații. Acest lucru permite instituțiilor să răspundă rapid și eficient, reducând timpul de așteptare pentru cetățeni și contribuind la un serviciu public mai eficient [3].

AI poate avea un impact semnificativ în analiza datelor pentru politici publice. Multe instituții publice se confruntă cu un volum mare de date, de la informații economice și financiare, până la date privind sănătatea, educația sau traficul urban. AI poate ajuta guvernele și autoritățile locale să extragă informații valoroase din aceste seturi de date, să identifice tendințele emergente și să anticipeze nevoile viitoare ale cetățenilor. De exemplu, prin analiza datelor de trafic, AI poate ajuta la optimizarea infrastructurii rutiere, reducând congestionarea și îmbunătățind mobilitatea urbană. În același mod, datele colectate din sectorul sănătății pot fi folosite pentru a formula politici publice mai eficiente și pentru a implementa măsuri preventive adaptate nevoilor comunității [3].

Un alt domeniu în care AI poate revoluționa administrația publică este oferirea de servicii personalizate pentru cetățeni. Tehnologiile de AI, precum asistenții virtuali sau chatboții, pot interacționa cu cetățenii 24/7, oferind informații personalizate și răspunsuri rapide la întrebările acestora. De exemplu, un chatbot implementat într-un portal guvernamental poate ghida cetățenii prin procesul de depunere a declarațiilor fiscale sau de obținere a unor documente administrative, răspunzând întrebărilor frecvente și reducând nevoia de asistență umană. În plus, AI poate ajuta autoritățile să personalizeze ofertele de servicii în funcție de nevoile specifice ale cetățenilor, asigurându-se că resursele sunt utilizate eficient și că fiecare individ primește soluțiile adecvate pentru situația sa [3].

2.5.2. *Provocări în implementarea AI*

Adoptarea inteligenței artificiale (AI) în administrația publică și în dezvoltarea orașelor inteligente promite o eficientizare semnificativă a proceselor administrative și o îmbunătățire a calității serviciilor publice, însă vine la pachet cu provocări complexe care necesită o abordare strategică și o guvernanță riguroasă. Una dintre cele mai importante probleme este gestionarea datelor sensibile, deoarece utilizarea AI implică procesarea unor volume mari de informații personale, financiare, medicale sau alte tipuri de date confidențiale. Aceste date sunt expuse riscurilor de securitate, cum ar fi atacurile cibernetice sau accesul neautorizat, ceea ce impune măsuri stricte de protecție. Instituțiile publice trebuie să implementeze tehnologii avansate de criptare, autentificare multifactorială și politici clare de gestionare a datelor, respectând reglementări precum Regulamentul General privind Protecția Datelor (GDPR) al Uniunii Europene. De asemenea, monitorizarea continuă a sistemelor AI și evaluarea periodică a riscurilor

sunt esențiale pentru a preveni breșele de securitate și pentru a menține încrederea cetățenilor în utilizarea tehnologiilor digitale [3].

O altă provocare majoră este necesitatea unei infrastructuri IT moderne, capabile să susțină cerințele tehnice ale sistemelor AI. Aceasta presupune investiții în servere de înaltă performanță, rețele de comunicații rapide și fiabile, precum și soluții de stocare scalabile, care să poată gestiona cantități mari de date în timp real. În plus, integrarea soluțiilor AI în procesele administrative existente necesită platforme software compatibile și interoperabile. Lipsa unei astfel de infrastructuri poate duce la performanțe slabe sau la imposibilitatea implementării eficiente a tehnologiilor AI. Un alt aspect critic este disponibilitatea personalului calificat, cu competențe în domenii precum ingineria AI, analiza datelor și securitatea cibernetică. Administrațiile publice trebuie să prioritizeze formarea continuă a angajaților și recrutarea de specialiști pentru a gestiona și întreține aceste sisteme, astfel încât să asigure funcționarea optimă a tehnologiilor adoptate [3].

Succesul implementării AI depinde, de asemenea, de acceptarea și încrederea cetățenilor în aceste tehnologii. Temerile legate de confidențialitatea datelor, corectitudinea deciziilor automate sau riscul de abuzuri pot genera reticență în rândul publicului. Pentru a construi încredere, autoritățile publice trebuie să adopte o abordare transparentă, explicând clar modul în care datele sunt colectate, procesate și utilizate de sistemele AI. Cetățenii au nevoie de asigurări că drepturile lor sunt protejate și că deciziile automate sunt echitabile. Un cadru legislativ bine definit, care să includă mecanisme de audit al algoritmilor și proceduri pentru contestarea deciziilor, este indispensabil pentru prevenirea abuzurilor. În plus, consultarea publicului și campaniile de informare privind beneficiile AI pot contribui la reducerea scepticismului și la promovarea unei acceptări mai largi. Transparența, responsabilitatea și implicarea cetățenilor sunt esențiale pentru a transforma AI într-un instrument de încredere în modernizarea administrației publice [3].

Implementarea inteligenței artificiale în administrația publică necesită abordarea simultană a provocărilor legate de securitatea datelor, modernizarea infrastructurii tehnologice și obținerea încrederii cetățenilor. Prin măsuri stricte de protecție a datelor, investiții în tehnologie și personal calificat, precum și promovarea transparenței, autoritățile pot maximiza beneficiile AI, reducând în același timp riscurile. O guvernanță responsabilă, aliniată la reglementările legale și bazată pe dialog cu cetățenii, este fundamentul pentru o integrare de succes a AI, contribuind la crearea unui sistem administrativ mai eficient, echitabil și orientat către nevoile societății [3].

2.5.3. Provocări etice și de reglementare în utilizarea inteligenței artificiale

Adoptarea inteligenței artificiale (AI) în administrația publică aduce avantaje notabile, precum optimizarea proceselor administrative și reducerea timpilor de răspuns, dar generează totodată provocări etice și juridice care necesită o abordare atentă și reglementări bine definite. Utilizarea AI în luarea deciziilor administrative poate spori eficiența, însă, fără un cadru normativ adecvat, există riscul ca algoritmii să producă rezultate discriminatorii sau să aplice criterii care nu respectă principiile de justiție și moralitate. De pildă, sistemele automate bazate pe modele statistice pot exclude anumite categorii de cetățeni din accesul la servicii publice, favorizând tipare generale în detrimentul evaluărilor individualizate. Acest lucru contravine normelor de echitate și transparență, fundamentale pentru buna funcționare a administrației publice.

Un alt aspect critic este lipsa transparenței în funcționarea multor tehnologii AI, deseori descrise ca „cutii negre”. Algoritmii complecși pot genera decizii automate fără ca utilizatorii, fie ei cetățeni sau funcționari publici, să înțeleagă mecanismele din spatele acestora. Această opacitate erodează încrederea cetățenilor în instituțiile publice, alimentând percepții legate de posibile abuzuri sau manipulări algoritmice. Pentru a contracara aceste riscuri, este esențială elaborarea unui cadru legal care să impună responsabilitatea clară pentru deciziile automate, să ofere dreptul la explicații accesibile pentru cei afectați și să faciliteze auditarea periodică a algoritmilor utilizați.

Un astfel de cadru ar asigura nu doar conformitatea cu principiile etice, ci și o mai mare acceptare a tehnologiilor AI în sectorul public.

De asemenea, protecția vieții private reprezintă o preocupare centrală în contextul utilizării AI, în special în aplicații care implică procesarea datelor personale sau monitorizarea comportamentului digital al cetățenilor. De exemplu, sistemele AI folosite pentru analiza datelor în scopuri de securitate sau pentru gestionarea cererilor administrative pot ridica întrebări legate de respectarea drepturilor fundamentale. Gestionarea datelor cu caracter personal trebuie să fie însoțită de mecanisme stricte de protecție, conform reglementărilor europene, cum ar fi Regulamentul General privind Protecția Datelor (GDPR). Asigurarea unui echilibru între eficiența operațională, securitatea datelor și respectarea drepturilor cetățenilor este o provocare complexă, care necesită implementarea unor politici de guvernanță solide, bazate pe transparență, responsabilitate și supraveghere umană. Numai astfel, utilizarea AI în administrația publică poate fi aliniată cu valorile democratice și cu așteptările cetățenilor.

În concluzie, implementarea inteligenței artificiale în administrația publică trebuie să fie însoțită de un cadru etic și legal bine definit, care să prevină discriminarea, să asigure transparența și să protejeze drepturile fundamentale. Prin stabilirea unor reglementări clare, promovarea auditării algoritmilor și prioritizarea vieții private, administrația publică poate valorifica beneficiile AI, minimizând în același timp riscurile asociate. Acest demers necesită o colaborare strânsă între autorități, experți în tehnologie și societatea civilă pentru a construi un sistem administrativ digital care să fie eficient, echitabil și demn de încredere.

2.5.4. Ghişeul.ro: digitalizarea plăților publice și securitatea infrastructurii IT

„ghiseul.ro” este o platformă importantă în digitalizarea administrației publice din România, care facilitează plata taxelor și impozitelor online pentru cetățeni și firme. Aceasta aduce mai multe beneficii semnificative:

- Accesibilitate și comoditate: Cetățenii pot efectua plăți ale taxelor și impozitelor direct din confortul casei lor, fără a fi nevoie să se deplaseze la ghiseele instituțiilor publice. Acest lucru economisește timp și costuri.
- Transparență și monitorizare: Platforma oferă un sistem transparent, unde utilizatorii pot vedea istoricul plăților lor și pot verifica statusul acestora. De asemenea, instituțiile publice pot urmări mai ușor plățile efectuate.
- Eficiență și reducerea birocrației: Automatizarea procesului de plată ajută la simplificarea procedurilor administrative și reduce timpul de procesare al plăților, oferind o experiență mai rapidă și mai eficientă pentru utilizatori.
- Securitate sporită: Platforma utilizează metode de securitate digitală (precum autentificarea cu certificate digitale și metode de criptare a datelor) pentru a proteja datele cetățenilor și tranzacțiile efectuate.
- Reducerea erorilor umane: Automatizarea procesului de plată reduce riscurile de eroare umană, care pot apărea în timpul procesării plăților prin metode tradiționale.

Fig. 5. Platforma „ghișeul.ro”

Autoritățile române și instituțiile implicate în gestionarea platformei iau măsuri de securitate stricte pentru a preveni astfel de incidente. De exemplu, platforma utilizează criptare SSL pentru a securiza comunicațiile între utilizatori și servere și autentificarea prin certificate digitale pentru a proteja datele de autentificare ale utilizatorilor.

Până în acest moment nu a avut loc niciun atac cibernetic asupra acestei platforme. Totuși, riscurile cibernetice nu pot fi eliminate complet, iar securitatea platformei trebuie să fie monitorizată continuu pentru a preveni eventualele breșe de securitate. Instituțiile responsabile cu gestionarea „ghiseul.ro” trebuie să se asigure că platforma este actualizată și că sunt implementate măsuri de protecție adecvate pentru a face față noilor amenințări cibernetice.

Securitatea infrastructurii IT a platformei „ghiseul.ro” joacă un rol crucial în protejarea datelor sensibile ale cetățenilor și asigurarea funcționării eficiente a serviciilor publice. Platforma este construită pe o infrastructură IT solidă și securizată, care include o serie de măsuri tehnice avansate pentru a preveni accesul neautorizat, atacurile cibernetice și pentru a proteja integritatea și confidențialitatea datelor utilizatorilor.

Unul dintre pilonii fundamentali ai securității infrastructurii IT este utilizarea firewall-urilor avansate, care sunt configurate să monitorizeze și să blocheze traficul de rețea neautorizat. Aceste dispozitive de securitate filtrează pachetele de date și permit doar traficul legitim, care corespunde regulilor stabilite de administrația platformei. În acest mod, firewall-urile protejează platforma împotriva unor atacuri de tipul „DoS” (Denial of Service) sau „DDoS” (Distributed Denial of Service), care pot afecta disponibilitatea serviciilor online. De asemenea, firewall-urile sunt configurate pentru a preveni accesul la resursele sensibile ale infrastructurii IT, asigurându-se că doar utilizatorii autorizați pot interacționa cu datele sensibile [33].

Pentru a detecta orice activitate suspectă sau potențiale amenințări, platforma utilizează soluții de monitorizare continuă a traficului de rețea. Aceste instrumente sunt capabile să analizeze în timp real fluxurile de date și să identifice modele anormale sau neautorizate care ar putea sugera un atac cibernetic. De exemplu, soluțiile de monitorizare pot semnala încercările de acces neautorizat la sisteme sau modificarea neautorizată a datelor, iar administratorii pot interveni imediat pentru a preveni orice breșă de securitate. Monitorizarea activității rețelei include analiza comportamentului utilizatorilor și identificarea oricăror încercări de infiltrare a rețelei, garantând o reacție rapidă în fața oricăror atacuri.

Într-o eră în care vulnerabilitățile software sunt frecvent exploatate de atacatori, platforma „ghiseul.ro” implementează un proces riguros de actualizare a software-ului. Aceste actualizări, cunoscute sub denumirea de „patch-uri de securitate”, sunt aplicate periodic pentru a remedia vulnerabilitățile descoperite în sistemele utilizate de platformă. Patch-urile de securitate sunt

esențiale pentru protejarea infrastructurii împotriva exploit-urilor, care sunt tehnici prin care atacatorii folosesc breșe de securitate pentru a accesa sau compromite sistemele. De asemenea, platforma beneficiază de actualizări care includ îmbunătățiri ale performanței și stabilității sistemelor, asigurându-se că infrastructura IT rămâne actualizată și funcțională.

Pentru a preveni orice tip de atacuri complexe, platforma utilizează sisteme de prevenire a intruziunilor (IPS – Intrusion Prevention Systems). Aceste sisteme sunt configurate pentru a detecta și a bloca activitățile malițioase înainte ca acestea să ajungă să afecteze infrastructura IT. De exemplu, dacă un atac cibernetic încearcă să exploateze o vulnerabilitate cunoscută sau o tehnică de phishing, IPS va detecta atacul pe baza semnăturilor comportamentale și va interveni pentru a proteja datele și aplicațiile platformei. Aceste soluții sunt integrate cu firewall-urile și sistemele de monitorizare pentru a asigura un nivel de securitate maxim.

Pentru a proteja datele, serverele pe care este găzduită platforma „ghiseul.ro" sunt configurate într-o manieră robustă din punct de vedere fizic și logic. Accesul la aceste servere este limitat la personalul autorizat și se efectuează printr-un control strict al accesului fizic, pentru a preveni orice încercare de furt sau sabotaj. În plus, echipamentele IT ale platformei sunt protejate cu parolă puternică și autentificare multifactorială pentru a preveni accesul neautorizat. Acest tip de securitate este esențial în protejarea infrastructurii, având în vedere că orice vulnerabilitate fizică poate pune în pericol întreaga securitate cibernetică a platformei.

Pentru a minimiza riscul de pierdere a datelor sau de oprire a serviciilor, platforma „ghiseul.ro" implementează soluții de redundanță și backup al datelor. Astfel, informațiile sensibile și tranzacțiile utilizatorilor sunt stocate în locații multiple și sunt protejate prin proceduri de backup regulat. În caz de incident major, cum ar fi un atac cibernetic sau o defecțiune hardware, datele pot fi restaurate rapid din copiile de rezervă, asigurând continuitatea serviciilor pentru cetățeni.

Platforma Ghişeul.ro, lansată în 2011 ca parte a Sistemului Național Electronic de Plată (SNEP), facilitează plata online a taxelor, impozitelor și amenzilor, contribuind semnificativ la reducerea birocrației și la modernizarea administrației publice din România. Conform datelor din noiembrie 2017, platforma avea 252.432 de utilizatori activi, majoritatea din zone urbane, reflectând o adopție mai mare în orașe datorită accesului sporit la internet (65,4% din gospodăriile urbane în 2016, conform INS). Ghişeul.ro permite acces 24/7, eliminând barierele de timp și distanță, și oferă utilizatorilor posibilitatea de a consulta în timp real obligațiile de plată și istoricul tranzacțiilor, sporind transparența. De asemenea, din decembrie 2016, platforma suportă plăți cu carduri emise în străinătate, adresându-se românilor din diaspora și extinzând astfel accesibilitatea serviciilor [42].

Securitatea platformei este consolidată prin măsuri tehnice avansate, cum ar fi criptarea SSL și conformitatea cu standardul PCI-DSS, asigurând protecția datelor bancare procesate exclusiv prin procesatori externi, fără stocare pe platformă. Ghişeul.ro integrează 308 instituții publice, inclusiv ANAF și primăriile din toate sectoarele Bucureștiului, permițând plata flexibilă a contribuțiilor, utilizatorii putând selecta ce taxe sau impozite să achite, spre deosebire de ghișeele fizice unde amenzile au prioritate. În ciuda acestor avantaje, adoptarea platformei rămâne limitată, doar 2,381% din utilizatorii de internet din România folosind-o în 2017, ceea ce indică un potențial semnificativ de creștere, mai ales în zonele rurale unde numărul utilizatorilor este redus sau inexistent. [42]

2.6. Dificultăți de integrare digitală pentru categoriile vulnerabile

Integrarea digitală a populației din mediul rural și a persoanelor vârstnice rămâne una dintre cele mai mari provocări în contextul digitalizării administrației publice. Deși transformarea digitală promite eficiență și acces rapid la servicii, există riscul ca o parte semnificativă a populației să fie exclusă din acest proces din cauza lipsei de infrastructură, competențe sau resurse.

În ceea ce privește accesul la tehnologie, discrepanțele dintre mediul urban și cel rural sunt evidente. În timp ce majoritatea orașelor beneficiază de conectivitate stabilă și acces la echipamente digitale moderne, zonele rurale încă suferă din cauza infrastructurii slabe. Conform unui studiu național, în 2022 doar 66% dintre gospodăriile din mediul rural aveau acces la internet, comparativ cu peste 90% în zonele urbane.

Competențele digitale reprezintă o altă barieră majoră. România ocupă ultimul loc în Uniunea Europeană în ceea ce privește abilitățile digitale de bază: doar 28% dintre persoanele între 16 și 74 de ani dețin competențele necesare pentru a folosi internetul în mod activ și sigur. Situația este și mai delicată în cazul persoanelor vârstnice, care adesea nu au avut contact anterior cu tehnologia digitală și nu beneficiază de suportul necesar pentru a o învăța [43].

Pentru a combate aceste decalaje, au fost dezvoltate inițiative locale și naționale, spre exemplu, programe care oferă cursuri gratuite pentru persoanele în vârstă din mediul urban, adaptate nivelului lor de cunoștințe. Totodată, pandemia de COVID-19 a accentuat dependența de tehnologie pentru accesarea serviciilor esențiale și a evidențiat și mai clar excluderea digitală a categoriilor vulnerabile [44].

Pentru a reduce aceste inegalități, este necesară o strategie națională coerentă de incluziune digitală, care să combine: investiții în infrastructura din zonele rurale, programe de educație digitală adaptate nevoilor specifice ale populației și parteneriate locale pentru implementarea acestora. Doar printr-o abordare integrată se poate asigura participarea echitabilă a tuturor cetățenilor la transformarea digitală a administrației publice [44].

Tabel 2. Procentul gospodăriilor fără acces la internet pe regiuni în România (2022)

Regiune	Gospodării fără acces la internet (%)
București-Ilfov	5.00%
Centru	14.8%
Nord-Vest	15.0%
Vest	8.0%
Nord-Est	23.4%
Sud-Muntenia	22.5%
Sud-Est	21.6%

Sursa: Institutul Național de Statistică

Datele privind accesul la internet în gospodăriile din România evidențiază disparități semnificative între regiunile țării. În anul 2022, regiunile Nord-Est și Sud-Vest Oltenia au înregistrat cele mai mici procente de gospodării conectate la internet, situându-se sub media națională, care era de aproximativ 89% [45]. În schimb, regiunile București-Ilfov și Vest se apropie sau chiar depășesc pragul de 95%, semnalând o digitalizare mai avansată în zonele urbane și dezvoltate economic.

Această lipsă de acces uniform la infrastructura digitală contribuie în mod direct la adâncirea decalajului digital. Populația din mediul rural, unde se concentrează cele mai multe gospodării fără internet, întâmpină dificultăți majore în accesarea serviciilor publice digitalizate, participarea la educație online, dar și în utilizarea aplicațiilor de e-guvernare. De asemenea, multe dintre aceste persoane nu dețin cunoștințele de bază privind utilizarea tehnologiilor moderne, ceea ce limitează semnificativ beneficiile transformării digitale pentru o parte importantă a cetățenilor.

Mai mult decât atât, persoanele fără acces regulat la internet sau fără competențe digitale sunt mult mai vulnerabile în fața amenințărilor cibernetice. Aceștia pot fi ușor ținte ale tentativelor de

phishing, ale fraudelor online sau ale dezinformării, deoarece nu au mijloacele tehnice sau educaționale pentru a se proteja în mediul online. În lipsa unor campanii de alfabetizare digitală și a unor investiții în infrastructură, procesul de digitalizare riscă să excludă tocmai acele categorii sociale care ar avea cel mai mult de câștigat de pe urma accesului la servicii digitale sigure și eficiente [33].

Pentru ca digitalizarea administrației publice să fie un proces incluziv și eficient, este esențială abordarea inegalităților în accesul la internet și în competențele digitale. Aceste măsuri nu doar că ar facilita utilizarea noilor platforme și servicii publice, dar ar contribui și la consolidarea rezilienței cibernetice a întregii societăți.

Capitolul 3. Cercetarea privind percepția și nivelul de pregătire în fața provocărilor digitalizării și securității cibernetice

În vederea susținerii aspectelor teoretice prezentate în capitolele anterioare și pentru a obține o imagine cât mai realistă asupra gradului de pregătire în domeniul digitalizării și al securității cibernetice în administrația publică din România, a fost realizată o cercetare de tip cantitativ, pe baza a două chestionare distincte.

Primul chestionar a fost adresat persoanelor fizice, cetățeni obișnuiți, în vederea evaluării gradului de utilizare a platformelor digitale ale administrației publice, a nivelului de încredere în securitatea acestor platforme, precum și a nivelului de conștientizare privind riscurile cibernetice.

Cel de-al doilea chestionar a fost destinat funcționarilor publici și angajaților din instituții ale administrației publice, atât la nivel local, cât și central. Scopul acestuia a fost de a analiza percepțiile și experiențele profesionale în raport cu procesul de digitalizare, competențele digitale proprii, accesul la instruire, precum și gradul de conștientizare și pregătire în fața potențialelor atacuri cibernetice.

Cercetarea a fost desfășurată în perioada martie-mai 2025, răspunsurile fiind colectate în mod anonim prin intermediul a două formulare online, realizate cu ajutorul platformei Google Forms. Rezultatele obținute oferă perspective valoroase atât din partea beneficiarilor serviciilor publice digitale, cât și din partea celor care le gestionează și implementează, contribuind la o mai bună înțelegere a provocărilor actuale în contextul transformării digitale a administrației publice din România.

3.1. Analiza generală a datelor

Pentru a evalua nivelul de digitalizare și gradul de conștientizare privind securitatea cibernetică în rândul funcționarilor publici, a fost aplicat un chestionar structurat, completat de 17 respondenți cu activitate în diferite instituții ale administrației publice. Analiza răspunsurilor oferă o imagine relevantă asupra percepțiilor și provocărilor întâlnite în procesul de digitalizare a sectorului public din România.

Profilul respondenților arată că majoritatea persoanelor chestionate (47%) au vârste cuprinse între 55 și 64 de ani și o experiență profesională de peste 10 ani în administrația publică (76%). Aceștia activează preponderent în alte instituții publice centrale, precum autorități de control sau organisme legislative.

Utilizarea platformelor digitale este ridicată: 94% dintre respondenți le folosesc zilnic în activitatea profesională. Cu toate acestea, doar 6 persoane au participat la cursuri de formare în domeniul digitalizării în ultimii 3 ani, ceea ce sugerează o lipsă de oportunități de dezvoltare profesională continuă în acest sens. Autoevaluarea competențelor digitale indică un nivel mediu spre ridicat, cu majoritatea notându-se cu 4 sau 5 din 5.

În ceea ce privește gradul de digitalizare al instituției în care activează, doar 2 respondenți o consideră complet digitalizată, în timp ce 6 afirmă că este doar parțial digitalizată și alți 5 o consideră nedigitalizată. Instrumentele digitale cel mai frecvent utilizate sunt aplicațiile din suita Microsoft Office, emailul, platformele de videoconferință și semnătura electronică. Aplicațiile specializate, precum sistemele ERP sau cele de e-learning, sunt utilizate într-o proporție mai redusă.

Percepția asupra impactului digitalizării este în general pozitivă: 53% consideră că aceasta a îmbunătățit în mare măsură activitatea profesională. Totuși, sunt identificate mai multe obstacole în procesul de transformare digitală, printre care se regăsesc: lipsa instruirii adecvate a personalului, infrastructura IT deficitară, lipsa fondurilor și reticența la schimbare a angajaților.

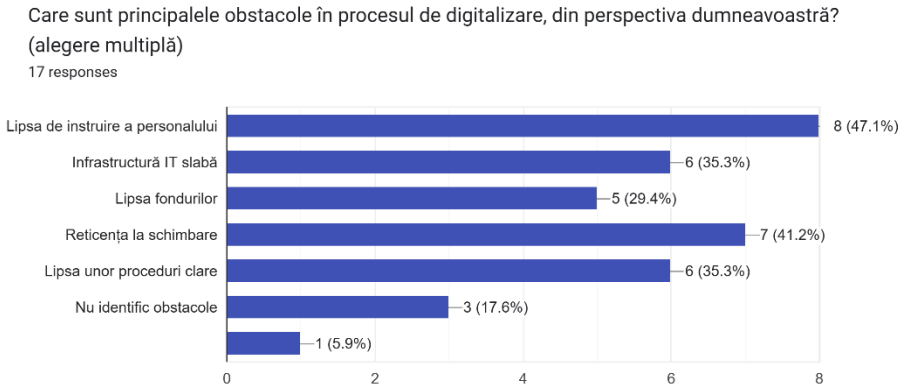


Fig 6. Procente obțiunute cu privire la obstacolele din prpcesul de digitalizare

În domeniul securității cibernetice, 47% dintre respondenți declară că sunt puțin informați cu privire la amenințările cibernetice, în timp ce 41% se consideră bine sau foarte bine informați. Cu toate acestea, doar o treime din respondenți au beneficiat de instruire periodică în acest domeniu, iar 53% afirmă că instituția în care activează este doar parțial pregătită pentru a face față incidentelor cibernetice.

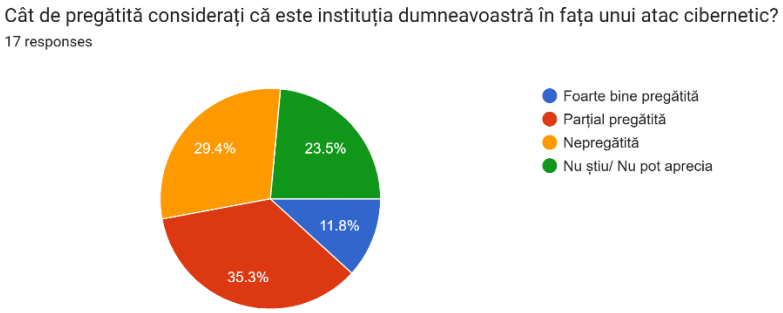


Fig 7. Procente cu privire la nivelul de pregătire al instituțiilor

Graficul arată că doar 11,8% dintre respondenți consideră instituția „foarte bine pregătită” pentru un atac cibernetic, în timp ce 35,3% o consideră doar „parțial pregătită” și 29,4% „nepregătită”. Acest lucru indică o încredere redusă în capacitatea instituțiilor publice de a face față amenințărilor cibernetice, confirmând preocupările exprimate în ipoteza ta 1.

Cele mai frecvent menționate măsuri de protecție existente sunt soluțiile antivirus și backup-urile regulate, însă mecanisme mai avansate, precum autentificarea multifactorială, sunt mai puțin

răspândite. Niciunul dintre respondenți nu a fost implicat direct sau martor la un incident cibernetic, ceea ce ar putea indica fie o bună protecție până în prezent, fie o subraportare a acestor cazuri.

Accesul la echipamente IT este aproape universal (94%), dar interacțiunea digitală cu cetățenii este redusă: 41% nu utilizează deloc platforme digitale pentru comunicare externă, iar 29% le utilizează doar ocazional.

În ceea ce privește percepția riscurilor, majoritatea consideră că digitalizarea implică riscuri suplimentare pentru securitatea datelor. Cu toate acestea, 65% dintre respondenți afirmă că se simt pregătiți să recunoască tentativele de atac cibernetic, cum ar fi phishing-ul sau accesul neautorizat. De asemenea, 94% dintre participanți se consideră pregătiți, într-o anumită măsură, pentru cerințele impuse de digitalizarea proceselor administrative.

În final, opiniile privind viitorul digitalizării administrației publice în România sunt împărțite: 47% dintre respondenți estimează că digitalizarea completă va fi atinsă în 5–10 ani, în timp ce 41% consideră că va fi nevoie de mai mult de un deceniu pentru atingerea acestui obiectiv.

Această analiză evidențiază un decalaj între utilizarea frecventă a tehnologiei și nivelul relativ scăzut de pregătire și instruire în domenii cheie precum securitatea cibernetică. Totodată, se conturează o nevoie urgentă de investiții în infrastructură, formare continuă și campanii de conștientizare care să susțină tranziția digitală a administrației publice românești.

Rezultatele obținute în urma aplicării chestionarului adresat funcționarilor publici relevă o serie de aspecte semnificative privind nivelul actual al digitalizării și gradul de conștientizare asupra importanței securității cibernetice în administrația publică din România. Deși tehnologia digitală este utilizată pe scară largă în activitatea zilnică, se remarcă deficiențe considerabile în ceea ce privește formarea profesională continuă și implementarea unor măsuri solide de protecție împotriva riscurilor cibernetice.

Majoritatea respondenților declară că folosesc frecvent platforme digitale și se consideră pregătiți pentru provocările impuse de digitalizare. Cu toate acestea, percepția asupra gradului de digitalizare al instituțiilor este preponderent rezervată, fiind considerat mai degrabă parțial decât complet. În plus, lipsa instruirii sistematice în domeniul securității cibernetice și aplicarea limitată a unor măsuri avansate de protecție denotă o vulnerabilitate considerabilă în fața amenințărilor digitale.

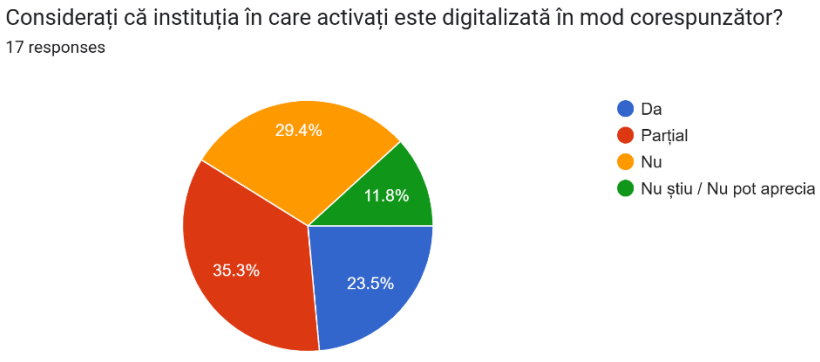


Fig 8. Digitalizarea corespunzătoare al instituțiilor

Prin urmare, concluzia care se desprinde este că procesul de digitalizare este în plină evoluție, dar necesită o direcție mai bine coordonată și strategică. Este esențială o investiție constantă în infrastructura IT, programe de formare dedicate personalului și dezvoltarea unor politici clare și

eficiente în domeniul securității cibernetice. Doar printr-o astfel de abordare integrată se poate construi o administrație publică modernă, sigură și adaptată exigențelor erei digitale.

Pentru a înțelege percepția cetățenilor asupra platformelor digitale utilizate de administrația publică din România, dar și gradul de încredere în securitatea acestora, a fost aplicat un chestionar cu 88 de respondenți. Acesta a vizat aspecte demografice, nivelul competențelor digitale, utilizarea serviciilor publice online, percepția privind protecția datelor cu caracter personal și încrederea în diverse tipuri de platforme digitale.

Majoritatea respondenților se încadrează în categoriile de vârstă 26–35 de ani (37.5%) și 36–45 de ani (29.5%), reflectând o populație activă, aflată în plin proces de interacțiune cu administrația publică. Distribuția de gen este relativ echilibrată, iar nivelul de studii este preponderent mediu și superior (liceal, universitar, postuniversitare (44.3%). Majoritatea respondenților sunt angajați, ceea ce sugerează un grad crescut de expunere la tehnologie și la interacțiuni cu instituții publice în mediul digital. În ceea ce privește venitul lunar net, intervalul cel mai frecvent raportat este 3001–5000 RON (42%), reflectând o clasă de mijloc cu acces stabil la resurse digitale (internet, dispozitive mobile, aplicații online).

Toți respondenții dispun de acces la internet acasă, iar peste 90% utilizează zilnic internetul, în special prin intermediul telefonului mobil, urmat de laptopuri și computere personale. În ceea ce privește competențele digitale de bază, participanții au apreciat nivelul propriu de cunoștințe la valori ridicate, scorul 5 (din 5) fiind cel mai frecvent selectat. Aceste date indică un grad înalt de alfabetizare digitală (70.5%).

Pe lângă competențele generale, majoritatea respondenților s-au declarat capabili să efectueze sarcini digitale specifice: instalarea de aplicații, utilizarea emailului, completarea de formulare online, crearea de conturi, resetarea de parole. Acest nivel ridicat de autonomie digitală constituie un element favorabil în ceea ce privește digitalizarea serviciilor publice și adoptarea acestora la scară largă.

Rezultatele arată că majoritatea respondenților au cunoștință despre existența unor platforme digitale precum Ghișeul.ro, Spațiul Privat Virtual (SPV), ROeID sau e-guvernare.ro. Aproximativ 60% dintre aceștia au declarat că au folosit cel puțin una dintre aceste platforme.

Platformele cel mai frecvent utilizate sunt Ghișeul.ro și SPV, în principal pentru plata taxelor, impozitelor și accesarea de informații fiscale. Experiența de utilizare a fost descrisă drept facilă de majoritatea respondenților, ceea ce sugerează că dificultățile tehnice nu reprezintă principalul obstacol în adoptarea serviciilor publice digitale.

Printre principalele motive pentru neutilizarea platformelor digitale, respondenții au menționat:

- lipsa de informare privind existența și funcționalitatea acestora;
- reticența de introducere date personale într-un mediu perceput ca nesigur;
- preferința pentru interacțiunea directă cu instituțiile, din considerente de încredere.

Îmbunătățirile propuse de participanți includ simplificarea interfeței platformelor, extinderea funcționalităților, introducerea de ghiduri de utilizare accesibile și campanii de informare privind beneficiile și siguranța utilizării acestora. De asemenea, s-a evidențiat nevoia unei mai bune asistențe tehnice în cazul dificultăților întâmpinate (45.5%).

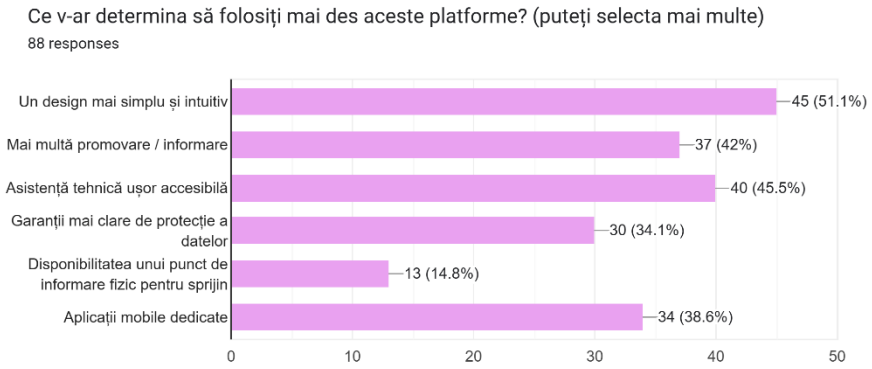


Fig 9. Ce i-ar determina pe cetățeni să folosească platformele

Rezultatele arată că peste jumătate dintre respondenți ar folosi mai des platformele digitale dacă acestea ar avea un design mai intuitiv, ceea ce evidențiază nevoia de interfețe prietenoase și simplificate. De asemenea, asistența tehnică accesibilă și promovarea mai eficientă sunt esențiale pentru creșterea gradului de utilizare. Lipsa încrederii în protecția datelor și dorința de aplicații mobile dedicate indică necesitatea unor măsuri concrete de îmbunătățire a experienței utilizatorului și de creștere a încrederii în serviciile digitale publice.

Una dintre cele mai relevante secțiuni ale chestionarului a vizat percepția asupra siguranței datelor personale. Doar o treime dintre respondenți au afirmat că se simt confortabil să introducă informații sensibile precum CNP-ul sau datele bancare pe platformele administrației publice. O proporție semnificativă a declarat că nu are încredere că datele personale sunt protejate în mod adecvat de către statul român.

Datele considerate de respondenți ca fiind cele mai sensibile și mai expuse riscului includ: CNP-ul, datele bancare, adresa de domiciliu și documentele personale (scanate sau atașate). Aceste răspunsuri indică o percepție de vulnerabilitate și lipsa unei comunicări eficiente privind măsurile de protecție a datelor aplicate de instituțiile publice.

Participanții la chestionar au fost rugați să evalueze încrederea în mai multe tipuri de platforme digitale, din perspectiva securității datelor. Cele mai ridicate scoruri au fost atribuite aplicațiilor bancare și sistemelor informatice din domeniul medical. Platformele administrației publice se situează la un nivel intermediar de încredere, în timp ce rețelele sociale și magazinele online au fost percepute drept cele mai nesigure.

Această ierarhie reflectă percepția că platformele publice sunt mai sigure decât cele comerciale, dar încă nu oferă garanții suficiente pentru a inspira o încredere similară cu domeniul bancar, unde măsurile de securitate sunt mai vizibile și comunicate mai eficient.

Majoritatea respondenților au declarat că știu ce înseamnă un atac cibernetic, iar un procent mai redus a recunoscut că a fost victima unei tentative de fraudă online (48.9%). În cazul mesajelor suspecte primite prin email sau aplicații de mesagerie, comportamentul dominant este acela de a le ignora sau raporta, deși o parte a respondenților recunoaște că le deschide din curiozitate – fapt ce indică o vulnerabilitate comportamentală importantă.

Rezultatele obținute în urma aplicării chestionarului oferă o imagine relevantă asupra modului în care cetățenii percep și utilizează platformele digitale ale administrației publice din România, dar și asupra gradului de încredere pe care îl manifestă față de protecția datelor personale în mediul digital.

În primul rând, datele indică un grad înalt de alfabetizare digitală în rândul respondenților. Accesul constant la internet, utilizarea frecventă a dispozitivelor mobile și încrederea în propriile competențe tehnologice constituie fundamente solide pentru adoptarea serviciilor digitale în administrația publică.

Totodată, se constată o tendință pozitivă privind utilizarea platformelor precum Ghișeul.ro sau Spațiul Privat Virtual, iar majoritatea celor care le-au folosit raportează o experiență facilă. Cu toate acestea, nivelul general de utilizare rămâne moderat, reflectând posibile bariere legate de lipsa informării, reticența în a furniza date personale online și preferința pentru interacțiunea directă cu instituțiile publice.

Una dintre cele mai semnificative concluzii vizează încrederea în protecția datelor personale. Chiar dacă respondenții demonstrează un comportament digital activ, nivelul de încredere în capacitatea statului de a proteja aceste date este relativ scăzut. Mulți participanți sunt reticenți în a furniza informații sensibile în mediul online, ceea ce sugerează o percepție deficitară a securității cibernetice în sectorul public.

De asemenea, se remarcă o conștientizare destul de ridicată a riscurilor cibernetice, inclusiv a fenomenului phishing. Cu toate acestea, unele comportamente raportate – cum ar fi deschiderea mesajelor suspecte „din curiozitate" – indică o vulnerabilitate reală ce necesită atenție, în special din perspectiva educației digitale și a formării continue.

3.1. Verificarea ipotezelor în urma răspunsurilor obținute

„Digitalizarea administrației publice facilitează creșterea eficienței operaționale, însă amplifică riscurile asociate securității cibernetice."

Rezultatele colectate din ambele chestionare susțin în mod clar această ipoteză. Din perspectiva angajaților din instituțiile publice, 55,9% consideră că digitalizarea a contribuit la îmbunătățirea activității instituției, iar 32,4% apreciază că acest impact este parțial. Acest lucru indică faptul că procesele administrative au devenit mai eficiente, în special prin utilizarea instrumentelor de lucru digitale, comunicarea rapidă și accesul la documente în format electronic.

Pe de altă parte, 76,5% dintre funcționari afirmă că digitalizarea implică riscuri suplimentare privind securitatea informațiilor, ceea ce subliniază o conștientizare larg răspândită a vulnerabilităților generate de tranziția digitală. De asemenea, aproape 65% dintre respondenți consideră instituția lor vulnerabilă sau parțial vulnerabilă la atacuri cibernetice, iar 35,3% au declarat că au fost martori sau implicați într-un incident cibernetic.

Din partea cetățenilor, 53,1% afirmă că nu au încredere să introducă date personale în platformele digitale ale administrației publice, iar 28,1% consideră că statul nu protejează în mod adecvat aceste date. Chiar dacă platformele precum Ghișeul.ro și SPV sunt utilizate frecvent, gradul de încredere în securitatea acestora rămâne limitat.

Aceste date demonstrează că, deși digitalizarea aduce beneficii clare în ceea ce privește eficiența administrativă, aceasta nu este însoțită în mod proporțional de mecanisme robuste de securitate cibernetică. Așadar, ipoteza este confirmată, evidențiind un dezechilibru între progresul digital și capacitatea instituțională de protecție împotriva riscurilor.

„Educația și conștientizarea în materie de securitate cibernetică reduc vulnerabilitățile din cadrul organizațiilor."

Această ipoteză este, de asemenea, susținută de datele obținute. Dintre funcționarii chestionați, 41,2% au participat în ultimii 3 ani la cursuri de formare în domeniul digitalizării sau securității

cibernetice, în timp ce 44,1% nu au beneficiat de niciun program de instruire. Această lipsă de formare afectează percepția riscului și capacitatea de reacție în situații reale.

Mai mult, doar 47,1% dintre angajați se consideră capabili să recunoască o tentativă de atac cibernetic, iar 41,2% spun că sunt „parțial pregătiți". Această incertitudine reflectă impactul insuficienței instruirii asupra comportamentului digital defensiv. În același timp, instituțiile care oferă instruire periodică au angajați care aplică frecvent măsuri de protecție, precum utilizarea parolelor complexe sau a autentificării multifactoriale.

În ceea ce privește cetățenii, doar o treime declară că s-ar simți în siguranță să introducă informații sensibile pe platformele publice. Comportamentele raportate — cum ar fi deschiderea mesajelor suspecte „din curiozitate" sau lipsa autentificării în doi pași — indică o vulnerabilitate comportamentală ce poate fi corectată doar prin campanii de educație digitală.

Astfel, ipoteza este confirmată: nivelul de educație și conștientizare în materie de securitate influențează direct gradul de protecție în fața amenințărilor digitale. Fără instruire constantă, vulnerabilitățile rămân active, iar riscul de eroare umană crește.

„Adoptarea tehnologiilor inovatoare și a soluțiilor bazate pe inteligență artificială asigură o protecție cibernetică completă în administrația publică."

Ipoteza 3 este formulată într-o manieră deliberat absolută pentru a testa realismul percepției asupra inovației tehnologice. Rezultatele arată că, în ciuda entuziasmului teoretic față de digitalizare, funcționarii publici sunt rezervați în a considera că tehnologia singură oferă protecție completă. Deși 29,4% estimează că digitalizarea completă va fi atinsă în următorii 5 ani și 32,4% în 5–10 ani, doar 8,8% sunt de părere că acest proces ar putea fi finalizat în mai puțin de 3 ani.

Mai mult, doar 17,6% dintre funcționari evaluează instituția lor ca fiind „foarte bine digitalizată", iar restul indică un grad de digitalizare mediu sau slab. În plus, majoritatea nu menționează utilizarea unor tehnologii avansate precum inteligența artificială, RPA (automate) sau sisteme proactive de detecție a atacurilor.

Cetățenii, de asemenea, exprimă neîncredere: 35,7% nu cred că datele lor sunt protejate în mod adecvat, iar 28,1% nu ar introduce date personale în platformele actuale. Acest nivel de percepție reflectă faptul că tehnologia, fără comunicare și transparență instituțională, nu este suficientă pentru a inspira încredere.

Prin urmare, ipoteza este infirmată în forma sa absolută. Deși tehnologiile moderne pot contribui semnificativ la securitatea cibernetică, acestea nu sunt suficiente în lipsa unei infrastructuri solide, a unor politici clare și a unui nivel adecvat de pregătire profesională în rândul personalului.

Concluzii

Lucrarea de față și-a propus să analizeze securitatea cibernetică în administrația publică din România, plecând de la premisa că digitalizarea nu poate fi separată de nevoia de protecție a informației. În contextul în care serviciile publice migrează tot mai mult în mediul online, protecția datelor, infrastructura digitală sigură și încrederea utilizatorilor devin piloni centrali ai unei administrații funcționale.

Cercetarea teoretică a arătat că digitalizarea administrației este un proces complex, interdependent cu dezvoltarea tehnologică, dar și cu realitățile instituționale și culturale. Introducerea unor sisteme informatice moderne sau a inteligenței artificiale nu garantează, în sine, o administrație mai performantă sau mai sigură. Din contră, dacă nu sunt însoțite de politici publice coerente, de competențe digitale reale și de standarde etice clare, aceste soluții pot deveni surse suplimentare de risc sau de inegalitate în accesul la servicii.

Pe plan empiric, rezultatele chestionarelor aplicate în rândul cetățenilor arată o tendință clară spre digitalizare: majoritatea respondenților utilizează internetul zilnic și au conturi bancare, ceea ce presupune un grad minim de alfabetizare digitală. În același timp, un procent semnificativ dintre ei folosesc platformele digitale ale administrației, precum Ghișeul.ro sau SPV. Totuși, în pofida acestei familiarizări, mulți cetățeni exprimă neîncredere față de siguranța datelor personale și se tem de fraude informatice. Această tensiune între utilizare și neîncredere indică faptul că digitalizarea, deși avansată tehnologic, nu a reușit încă să convingă prin securitate și transparență.

În ceea ce privește răspunsurile funcționarilor publici, analiza arată că aceștia recunosc importanța securității cibernetice, dar se confruntă cu obstacole practice precum lipsa de instruire formală, accesul limitat la specialiști IT și absența unor proceduri clare în cazul unui incident cibernetic. Aproape jumătate dintre respondenți nu au participat niciodată la un curs dedicat securității informatice, iar un număr considerabil folosesc parole slabe sau reutilizate, ceea ce confirmă vulnerabilitatea factorului uman. Cu toate acestea, majoritatea exprimă disponibilitatea de a participa la cursuri de formare și văd securitatea cibernetică ca pe o responsabilitate colectivă, nu doar a departamentului IT.

Astfel, una dintre principalele concluzii ale acestei lucrări este că securitatea cibernetică nu trebuie privită exclusiv ca un aspect tehnic, ci mai ales ca un proces continuu de adaptare organizațională și de educație. Protejarea infrastructurii digitale nu poate fi separată de competențele angajaților care o operează și de nivelul de conștientizare a riscurilor, la toate nivelurile – de la factorii de decizie la utilizatorul final.

Tehnologiile emergente, precum inteligența artificială, oferă un potențial semnificativ în detectarea timpurie a atacurilor, în optimizarea răspunsului la incidente și în automatizarea proceselor repetitive. Cu toate acestea, ele introduc noi provocări, în special legate de transparență, responsabilitate și controlul asupra deciziilor automatizate. Din perspectiva administrației publice, utilizarea AI necesită o atenție deosebită pentru asigurarea echității, respectarea principiilor etice și evitarea abuzului de putere algoritmică.

Pe fondul acestei complexități, o abordare eficientă a securității cibernetice ar trebui să combine:

- măsuri tehnice (firewall, criptare, backup automat),
- intervenții educaționale (formare continuă, testări periodice),
- soluții instituționale (centre de răspuns la incidente, audituri externe),
- și o cultură organizațională deschisă spre învățare și colaborare.

Această cercetare nu oferă un răspuns final la toate întrebările ridicate de digitalizarea administrației, și nici nu își propune să formuleze „rețete” general valabile. Dimpotrivă, rezultatele evidențiază că adevărul în domeniul securității cibernetice este mereu relativ, situat între context, resurse disponibile, voință politică și nivelul de educație al celor implicați. Tocmai de aceea, concluziile trebuie interpretate ca puncte de plecare pentru dezbatere și aprofundare, nu ca afirmații absolute.

În spiritul acestei deschideri, considerăm că viitoare direcții de cercetare ar putea include:

- studii comparative între administrațiile locale din România și alte state membre UE privind implementarea Directivei NIS2;
- analiza impactului reglementărilor europene asupra practicilor curente de securitate în instituțiile publice;
- studii de caz privind modul în care inteligența artificială a fost integrată responsabil în procese administrative;
- evaluarea eficienței instruirii angajaților publici în domeniul securității cibernetice, prin experimente sau simulări de atacuri controlate;

- cercetări longitudinale privind încrederea publicului în platformele digitale ale administrației, corelată cu percepția asupra riscurilor informatice.

În concluzie, construirea unei administrații digitale sigure nu se face doar prin investiții în tehnologie, ci mai ales prin investiții în oameni, în principii și în colaborare. Securitatea cibernetică este mai mult decât un obiectiv tehnic – este o condiție de încredere socială și de guvernare responsabilă într-o epocă digitală.

Anexa A. Chestionar adresat funcționarilor publici

Titlul chestionarului: Chestionar privind securitatea cibernetică și digitalizarea în administrația publică

I. Date generale
Q1. Varsta *
Q2. De câți ani activați în administrația publică? *
Q3. În ce tip de instituție publică lucrați? *

II. Digitalizare
Q4. Cât de des folosiți aplicații sau platforme digitale în activitatea zilnică? *
Q5. Cum evaluați nivelul dumneavoastră de competențe digitale? *
Q6. Ați participat, în ultimii 3 ani, la cursuri de formare în domeniul digitalizării sau al serviciilor electronice?
Q7. Considerați că instituția în care activați este digitalizată în mod corespunzător? *
Q8. Ce tipuri de instrumente digitale utilizați frecvent în activitatea profesională?
Q9. Considerați că digitalizarea a îmbunătățit activitatea instituției în care lucrați? *
Q10. Care sunt principalele obstacole în procesul de digitalizare, din perspectiva dumneavoastră?

III. Securitate cibernetică
Q11. Sunteți informat(ă) cu privire la riscurile cibernetice din administrația publică? *
Q12. Ați primit instruire sau informare privind securitatea cibernetică în cadrul instituției?Q13. Cât de pregătită considerați că este instituția dumneavoastră în fața unui atac cibernetic?
Q14. Ce măsuri de protecție a datelor sunt implementate în instituția dumneavoastră?
Q15. Ați fost implicat(ă) direct sau ați fost martor(ă) la un incident de securitate cibernetică în cadrul instituției dumneavoastră?
Q16. Aveți acces permanent la echipamentele IT necesare pentru desfășurarea activității?
Q17. Utilizați platforme electronice pentru comunicarea cu cetățenii? *

IV. Opinii personale
Q18. Considerați că digitalizarea implică riscuri suplimentare privind securitatea informațiilor?
Q19. Ce considerați că ar trebui îmbunătățit în instituția dvs. în domeniul securității cibernetice?
Q20. Vă simțiți pregătit(ă) să faceți față cerințelor impuse de digitalizarea administrației publice?
Q21. În ce măsură considerați că cetățenii beneficiază în prezent de pe urma digitalizării serviciilor publice?
Q22. Considerați că instituția în care lucrați este vulnerabilă la atacuri cibernetice? *
Q23. Considerați că sunteți suficient de pregătit(ă) pentru a recunoaște o tentativă de atac cibernetic (ex: e-mailuri suspecte, linkuri periculoase etc.)?
Q24. În cât timp considerați că administrația publică din România va fi complet digitalizată, folosind platforme funcționale și sigure din punct de vedere al securității cibernetice?
https://forms.gle/muziKuwtRefqtyvB8

Anexa B. Chestionar adresat cetățenilor

Titlul chestionarului: Utilizarea Tehnologiei și Percepția asupra Platformelor Digitale ale Administrației Publice

I. Informații demografice
Q1. Vârsta:
Q2. Genul:
Q3. Nivelul de studii absolvit:
Q4. Statut profesional:
Q5. Venitul lunar net (individual):

II. Competențe digitale
Q6. Aveți acces la internet în gospodăria dumneavoastră?
Q8. Cum vă descurcați în general cu tehnologia (calculatoare, telefoane, aplicații)?
Q9. Pe ce dispozitive accesați cel mai des internetul? (puteți alege mai multe opțiuni) *
Q10. Cât de autonom(ă) sunteți când vine vorba de..
Q11. Ce tipuri de aplicații sau platforme folosiți frecvent?
Q12. Apelați la ajutorul altcuiva când trebuie să folosiți o platformă online necunoscută?
Q13. Aveți cont bancar?

III. Platforme digitale publice
Q14. Ați auzit de existența platformelor online ale administrației publice (ex: Ghiseul.ro, ROeID, SPV, e-guvernare.ro)?
Q15. Ați folosit vreuna dintre aceste platforme? (puteți selecta mai multe) *
Q16. Dacă le-ați folosit, cum a fost experiența? *
Q17. Care sunt motivele pentru care NU ați folosit până acum platformele digitale publice?
Q18. Dacă ați folosit vreuna din aceste platforme, ce tip de operațiuni ați realizat pe platformele administrației publice?
Q19. Ce v-ar determina să folosiți mai des aceste platforme?
Q20. Considerați că aceste platforme sunt importante pentru digitalizarea administrației publice?
Q21. Aveți încredere să introduceți date personale (ex: CNP, venituri, documente) pe aceste platforme?

IV. Securitate și atacuri cibernetice
Q22. Știți ce este un atac cibernetic?
Q23. Ați fost vreodată victima unei tentative de fraudă online (ex: phishing, emailuri suspecte)?
Q24. Vă simțiți în siguranță atunci când folosiți internetul pentru a trimite informații personale?
Q25. Câtă încredere aveți în următoarele tipuri de platforme digitale în ceea ce privește protecția datelor personale?
Q26. Ce date personale considerați cele mai riscante dacă ar fi expuse online?
Q27. Considerați că statul român protejează suficient datele personale ale cetățenilor în mediul digital?
Q28. Cum reacționați dacă primiți un email sau mesaj suspect care pare a veni de la o instituție oficială?
https://forms.gle/mDWzTpx15FJD5Fr47

References

[1] G.-T. Samoilă, „Implementation of digital reforms in public administration through efficient management of intelligent systems,” *Smart Cities International Conference (SCIC) Proceedings,,* pp. 323-335, 11 Mar 2023.

[2] „DIGITALIZAREA ADMINISTRATIEI LOCALE DIN ROMANIA - Instrumentarul tehnic pentru digitalizarea serviciilor sociale,” *Student Papers on Smart Cities and E-Governance (SPoSC&EGOV),* 2023.

[3] E. Grabocka și E. NDOKA, „AI-driven innovation within the ICT sector,” *Smart Cities and Regional Development (SCRD),* vol. 9, nr. 1, pp. 77-97, 2025.

[4] C. Rădulescu, „Public sector renewal through ICT, a life-long learning approach,” *Smart Cities Int. Conf. (SCIC) Proceedings,* pp. 196-2002, 2021.

[5] C. Sîrbu, „Cybersecurity: information and defence against data phishing,,” *Proc. 5th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST),* vol. 1, pp. 107-110, 2024.

[6] C. Vrabie, „Convergența securității digitale,” *Smart Cities Int. Conf. (SCIC) Proceedings,* vol. 3, pp. 267-277, 2023.

[7] A.-M. Tîrziu şi A. Ciupercă, „Protecția și securitatea informațiilor la nivelul autorităților publice naționale din România,” *Smart Cities Int. Conf. (SCIC) Proceedings,* vol. 2, pp. 120-138, 2023.

[8] B. Trifan, „Impactul e-guvernării asupra administrației publice locale din România: studiu de caz – Primăria Comunei Mărașu, Județul Brăila,,” *Student Papers on Smart Cities and E-Governance (SPoSC&EGOV) Repository,* vol. 2, 2024.

[9] A. NEDELCU și A. NIMU, „Emerging trends: how is the Internet of Things (IoT) transforming our homes,” *Smart Cities International Conference (SCIC) Proceedings,,* vol. 5, pp. 78-89, 2017.

[10] Guvernul României, „Hotărârea Guvernului nr. 1321/2021 privind aprobarea Strategiei de securitate cibernetică a României pentru perioada 2022–2027 și a Planului de acțiune pentru implementarea acesteia,” Monitorul Oficial al României, Partea I, nr. 2, 3 ian. 2022, 2022.

[11] Agenția pentru Regii și Administrație Publică, „Programul GovITHub: Sprijin pentru digitalizarea administrației publice,” Agenția pentru Regii și Administrație Publică, București, 2024.

[12] C. Vrabie, „Promisiunile Inteligenței Artificiale (AI) Administrației Publice și Orașelor Inteligente,” *Smart Cities Int. Conf. (SCIC) Proceedings,* Vol. %1 din %2vol. 11, “Sustainability and Innovation”, pp. 9-46, 2023.

[13] Guvernul României, „Strategia Națională privind Agenda Digitală pentru România,” Ministerul pentru Societatea Informațională,, București, 2020.

[14] A. Matei și D. V. Dinca, „Future online learning for public administration,” *Sustainability,* vol. 14, nr. 18, 2022.

[15] Ziare.com, „Atacurile cibernetice în instituții și firme din România sunt în creștere,” *Ziare.com,* 2025.

[16] Ministerul Cercetării, Inovării și Digitalizării, „Strategia națională în domeniul inteligenței artificiale,” 2024.

[17] Ministerul Cercetării, Inovării și Digitalizării, „Strategia națională pentru dezvoltarea și susținerea Centrelor de Inovare și Digitalizare,” Monitorul Oficial al României, București, 2024.

[18] American Chamber of Commerce in Romania, „Transformarea digitală la nivelul administrației publice locale – Stadiul implementării în 2021,” în *AmCham Romania Public Administration Digitalization Conference*, București, 2021.

[19] R. C. Grigore, „Digitalizarea și Inteligența Artificială în Administrația Publică,” *Student Papers on Smart Cities and E-Governance (SPoSC&EGOV) Repository,* vol. 2, nr. 1, 2024.

[20] C. Manda, „Digitalizarea administrației publice din România – între nevoile și aspirațiile unei societăți moderne a secolului XXI,” *Smart Cities Int. Conf. (SCIC) Proceedings,* vol. vol. 9 (Speeding Up History), p. 41–61, 2023.

[21] R. Müller-Török, A. Prosser și S. Sroka, „The digital (il)literacy of local and regional politicians and civil servants – An analysis based on recent data from Romania,” *Smart Cities and Regional Development Journal,* vol. 8, nr. 2, p. 9–18, 2024.

[22] C. Vrabie, „Artificial intelligence promises to public organizations and smart cities,” *Digital Transformation. PLAIS EuroSymposium,* vol. 465, pp. 3-14, 2022.

[23] B. Fabrègue și A. Bogoni , „Privacy and Security Concerns in Smart Cities,” *Smart Cities,* vol. 6, p. 586–613, 2023.

[24] European Commission, „Cybersecurity in European Governments: Best Practices and Challenges. European Union Report,” Publications Office of the European Union, Luxembourg, 2023.

[25] Bitdefender, „Raport anual privind amenințările cibernetice,” 2023.

[26] European Union, „Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation),” Official Journal of the European Union, Luxembourg, 2016.

[27] J. O. Fayomi și Z. A. Sani, „Application and challenges of web 3.0 in smart cities,” *Smart Cities and Regional Development (SCRD) Journal,* vol. 7, nr. 1, pp. 31-42, 2023.

[28] European Union Agency for Cybersecurity (ENISA), „ENISA Threat Landscape 2023: Attack Trees for Cybersecurity Incidents,” ENISA, Heraklion, 2023.

[29] Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), „Raport anual privind atacurile cibernetice în România – 2022,” București, 2023.

[30] C. Vrabie, „E-government best cases. Cele mai interesante și de succes inițiative regăsite în plan național și internațional," *Impact Studies on E-Government and Smart Cities (ISEGOV),* vol. 4, pp. 15-48, 2015.

[31] International Organization for Standardization (ISO), „ISO/IEC 27001:2013 – Information Security Management Systems (ISMS) – Requirements," ISO, Geneva, 2013.

[32] Angenția Națională a Funcționarilor Publici, „Parteneriat strategic pentru securitatea cibernetică a României," [Interactiv]. Available: https://www.anfp.gov.ro/anunturi/anfp-dnsc-parteneriat-strategic-pentru-securitatea-cibernetica-a-romaniei/. [Accesat 2025].

[33] Centrul Național de Răspuns la Incidente de Securitate Cibernetică, „Cum să protejezi platformele publice împotriva atacurilor DDoS," *CERT-RO Bulletin,* 2023.

[34] J. Kausch-Zongo și B. Schenk, „General technological competency and usage in public administration education: An evaluation study considering on-the-job trainings and home studies," *Smart Cities and Regional Development (SCRD) Journal,* vol. 6, nr. 1, pp. 55-65, 2022.

[35] A. E. Frățilă, „CREAREA UNEI NOI PLATFORME PIAS ÎN SĂNĂTATE ȘI IMPLEMENTAREA DIRECTIVEI EUROPENE NIS 2," *Student Papers on Smart Cities and E-Governance (SPoSC&EGOV) Repository,* vol. 3, nr. 1, 2025.

[36] D. West, Digital Government: Technology and Public Sector Performance, Washington, DC: Brookings Institution Press, 2015.

[37] M. Peters, Cloud Security and Compliance: A Practical Guide, Wiley, 2020.

[38] R. von Solms și J. van Niekerk, Information Security Governance for Public Sector Organizations, Cham: Springer, 2021.

[39] G. Misuraca, Managing E-Governance: A Framework for Analysis and Planning, London: Routledge, 2022.

[40] E. Maler și P. Hallam-Baker, Digital Identity Management, Hoboken, NJ: Wiley, 2019.

[41] A. J. Menezes, P. C. Van Oorschot și S. A. Vanstone, Handbook of Applied Cryptography, Boca Raton, FL: CRC Press, 1996.

[42] A. C. Kispal, „Implementarea in Romania a agendei digitale pentru Europa. Studiu de caz: Sistemul national electronic de plata (Ghiseul. ro)," *Smart Cities International Conference (SCIC) Proceedings,* vol. 5, 2017.

[43] M. Rosca și R. Ciobanu, „Smart Cities and the rural-urban divide in Moldova: Balancing innovation and tradition," *Smart Cities and Regional Development (SCRD) Journal,* vol. 9, nr. 3, pp. 39-52, 2025.

[44] R. C. Marin, „MODERNIZAREA SERVICIULUI PUBLIC DE EDUCAȚIE PRIN DIGITALIZARE.," *Student Papers on Smart Cities and E-Governance (SPoSC&EGOV) Repository,* vol. 2, nr. 1, 2024.

[45] Institutul Național de Statistică, „Accesul populaţiei la tehnologia informaţiilor şi comunicaţiilor, în anul 2023,” Institutul Național de Statistică, București, 2023.