



Școala Națională de Studii Politice și Administrative
Facultatea de Administrație Publică

E-GUVERNAREA ÎN ROMÂNIA

- lucrare de licență, specializarea Administrație Publică -

Coordonator

Conf. Univ. Dr. Cătălin VRABIE

Absolventă

Nițulescu Ionela-Denisa

**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: Nițulescu Ionela-Denisa

Data și semnătura: 22.12.2024



Cuprins

Abstract	4
Introducere	4
Întrebările / ipotezele de cercetare	5
Obiective	5
Metodologia de cercetare	5
Capitolul 1. Transformarea administrației publice prin digitalizare	6
1.1 Definiția și importanța e-guvernării	6
1.2. Platforme digitale, inteligența artificială și protejarea datelor	8
1.3. Impactul pandemiei COVID-19 asupra transformării digitale	11
Capitolul 2. Provocări actuale și condiții necesare pentru e-guvernarea în România	12
2.1. Impactul "fake news" asupra e-guvernării și încrederea în instituțiile publice	12
2.1.2. Dezinformarea în timpul pandemiei COVID-19	13
2.2. Accesul populației la internet în România	14
2.3. Atacuri cibernetice și securitatea datelor	16
2.3.1. Exemple de atacuri cibernetice	19
2.3.2. Proiect de digitalizare a atacurilor cibernetice în sectorul de sănătate	20
2.4. Dezvoltarea competențelor digitale ale funcționarilor publici	21
2.5. Beneficiile e-guvernării	22
Capitolul 3. Studiu de caz comparativ: România vs. Estonia în implementarea e-guvernării	23
3.1. E-guvernarea în Estonia	24
3.1.1. Transformarea digitală în Estonia prin programul Tiger Leap	24
3.1.2. Transformarea guvernării digitale în Estonia prin X-Road	25
3.1.3. Transformarea identității digitale în Estonia prin e-Identity	26
3.1.4. Transformarea sistemului de sănătate în Estonia prin e-Health	28
3.2. E-guvernarea în România	29
3.2.1. Implementarea Cardului Național de Sănătate în România	29
3.2.2. E-Factura și digitalizarea procesului fiscal în România	30
3.2.3. Platforma e-guvernare.ro și digitalizarea serviciilor publice	31
3.2.4. Transformarea procesului administrativ prin platforma Ghișeul.ro	31
3.2.5. E-licitație și digitalizarea procesului de achiziții publice în România	32
3.3. Comparație între România și Estonia în domeniul e-guvernării	33
Capitolul 4. Analiza rezultatelor chestionarului	34
Concluzii	38
Anexa	39
Referințe Bibliografice	43

Abstract

E-guvernarea reprezintă un concept esențial în procesul de modernizare al administrației publice din România, având scopul de a îmbunătăți eficiența și accesibilitatea serviciilor publice oferite cetățenilor. Lucrarea analizează implementarea e-guvernării în România, cu un accent pe evoluția digitalizării administrației publice și pe impactul acesteia asupra relației dintre stat și cetățeni. Obiectivele principale ale cercetării sunt de a evalua gradul de adoptare a tehnologiilor digitale în instituțiile publice din România, de a identifica beneficiile și provocările asociate acestui proces și de a propune soluții pentru îmbunătățirea implementării e-guvernării la nivel național și local. Lucrarea se bazează pe cercetări anterioare privind digitalizarea sectorului public, inclusiv studii comparate ale implementării de soluții de e-guvernare în alte state membre ale Uniunii Europene. Abordarea metodologică include analiza datelor statistice și a rapoartelor privind digitalizarea serviciilor publice, precum și un studiu de caz asupra implementării platformelor de e-servicii, cum ar fi portalurile de plăți online și sistemele de gestionare a documentelor. Printre principalele rezultate se numără progresele semnificative în oferirea de servicii digitale, precum plata impozitelor și accesul la informații publice, dar și provocările legate de accesibilitatea digitală și interoperabilitatea sistemelor. Concluziile sugerează necesitatea unui cadru legislativ clar și a unor investiții continue în infrastructura IT pentru a susține dezvoltarea unui sistem de e-guvernare eficient și sustenabil. Acestea vor sprijini nu doar administrarea mai bună a resurselor publice, ci și încrederea cetățenilor în instituțiile statului.

Cuvinte cheie: e-guvernare, digitalizare, administrație publică, România, servicii digitale

Introducere

E-guvernarea reprezintă utilizarea tehnologiilor informației și comunicațiilor (TIC) pentru a îmbunătăți funcționarea administrației publice și serviciile furnizate cetățenilor. Este un proces esențial în cadrul strategiei globale de modernizare a administrației publice, iar în contextul Uniunii Europene, România se află într-un proces continuu de integrare a soluțiilor digitale în sectorul public. Această transformare digitală vizează nu doar eficiența administrativă, dar și transparența, reducerea birocrăției, îmbunătățirea accesibilității la servicii și creșterea încrederii cetățenilor în instituțiile statului [1].

În anul 2001, prin Hotărârea Guvernului nr. 20/2001, Ministerul Comunicațiilor și Tehnologiei Informației (MCTI) a fost reorganizat, având ca atribuții elaborarea și implementarea politicilor și strategiilor în domeniul comunicațiilor și tehnologiei informației, astfel fiind un pas important în direcția reformei digitale în România [2], marcând primele etape ale implementării e-guvernării. În acest context, au fost create primele platforme online pentru furnizarea de servicii publice, cum ar fi platformele de plăți online, site-urile pentru depunerea declarațiilor fiscale și portalurile pentru accesul la informații publice. Printre inițiativele importante, a fost lansat Sistemul de Achiziții Publice (www.e-licitatie.ro) [3], a fost introdus Sistemul Electronic Național, sub forma unui portal de guvernare electronică (www.e-guvernare.ro) [4], care avea ca scop oferirea de informații și servicii electronice atât cetățenilor, cât și mediului de afaceri. Tot în aceeași perioadă, a fost lansat portalul www.ghiseul.ro [5], care permitea plata amenzilor prin internet și expedierea declarațiilor către poliție, contribuind astfel la simplificarea interacțiunii dintre cetățeni și autorități. Deși progresele au fost semnificative, România se confruntă încă cu o serie de provocări legate de digitalizarea completă a administrației publice. În acest sens, Guvernul României a adoptat mai multe strategii naționale, cum ar fi „Strategia Națională de E-guvernare 2014-2020” [6], care vizează digitalizarea întregului sector public și crearea unui cadru legislativ coerent pentru implementarea acestora.

Deși e-guvernarea în România a înregistrat progrese considerabile, procesul se confruntă cu mai multe provocări. În primul rând, infrastructura IT a instituțiilor publice nu este uniformă, iar unele zone rurale nu au acces la internet de mare viteză, ceea ce limitează accesul cetățenilor la serviciile online. În al doilea rând, există o lacună semnificativă în educația digitală a cetățenilor și funcționarilor publici, care nu sunt întotdeauna familiarizați cu utilizarea platformelor digitale. Acest lucru poate crea o barieră pentru persoanele care nu sunt obișnuite cu tehnologia, dar și

pentru angajații statului, care nu au pregătirea necesară pentru a opera eficient cu sistemele digitale.

Întrebările / ipotezele de cercetare

Lucrarea se bazează pe trei ipoteze de cercetare care urmăresc să analizeze impactul implementării e-guvernării în România. Ipotezele propuse explorează îmbunătățirea eficienței administrației publice prin digitalizare, provocările infrastructurii IT și educația digitală a funcționarilor publici, precum și impactul asupra încrederii cetățenilor în instituțiile publice.

Ipotezele sunt următoarele:

- Ipoteza 1: Implementarea e-guvernării în România va conduce la o îmbunătățire semnificativă a eficienței administrației publice, reducând timpul de procesare a cererilor și îmbunătățind accesul cetățenilor la serviciile publice;
- Ipoteza 2: Provocările legate de infrastructura IT deficitară și educația digitală insuficientă a funcționarilor publici vor continua să fie principalele obstacole în procesul de implementare a e-guvernării în România;
- Ipoteza 3: Implementarea e-guvernării în România va contribui la creșterea încrederii cetățenilor în instituțiile publice, datorită îmbunătățirii transparenței și accesibilității serviciilor guvernamentale;

Obiective

Scopul principal al acestei lucrări de licență este de a evalua impactul implementării e-guvernării asupra administrației publice din România, concentrându-se pe digitalizarea serviciilor publice și pe relația dintre stat și cetățeni. Lucrarea urmărește să ofere o analiză detaliată a gradului de adopție a tehnologiilor digitale în instituțiile publice din România și să identifice provocările și beneficiile procesului de e-guvernare.

Obiectivele specifice ale lucrării sunt:

1. Evaluarea gradului de implementare a soluțiilor de e-guvernare în instituțiile publice din România. Analiza adoptării platformelor de e-servicii (de exemplu, plăți online, gestionarea documentelor) și impactul acestora asupra eficienței serviciilor publice.
2. Identificarea beneficiilor și provocărilor în implementarea e-guvernării la nivel național și local. Studiarea avantajelor și dificultăților întâmpinate de administrațiile publice în procesul de digitalizare, inclusiv accesibilitatea digitală și interoperabilitatea sistemelor.
3. Propunerea de soluții pentru îmbunătățirea implementării e-guvernării în România. Recomandarea unor politici și strategii pentru îmbunătățirea infrastructurii IT, a formării funcționarilor publici și a cadrelor legislative necesare susținerii unui sistem eficient de e-guvernare.

Prin îndeplinirea acestor obiective, lucrarea își propune să contribuie la dezvoltarea unui cadru mai robust pentru implementarea e-guvernării în România, să sprijine adoptarea unor soluții digitale mai eficiente și să ajute la creșterea încrederii cetățenilor în instituțiile publice.

Metodologia de cercetare

Abordarea metodologică utilizată în cadrul acestei lucrări de licență se bazează pe o combinație de metode calitative și cantitative, menite să furnizeze o imagine completă asupra stadiului actual al implementării e-guvernării în România, precum și să identifice provocările și oportunitățile în digitalizarea serviciilor publice. Scopul principal al metodologiei este de a analiza modul în care instituțiile publice din România au adoptat și implementat soluții de e-guvernare și impactul acestora asupra eficienței administrației publice și accesibilității pentru cetățeni.

În prima fază a cercetării, se va efectua un studiu bibliografic detaliat, care va include analiza literaturii de specialitate privind e-guvernarea, digitalizarea serviciilor publice și implementarea tehnologiilor de tip e-servicii în administrația publică. Analiza va include și rapoartele guvernamentale și documentele oficiale emise de instituțiile statului referitoare la dezvoltarea infrastructurii IT și politici publice legate de digitalizarea serviciilor publice. Această etapă va ajuta la crearea unui cadru teoretic solid pentru înțelegerea conceptelor-cheie și pentru a evalua contextul general al e-guvernării în România.

În plus, pentru a oferi o perspectivă mai largă asupra implementării e-guvernării, metodologia va include o analiză comparativă între România și alte state membre ale Uniunii Europene. Această comparație va ajuta la identificarea celor mai bune practici și soluții utilizate în alte țări, care ar putea fi adaptate și aplicate în contextul românesc. Analiza va urmări atât aspecte legate de tehnologia utilizată, cât și de reglementările legale și infrastructura existentă în fiecare țară.

Un alt element important al metodologiei va fi realizarea unui studiu de caz asupra unei platforme de e-servicii implementate în România, pentru a evalua impactul concret asupra utilizatorilor și eficiența acesteia. Studiul de caz va include analiza unui portal specific (de exemplu, portalul de plăți online pentru taxe și impozite) pentru a înțelege cum a fost implementat și ce efecte are asupra procesului administrativ, atât pentru cetățeni, cât și pentru instituțiile implicate.

Capitolul 1. Transformarea administrației publice prin digitalizare

1.1 Definiția și importanța e-guvernării

Într-o lume aflată într-o continuă digitalizare, administrațiile publice se confruntă cu provocarea de a-și adapta procesele pentru a răspunde mai eficient nevoilor cetățenilor, pentru a îmbunătăți relația dintre cetățeni și instituțiile statului. Unul dintre cele mai importante concepte care sprijină această transformare este e-guvernarea, un model administrativ bazat pe utilizarea tehnologiei informației și a comunicațiilor (TIC) . Acesta urmărește optimizarea proceselor administrative, sporirea transparenței și facilitarea interacțiunii directe dintre cetățeni și autorități. Prin dezvoltarea unor platforme digitale, e-guvernarea facilitează accesul cetățenilor la servicii publice și informații guvernamentale, reducând timpul și resursele necesare interacțiunii cu autoritățile. În plus, această strategie contribuie la modernizarea administrației și la creșterea eficienței proceselor administrative. E-guvernarea poate fi definită ca utilizarea tehnologiilor digitale pentru a îmbunătăți interacțiunea dintre cetățeni, instituțiile publice și alte entități guvernamentale. Aceasta nu se limitează doar la digitalizarea documentelor sau la crearea unor platforme online, ci presupune o schimbare fundamentală în modul în care administrația publică funcționează [7].

Principalul obiectiv al e-guvernării este creșterea eficienței și accesibilității serviciilor publice. Prin intermediul platformelor electronice, cetățenii pot realiza diverse operațiuni administrative fără a fi nevoiți să se deplaseze la ghișeele instituțiilor. De exemplu, plata taxelor și impozitelor, solicitarea de documente oficiale sau înscrierea în diverse programe guvernamentale pot fi realizate online, economisind timp și resurse atât pentru cetățeni, cât și pentru administrație. În plus, contribuie la sporirea transparenței instituționale, deoarece cetățenii au acces mai rapid la informațiile publice. Prin publicarea datelor guvernamentale pe platforme deschise, se reduce riscul corupției și se asigură un control mai mare din partea societății asupra deciziilor luate de autorități.

E-guvernarea reprezintă o provocare semnificativă pentru administrația publică globală, având scopul de a transforma relațiile între cetățeni și instituțiile statului prin utilizarea tehnologiilor informatice. Totuși, în ciuda entuziasmului inițial, implementarea sa întâmpină obstacole majore, iar succesul acestei inițiative depinde de dezvoltarea continuă a tehnologiilor și de educația corespunzătoare a specialiștilor din sectorul public. În România, instituțiile publice au început

să adopte soluții digitale pentru a îmbunătăți eficiența serviciilor publice și pentru a reduce birocrația [8].

Implementarea e-guvernării diferă de la o țară la alta, fiind influențată de infrastructura digitală existentă, strategiile naționale și nivelul de adoptare a tehnologiei în rândul populației. În România, guvernarea electronică a marcat începutul unui proces de modernizare a administrației publice prin digitalizare. Acest concept a vizat atât furnizarea de servicii publice în format electronic, cât și crearea unor mecanisme prin care cetățenii să poată contribui activ la luarea deciziilor, prin instrumente specifice democrației digitale. Cu toate acestea, dezvoltarea e-guvernării nu a fost uniformă la nivel național. Un studiu realizat de Vrabie, Antonie, Iordache și Brosșer a analizat site-urile oficiale ale municipalităților din România, constatând că, deși majoritatea autorităților locale sunt prezente online, doar un număr redus oferă platforme bine dezvoltate, capabile să asigure o interacțiune eficientă și complexă între cetățeni și administrație [9]. Aceasta subliniază necesitatea unor investiții continue în infrastructura digitală și optimizarea serviciilor electronice, astfel încât beneficiile e-guvernării să fie resimțite la toate nivelurile administrației.

Conform C. Manda, digitalizarea „echivalează cu transformarea proceselor, activităților și serviciilor prin integrarea tehnologiilor digitale în scopul de a îmbunătăți eficiența, de a crea noi oportunități și de a genera valoare economică și comercială.” [10]. În acest context, digitalizarea nu doar că permite optimizarea activităților, ci și deschide posibilități noi pentru crearea de valoare în mediul de afaceri. Astfel, prin integrarea tehnologiilor digitale, organizațiile pot inova, îmbunătăți relațiile cu clienții și partenerii și pot deveni mai competitive pe piața globală.

În contextul societății actuale, e-guvernarea devine un instrument pentru eficientizarea timpului cetățenilor. Aceasta permite realizarea de activități într-un mod mai eficient, economisind timp pentru priorități, prin oferirea accesului continuu la servicii publice, disponibile 24 de ore din 24, 7 zile pe săptămână. În plus, ajută la transparență și permite cetățenilor să obțină informații fără a interacționa cu structuri complexe ale administrației publice. Aceste soluții sunt esențiale pentru a răspunde nevoilor cetățenilor, reducând neplăcerile și nemulțumirile care pot duce la scăderea încrederii în administrația publică [11].

În contextul transformării digitale a administrației publice, România se aliniază la tendințele globale, adaptându-și sistemele administrative pentru a răspunde noilor cerințe tehnologice. Autoritatea pentru Digitalizarea României subliniază implementarea unor soluții precum SEAP, PCUe, semnătura digitală, sistemele GIS și platformele de plată online a taxelor și impozitelor, ca parte a eforturilor de digitalizare a administrației. Aceste inițiative, inclusiv programele precum Antonia - primul funcționar virtual din România, Spațiul Privat Virtual și programarea online pentru eliberarea pașapoartelor, sunt exemple semnificative de evoluție în direcția unei administrații publice moderne și eficiente. În literatura de specialitate, guvernarea electronică este văzută ca un instrument esențial pentru îmbunătățirea interacțiunii dintre stat și cetățeni, cu beneficii majore în dezvoltarea economică și socială. Totodată, participarea activă a cetățenilor în procesul de guvernare este esențială pentru sporirea încrederii și îmbunătățirea calității serviciilor publice. Cu toate acestea, implementarea guvernării electronice avansează mai lent la nivelul administrațiilor publice locale, chiar dacă tehnologiile informaționale sunt din ce în ce mai utilizate, iar cetățenii sunt familiarizați cu soluțiile digitale. Un exemplu de succes în acest sens este bugetarea participativă online în Municipiul București, care ilustrează importanța transparenței și implicării cetățenilor, utilizând platforme digitale pentru o mai bună interacțiune între stat și cetățean [12].

Digitizarea și digitalizarea sunt două concepte strâns legate, dar distincte. În timp ce digitizarea se referă la procesul de transformare a informațiilor analogice în format digital, digitalizarea este un proces mai larg, care include nu doar digitizarea documentelor, ci și integrarea acestora în sisteme informatice care permit automatizarea și optimizarea proceselor organizaționale. După ce informațiile au fost digitizate și datele au fost extrase și structurate într-o bază de date, acestea pot

fi utilizate într-o varietate de aplicații software. Digitalizarea presupune dezvoltarea unor aplicații care permit accesul la datele digitalizate, precum și gestionarea acestora într-un mod eficient și integrat. Astfel, dacă digitizarea se axează pe transformarea documentelor fizice în formate digitale, digitalizarea se concentrează pe crearea unui ecosistem informatic care facilitează utilizarea și manipularea acestor date într-un mod automatizat, cu scopul de a îmbunătăți eficiența și performanța organizațională [13].

Comisia Europeană ia măsuri pentru dezvoltarea serviciilor publice digitale transfrontaliere, ce pot aduce beneficii semnificative, precum creșterea eficienței, economii și transparență. E-guvernarea presupune mai mult decât utilizarea tehnologiilor, implicând și regândirea proceselor administrative și schimbarea comportamentului instituțiilor pentru a oferi servicii mai eficiente. În Danemarca, utilizarea facturării electronice economisește anual 150 de milioane EUR pentru contribuabili și 50 de milioane EUR pentru întreprinderi, iar la nivelul Uniunii Europene economiile anuale pot depăși 50 de miliarde EUR. În Italia, sistemele de achiziții publice electronice au redus costurile cu peste 3 miliarde EUR. De asemenea, serviciile publice digitale transfrontaliere facilitează mobilitatea cetățenilor în UE, permițându-le să interacționeze mai ușor cu autoritățile din alte țări. Comisia Europeană promovează platforme europene interoperabile, creând un cadru comun pentru gestionarea identității electronice a cetățenilor și sprijinind inovația prin proiecte-pilot. Totodată, sunt încurajate standardele deschise pentru a evita dependențele de furnizori specifici de tehnologii [1].

Serviciile publice electronice reprezintă unul dintre cele mai dinamice sectoare ale economiei moderne, având un impact semnificativ asupra modului în care cetățenii, sectorul privat și sectorul public interacționează și beneficiază de servicii. Dezvoltarea acestora este sprijinită de mai mulți factori care urmăresc asigurarea unui echilibru între cererea și oferta de servicii, astfel încât să se răspundă eficient nevoilor utilizatorilor. Un aspect esențial în acest proces este proiectarea serviciilor electronice, care trebuie să fie orientată către satisfacerea așteptărilor utilizatorilor, iar acest lucru se poate realiza prin aplicarea unor metode creative de proiectare. În plus, dezvoltarea competențelor digitale și asigurarea unui acces nerestricționat la aceste servicii sunt factori cheie pentru extinderea utilizării acestora. Calitatea serviciilor publice electronice este un alt factor esențial, fiind strâns legată de îmbunătățirea continuă a performanței și managementului acestora în administrația publică [14].

Transparența, ca termen, împrumutată din sensul său din optică, referindu-se la capacitatea unui obiect de a lăsa să se vadă clar conturul și detaliile obiectelor aflate pe partea opusă. În contextul administrației publice, transparența presupune deschiderea instituțiilor față de cetățeni, prin furnizarea de informații, comunicare și evaluare, pentru a asigura o mai bună înțelegere și monitorizare a activităților guvernamentale. La nivelul Uniunii Europene, cerința de transparență se reflectă în strategia de guvernare electronică (e-guvernare), care are ca obiective integrarea tuturor categoriilor sociale ca beneficiari ai serviciilor publice, utilizarea tehnologiei pentru o guvernare mai eficientă și crearea unei identități electronice interoperabile între statele membre [13]. Potrivit Organizației pentru Cooperare și Dezvoltare Economică (OCDE) [15], transparența presupune publicarea și accesibilitatea informațiilor legate de politici, decizii și acțiuni guvernamentale, care sunt esențiale pentru ca cetățenii să poată participa activ la viața politică și pentru ca instituțiile publice să poată fi ținute responsabile de acțiunile lor. În contextul e-guvernării, transparența înseamnă că procesele administrative și documentele publice sunt disponibile într-un format digital accesibil, oferind cetățenilor posibilitatea de a urmări și înțelege mai ușor activitățile guvernamentale.

1.2. Platforme digitale, inteligența artificială și protejarea datelor

Prin intermediul platformelor online cetățenii pot acum accesa informații despre actele administrative și pot depune cereri pentru diverse servicii publice, ceea ce contribuie la creșterea transparenței și reducerea riscurilor de corupție, deoarece toate tranzacțiile sunt înregistrate electronic și pot fi monitorizate în timp real. Aceste platforme online permit cetățenilor să

participe activ la procesul decizional și să semneze petiții pentru modificarea unor reglementări sau politici publice active [16]. În același timp, rețelele sociale și tehnologiile moderne au început să joace un rol tot mai important în dezvoltarea e-guvernării în România. Inițial folosite pentru scopuri personale, platformele precum Facebook, Twitter și Instagram sunt acum folosite de administrațiile locale și naționale pentru a informa rapid populația despre schimbările legislative, evenimentele guvernamentale sau măsurile de urgență. Aceste platforme nu doar că facilitează accesul cetățenilor la informații, dar permit și implicarea activă a acestora în procesul decizional, prin semnătura electronică pentru susținerea unor inițiative de schimbare a legislației sau a politicilor publice.

Abordarea Uniunii Europene privind Inteligența Artificială (AI) se concentrează pe excelență și încredere, promovând cercetarea și dezvoltarea în domeniu, în timp ce asigură respectarea drepturilor fundamentale și protecția cetățenilor. În acest context, Comisia Europeană a lansat mai multe inițiative, cum ar fi pachetul din 2021 privind AI, care include un cadru de reglementare și măsuri de sprijin pentru IMM-uri și start-upuri din domeniul AI. De asemenea, inițiativa „GenAI4EU” încurajează adoptarea AI generative în diverse sectoare industriale. Strategia europeană promovează excelența prin coordonarea investițiilor publice și private și sprijinirea cercetării și dezvoltării în domeniu [17].

Conform NASA, inteligența artificială (AI) se referă la sisteme informatice capabile să îndeplinească sarcini complexe care, în mod obișnuit, necesită abilități umane, cum ar fi raționamentul, luarea deciziilor, crearea și altele. AI include orice sistem artificial care poate îndeplini sarcini în condiții variabile și imprevizibile, cu o supraveghere umană minimă, și care poate învăța din experiență și îmbunătăți performanța prin expunerea la seturi de date. Aceste sisteme pot fi dezvoltate prin software, hardware sau alte contexte și sunt capabile să rezolve sarcini ce necesită percepție, planificare, învățare, comunicare sau acțiune fizică de tip uman. Ele sunt adesea concepute pentru a gândi sau a acționa asemenea oamenilor, folosind arhitecturi cognitive și rețele neuronale, și includ tehnici precum învățarea automată pentru a apropia sarcini cognitive. În cele din urmă, sistemele AI sunt concepute pentru a acționa rațional, cum ar fi agenți software inteligenți sau roboți, care ating scopuri folosind percepție, planificare, raționament, învățare, luarea deciziilor și acțiune [18].

În cadrul procesului de digitalizare a administrației publice din România, un exemplu relevant de platformă de e-guvernare este Ghișeul.ro [5] care este o platformă guvernamentală din România, lansată pentru a facilita plățile online ale taxelor și impozitelor către autoritățile publice. Aceasta permite cetățenilor să plătească diverse taxe, inclusiv taxe locale și impozite, folosind carduri bancare sau transferuri bancare, fără a fi necesar să se deplaseze la ghișeele instituțiilor publice. Platforma este disponibilă non-stop, asigurând accesibilitate din orice locație, și contribuie la reducerea birocrăției și la eficientizarea proceselor administrative. De asemenea, oferă transparență, prin posibilitatea cetățenilor de a vizualiza istoricul plăților și de a genera dovezi electronice ale tranzacțiilor. Sprijină educația financiară și digitală, însă există încă provocări legate de accesul la internet și de necesitatea de a extinde funcționalitățile platformei pentru a include mai multe servicii publice.

Un alt exemplu este Sistemul Electronic de Achiziții Publice (SEAP) [3] care reprezintă inițiativă de digitalizare a administrației publice în România, având scopul de a facilita și de a transparenta procesul de achiziții publice. Lansat inițial în anul 2006, acest sistem a fost creat pentru a asigura conformitatea procedurilor de achiziții publice cu normele și reglementările europene. Platforma permite autorităților publice din România să lanseze proceduri de achiziție electronică, iar furnizorii și prestatorii de servicii pot depune oferte și se pot înscrie în licitații, totul într-un mediu digitalizat care reduce semnificativ riscurile de corupție și favorizează un proces mai transparent. În cadrul SEAP, toate anunțurile de licitație și rezultatele licitațiilor sunt disponibile publicului, ceea ce garantează accesibilitatea informațiilor și protejează interesele cetățenilor. De asemenea, platforma permite autorităților publice să gestioneze întregul ciclu al achiziției publice, de la publicarea anunțurilor până la semnarea și monitorizarea contractelor.

Unul dintre actele legislative în dezvoltarea e-guvernării în România este Legea nr. 161/2003, care reglementează măsurile necesare pentru accelerarea reformei economice și modernizarea administrației publice [19]. Adoptată pentru a sprijini digitalizarea și eficientizarea instituțiilor publice, legea promovează utilizarea tehnologiilor informatice în administrarea publică, facilitând accesul cetățenilor la servicii guvernamentale. De-a lungul timpului, aceasta a fost actualizată pentru a contribui la transparența administrativă și pentru a îmbunătăți interacțiunea dintre cetățeni și autoritățile publice.

Un alt aspect relevant în procesul de modernizare a administrației publice este implementarea semnăturii electronice care reprezintă o tehnologie folosită pentru autentificarea și validarea tranzacțiilor electronice, oferind o alternativă digitală semnăturii manuscrise. Ea are un cadru juridic stabilit la nivel european prin Directiva privind semnătura electronică, care permite recunoașterea acesteia ca fiind validă din punct de vedere legal în toate statele membre ale Uniunii Europene. Semnătura electronică este utilizată pentru a asigura securitatea și integritatea documentelor electronice și poate fi completată de servicii de încredere, cum ar fi marcarea timpului, sigiliul electronic, livrarea electronică și autentificarea site-urilor web, care contribuie la validitatea juridică a acestora. Aceste elemente sunt esențiale pentru furnizarea sigură a serviciilor publice electronice și facilitarea comerțului electronic, asigurându-se că documentele electronice nu au fost modificate și sunt recunoscute juridic, evitând astfel posibile litigii legate de tranzacțiile digitale [20].

Pentru a reglementa utilizarea semnăturii electronice în România, Legea nr. 455/2001 [21] privind semnătura electronică a fost adoptată pentru a asigura un cadru legal clar, care să garanteze validitatea juridică a documentelor semnate electronic. Legea reglementează modul în care semnătura electronică poate fi utilizată în tranzacțiile digitale și stabilește cerințele tehnice și procedurale pentru furnizorii de servicii de certificare. De asemenea, aceasta reglementează activitatea autorităților competente, care monitorizează și certifică prestatorii de servicii de semnătura electronică.

În contextul e-guvernării, Regulamentul General privind Protecția Datelor (RGPD) are un rol esențial, având în vedere că guvernul român, ca și alte entități publice, prelucrează și gestionează date personale ale cetățenilor în cadrul diferitelor servicii electronice. Într-o eră digitală, protecția datelor devine crucială pentru asigurarea încrederii cetățenilor în administrația publică, iar respectarea RGPD contribuie la dezvoltarea unui sistem de e-guvernare sigur și transparent. Protecția datelor personale în e-guvernare este esențială pentru garantarea confidențialității și securității informațiilor cetățenilor în România. Odată cu implementarea aceasta, autoritățile publice sunt obligate să asigure protecția datelor personale colectate prin intermediul platformelor de e-guvernare, cum ar fi cele pentru obținerea de acte administrative, accesul la servicii de sănătate, educație sau plata taxelor și impozitelor. Aceste platforme implică prelucrarea unor date sensibile ale cetățenilor, iar RGPD garantează drepturi fundamentale esențiale, cum ar fi dreptul de acces la informațiile despre prelucrarea datelor, dreptul la rectificarea acestora în cazul unor erori, dreptul de a solicita ștergerea datelor atunci când acestea nu mai sunt necesare și dreptul de a obiecta la prelucrarea datelor pe baza intereselor legitime ale autorităților. Adoptarea RGPD în cadrul administrației publice românești presupune ca autoritățile și instituțiile publice să desemneze un Responsabil cu Protecția Datelor (RPD) care să monitorizeze implementarea și respectarea reglementărilor. Astfel, instituțiile publice trebuie să fie transparente în gestionarea datelor cetățenilor, iar protecția acestora să fie prioritară în dezvoltarea și implementarea de noi platforme. Pentru a asigura conformitatea cu RGPD, autoritățile române trebuie să aplice sancțiuni în cazul în care instituțiile nu respectă reglementările privind protecția datelor. Amenziile pot ajunge până la 20 de milioane de euro sau 4% din cifra de afaceri globală a unei organizații [22].

Protecția datelor reprezintă ansamblul de strategii și procese de securitate care vizează securizarea datelor confidențiale, prevenind deteriorarea, compromiterea și pierderea acestora. Printre principalele amenințări se numără breșele de securitate și incidentele de pierdere a datelor, ce pot

fi cauzate de atacuri cibernetice, erori umane sau amenințări din interior. Breșele de date rezultă din accesul neautorizat la informații, rețele sau dispozitive, iar incidentele de pierdere includ pierderi de echipamente sau deteriorarea software-ului. Protecția datelor implică și gestionarea disponibilității acestora, asigurându-se că angajații au acces la datele necesare pentru desfășurarea activităților zilnice [23].

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) este o autoritate publică autonomă cu competență generală în domeniul protecției datelor personale, având rolul de garant al respectării drepturilor fundamentale la viață privată și protecția datelor personale, așa cum sunt statuate în documentele fundamentale ale Uniunii Europene și ale Convenției Europene pentru Apărarea Drepturilor Omului. Un moment semnificativ în acest domeniu a fost anul 2016, când Parlamentul European și Consiliul au adoptat Regulamentul General privind Protecția Datelor (GDPR), care a intrat în vigoare în mai 2018, alături de Directiva privind protecția datelor prelucrate în scopuri judiciare. Acest cadru normativ european impune o evaluare și adaptare a legislației naționale, consolidarea capacității administrative a autorității, și o cooperare eficientă cu alte autorități de protecție a datelor din Uniunea Europeană. În acest context, ANSPDCP se angajează să asigure aplicarea standardelor europene și să promoveze o cultură națională a protecției datelor, în colaborare cu autoritățile publice, organizațiile neguvernamentale și sectorul privat [24].

Regulamentul eIDAS (Electronic Identification and Trust Services) reprezintă un cadru european pentru facilitarea identificării electronice și a serviciilor de încredere în cadrul Uniunii Europene. Acesta are scopul de a asigura interacțiuni electronice mai sigure și mai eficiente între întreprinderi și administrațiile publice, independent de statul membru în care se desfășoară activitatea. Prin promovarea interoperabilității între sistemele de identificare electronică ale celor 27 de state membre ale UE, eIDAS garantează că aceste sisteme sunt reciproc recunoscute, iar serviciile de încredere furnizate de prestatori conform reglementărilor pot fi acceptate ca probe în proceduri legale. În acest context, eIDAS contribuie semnificativ la creșterea securității tranzacțiilor electronice și la eficientizarea proceselor de afaceri, prin reducerea costurilor administrative și îmbunătățirea experienței utilizatorilor. De asemenea, regulamentul facilitează tranzacțiile transfrontaliere, permițând întreprinderilor să efectueze verificări de identitate mai riguroase și să extindă încrederea în relațiile comerciale la nivel european, oferind un mediu favorabil pentru dezvoltarea economiei digitale [25].

În contextul transformării digitale, securitatea și integritatea datelor stocate devin esențiale pentru protejarea informațiilor sensibile și asigurarea funcționării neîntrerupte a sistemelor informatice. Astfel, măsurile de securitate trebuie să acopere atât securitatea fizică a echipamentelor, cât și protecția accesului la documentele arhivate prin mijloace electronice. În acest sens, instituțiile publice trebuie să adopte măsuri tehnice și non-tehnice pentru a asigura o protecție adecvată împotriva riscurilor cibernetice, cum ar fi atacurile externe sau pierderea datelor. Printre aceste măsuri esențiale se numără implementarea de firewall-uri care protejează infrastructura rețelei de accesul neautorizat. Firewall-urile sunt configurate astfel încât să permită doar accesul la serviciile de rețea necesare, reducând astfel vulnerabilitățile infrastructurii cibernetice. De asemenea, este crucială protejarea interfețelor administrative ale dispozitivelor de rețea și schimbarea parolelor implicite cu parole complexe și unice, precum și activarea autentificării multi-factor pentru a spori nivelul de securitate [13].

1.3. Impactul pandemiei COVID-19 asupra transformării digitale

Pandemia de COVID-19 a reprezentat o perioadă de schimbare radicală pentru întreaga lume, având un impact semnificativ asupra tuturor domeniilor de activitate, inclusiv în administrația publică. Restricțiile impuse pentru a limita răspândirea virusului au determinat o accelerare rapidă a transformării digitale, iar guvernele și instituțiile publice din întreaga lume au fost nevoite să adopte soluții tehnologice inovative pentru a asigura continuitatea serviciilor esențiale. În România, pandemia a forțat companiile și instituțiile să adopte rapid soluții digitale pentru a

asigura continuitatea activităților precum munca de la distanță și utilizarea platformelor de videoconferință (precum Zoom, Microsoft Teams).

COVID-19 este o boală infecțioasă cauzată de virusul SARS-CoV-2. Virusul a fost identificat pentru prima dată în decembrie 2019 în orașul Wuhan, China, iar răspândirea sa rapidă a determinat o pandemie globală. SARS-CoV-2 este genetic apropiat de virusul care a provocat epidemia de SARS din 2002-2004, fiind asociat inițial cu o piață din Wuhan care vindea produse acvatice și animale sălbatice. Cu toate acestea, studiile nu au confirmat rolul unor animale specifice, precum civetii sau pangolinii, ca gazde intermediare în transmiterea virusului la oameni [26]. În doar câteva săptămâni, virusul s-a răspândit rapid în alte țări, iar la 30 ianuarie 2020, World Health Organization (WHO) [27] a declarat o urgență internațională.

Până la momentul actual, la nivel global, au fost raportate 777.594.331 de cazuri confirmate de COVID-19, iar numărul deceselor a ajuns la 7.089.989. De asemenea, au fost administrate aproximativ 13.642.098.070 de doze de vaccin pentru combaterea pandemiei [28].

În urma crizei provocate de pandemie, strategia digitală a Comisiei Europene a dobândit o importanță semnificativă, având un rol în implementarea instrumentelor digitale pentru monitorizarea răspândirii virusului și pentru sprijinirea cercetării. În acest context, infrastructurile digitale și serviciile online au devenit esențiale pentru continuitatea activităților economice și sociale. O componentă importantă a acestei tranziții digitale a fost asigurarea unui mediu sigur și protejat pentru utilizatorii de internet, prin implementarea de soluții de securitate care să garanteze integritatea datelor și confidențialitatea acestora. Astfel, în perioadele de restricție, atât cetățenii, cât și întreprinderile s-au bazat pe e-guvernare, e-sănătate și servicii securizate, care au permis accesul rapid și eficient la serviciile publice, protejând în același timp identitatea utilizatorilor și asigurând încrederea în aceste platforme [29].

Pandemia a subliniat rolul tehnologiilor digitale în gestionarea crizelor de sănătate publică, instrumentele digitale fiind utilizate pentru monitorizarea și limitarea răspândirii virusului. Tehnologiile de încredere, cum ar fi aplicațiile bazate pe Bluetooth, au fost folosite pentru a monitoriza contactele și a avertiza cetățenii despre posibile expuneri la virus, facilitând, de asemenea, supravegherea medicală a pacienților. Astfel, 22 de autorități din domeniul sănătății publice au lansat aplicații de depistare și avertizare a contactilor pacienților infectați, care au contribuit la întreruperea lanțului de infectare la nivel național și transfrontalier, completând metodele tradiționale de depistare manuală a contactilor [30].

Implementarea Certificatului Digital COVID-19 al Uniunii Europene a fost un pas important în procesul de digitalizare al administrației publice din România în timpul pandemiei. Platforma a permis cetățenilor să obțină certificatul digital care atestă statutul de vaccinare, rezultatele testelor negative și starea de recuperare după infectarea cu SARS-CoV-2. Regulamentul UE privind instituirea certificatului digital al UE pentru COVID a fost valabil între 1 iulie 2021 și 30 iunie 2023. Acesta a avut scopul de a facilita libera circulație a cetățenilor europeni în contextul pandemiei de COVID-19, prin eliberarea de certificate interoperabile de vaccinare, testare și vindecare. După această perioadă, începând cu luna iunie 2023, World Health Organization (WHO) [27] a preluat sistemul UE de certificare digitală privind COVID-19, extinzându-l la nivel global [31].

Capitolul 2. Provocări actuale și condiții necesare pentru e-guvernarea în România

2.1. Impactul "fake news" asupra e-guvernării și încrederea în instituțiile publice

În ultimele decenii, digitalizarea a transformat profund modul în care guvernele interacționează cu cetățenii lor. E-guvernarea, care presupune utilizarea tehnologiilor informaționale și a internetului pentru a îmbunătăți serviciile publice și a facilita accesul la informații, a devenit un pilon esențial al administrației publice moderne. Guvernele, prin intermediul platformelor digitale, pot oferi o gamă largă de servicii online, precum acces la documente publice, plăți electronice, transparență în procesul decizional și interacțiune directă cu cetățenii. Aceste progrese nu doar că îmbunătățesc eficiența administrației publice, dar contribuie și la o guvernare mai transparentă, responsabilă și mai accesibilă pentru toți cetățenii.

Cu toate acestea, pe măsură ce digitalizarea avansează, crește și vulnerabilitatea la fenomenul dezinformării. Răspândirea rapidă a informațiilor false sau manipulative, în special prin intermediul unor canale online, reprezintă o provocare semnificativă. Dezinformarea, adesea denumită „fake news”, poate afecta profund încrederea publicului în instituțiile guvernamentale și poate distorsiona realitatea, influențând percepțiile cetățenilor și alegerea acestora în procesul electoral sau în alte decizii importante. Astfel, dezinformarea poate submina procesul democratic și poate pune în pericol eficiența e-guvernării, unde transparența și încrederea sunt esențiale.

Rețelele sociale au devenit un mediu favorabil pentru răspândirea informațiilor false, datorită vitezei cu care se diseminează conținutul și dezvoltării unor domenii de gândire foarte specializate. Platforme precum Facebook, Instagram sau Twitter sunt adesea menționate ca fiind factori care contribuie la propagarea rapidă a dezinformării, ceea ce poate avea efecte negative semnificative. Actorii care generează astfel de informații false sunt diversi, incluzând corporații, instituții guvernamentale sau persoane private, fiecare având propriile interese în diseminarea acestui tip de conținut. De exemplu, campaniile electorale din diverse țări, cum ar fi alegerile din Brazilia din 2018, cele din România din 2019 sau referendumul BREXIT din Marea Britanie, au arătat impactul semnificativ al informațiilor false asupra deciziilor politice. De asemenea, în domeniul sănătății publice, dezinformarea cu privire la eficiența și riscurile vaccinurilor anti-Covid a influențat comportamentele publicului. Astfel, atât persoanele bine informate, cât și cele care nu sunt la curent cu informațiile corecte, sunt frecvent expuse la materiale care pot influența în mod negativ alegerile și credințele acestora [32].

Dezinformarea nu provine doar din surse izolate sau din persoane bine intenționate care răspândesc zvonuri. În realitate, diverse entități – inclusiv corporații, guverne și grupuri politice – pot fi implicate în generarea și diseminarea de informații false. Aceste entități au scopuri variate: de la influențarea alegerilor și manipularea piețelor financiare, până la promovarea unor ideologii politice sau economice. În multe cazuri, corporațiile pot răspândi informații false pentru a proteja interesele lor economice sau pentru a influența consumatorii, în timp ce guvernele pot fi implicate în manipularea opiniei publice pentru a-și întări puterea politică.

2.1.2. Dezinformarea în timpul pandemiei COVID-19

Pandemia de COVID-19 a fost un fenomen global care a generat o criză de sănătate publică fără precedent, dar și un val imens de dezinformare care s-a răspândit rapid pe canalele digitale. Într-o perioadă în care informațiile corecte erau esențiale pentru gestionarea crizei, încrederea în autoritățile guvernamentale și în știință a fost serios erodată de fluxul constant de informații false, teorii ale conspirației și mituri răspândite pe platformele digitale. La începutul pandemiei, dezinformarea a avut un impact major asupra comportamentului publicului, influențând alegerile cetățenilor privind măsurile de prevenire a virusului și, ulterior, vaccinarea. Un exemplu semnificativ de dezinformare care a circulat în primele luni ale pandemiei a fost legat de presupusele „leacuri miraculoase” care ar fi putut vindeca sau preveni COVID-19. Diverse tratamente nevalidate științific, cum ar fi consumul de substanțe periculoase sau administrarea de medicamente fără dovezi de eficiență, au fost promovate intens pe rețelele sociale, punând în pericol sănătatea oamenilor.

De asemenea, în perioada inițială a pandemiei, au apărut numeroase teorii care sugerau că virusul

ar fi fost creat intenționat într-un laborator sau că guvernele ar fi ascuns informații esențiale despre răspândirea acestuia. Aceste teorii au fost propagate pe rețelele sociale, deși nu existau dovezi științifice care să susțină astfel de afirmații. Dezinformarea privind originile virusului a contribuit la frică și confuzie globală și a alimentat idei anti-guvernamentale, subminând încrederea publicului în autoritățile sanitare și în răspunsul oficial al guvernelor. Pe măsură ce informațiile false se răspândeau, mulți cetățeni au ajuns să se îndoiască de recomandările autorităților și ale experților, ceea ce a complicat procesul de implementare a măsurilor de protecție, cum ar fi purtarea măștilor sau distanțarea socială.

Un alt tip de dezinformare a vizat campaniile de vaccinare. În timp ce cercetările științifice au dovedit eficiența vaccinurilor împotriva COVID-19, numeroase informații false și teorii ale conspirației au înflorit, alimentând frica și reticența față de vaccinuri. Afirmații despre efectele adverse ale vaccinurilor, inclusiv ideea că acestea ar modifica ADN-ul sau că ar conține microcipuri, au fost răspândite pe larg pe rețelele sociale, iar aceste narațiuni au determinat un număr semnificativ de persoane să refuze vaccinarea. În multe cazuri, teama de efectele secundare și dezinformarea au împiedicat milioane de oameni să se vaccineze, contribuind astfel la o rată de vaccinare mai scăzută și la dificultăți în combaterea pandemiei.

Pandemia de COVID-19 a evidențiat un alt aspect esențial: impactul pe care platformele digitale, în special rețelele sociale, îl pot avea asupra răspândirii informațiilor. În loc ca aceste platforme să fie unelte eficiente de informare și educare a publicului, algoritmiile lor favorizează conținutul care generează mai multă interacțiune și mai multe vizualizări, adesea promovând știri sensaționaliste și informații false. Astfel, platformele au devenit terenuri fertile pentru răspândirea rapidă a dezinformării, iar utilizatorii care caută informații legate de pandemie au fost adesea expuși la mesaje contradictorii sau false, ceea ce a generat confuzie și scepticism.

În fața acestui fenomen, autoritățile și organizațiile internaționale, precum Organizația Mondială a Sănătății (OMS) [27], au încercat să combată dezinformarea prin campanii de educare și prin promovarea unor surse oficiale de informație. Cu toate acestea, pentru ca aceste inițiative să fie eficiente, a fost necesar să se adopte măsuri de reglementare a platformelor digitale și să se îmbunătățească mecanismele de monitorizare a conținutului. În unele cazuri, autoritățile au fost nevoite să aplice sancțiuni împotriva celor care răspândeau informații false în mod intenționat, iar platformele digitale au introdus instrumente pentru a limita distribuirea dezinformării. Cu toate acestea, chiar și cu aceste măsuri, dezinformarea a continuat să fie o problemă majoră pe parcursul pandemiei, demonstrând dificultatea de a controla fluxul masiv de informații în era digitală.

2.2. Accesul populației la internet în România

Conform Institutului Național de Statistică (INS), în anul 2024, 88,6% dintre gospodăriile din România au acces la rețeaua de internet de acasă. Aceasta reprezintă o creștere de 2,9 puncte procentuale față de anul anterior, ceea ce semnalează o îmbunătățire continuă a infrastructurii digitale și a accesibilității la internet.

Accesul la internet este mai răspândit în mediul urban decât în cel rural. În anul 2024, 92,5% dintre gospodăriile din mediul urban sunt conectate la internet, comparativ cu doar 83,2% în mediul rural. Diferența de 9,3 puncte procentuale reflectă disparitățile existente între zonele urbane și rurale, care pot influența accesul populației la serviciile online de administrație publică.

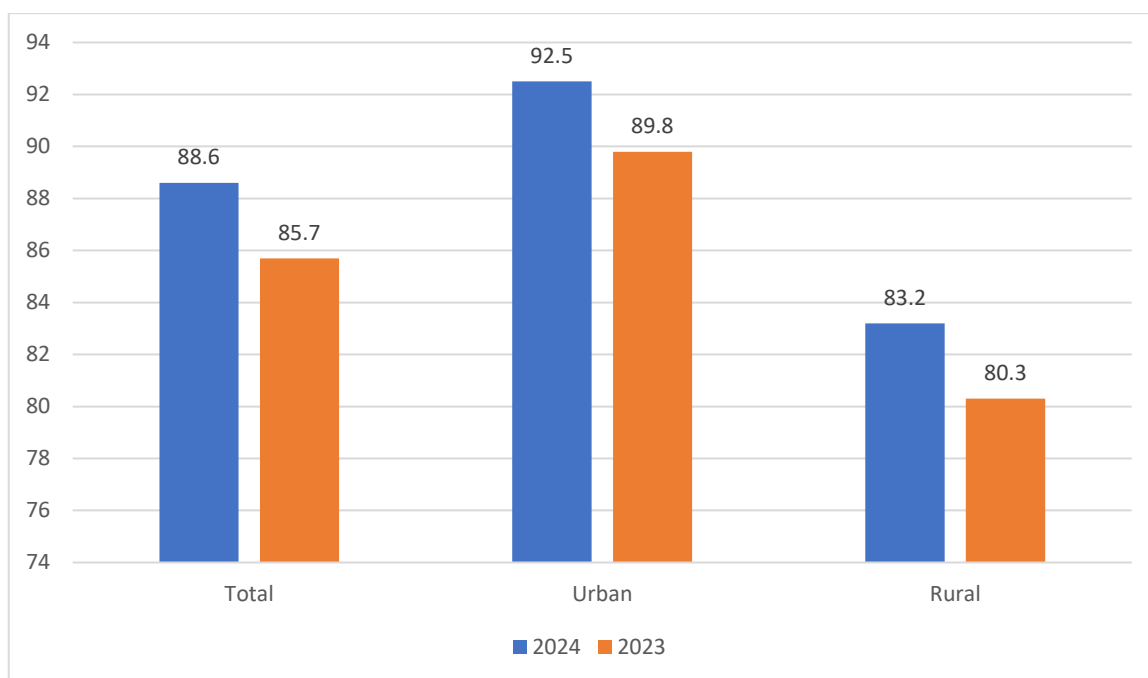


Fig. 1. Accesul la internet în gospodării

Sursa: https://insse.ro/cms/sites/default/files/com_presa/com_pdf/tic_r2024.pdf

În ceea ce privește distribuția geografică a accesului la internet, regiunea București-Ilfov înregistrează cel mai mare procent, cu 95,2% dintre gospodării având acces la internet de acasă. Alte regiuni cu valori ridicate sunt Vest (92,0%) și Nord-Vest (90,2%). Pe de altă parte, regiunile Nord-Est (85,1%) și Sud-Est (85,2%) au cele mai scăzute procente de gospodării conectate la internet [33].

Conform Institutului Național de Statistică (INS), în anul 2024, 94,7% dintre persoanele cu vârstă între 16 și 74 de ani au utilizat vreodată internetul, ceea ce reprezintă o creștere de 2,2 puncte procentuale față de anul 2023. INS raportează că dintre aceste persoane, 96,4% au utilizat internetul în ultimele 3 luni. Frecvența utilizării internetului variază semnificativ: 74,0% dintre persoanele care au folosit internetul în ultimele 3 luni l-au utilizat de mai multe ori pe zi, iar 19,5% l-au utilizat o dată pe zi sau aproape în fiecare zi.



Fig. 2. Ponderea persoanelor în vârstă de 16-74 ani care utilizează sau au utilizat vreodată internetul, pe regiuni de dezvoltare, în anul 2024

Sursa: https://insse.ro/cms/sites/default/files/com_presa/com_pdf/tic_r2024.pdf

Pe regiuni de dezvoltare, INS subliniază că ponderea celor care au utilizat sau au utilizat vreodată internetul este cea mai mare în regiunea București-Ilfov, cu 97,7%, urmată de Nord-Vest (96,6%) și Vest (96,5%). În contrast, regiunea Sud-Est are cea mai mică pondere a utilizatorilor de internet, de 92,2% [33].

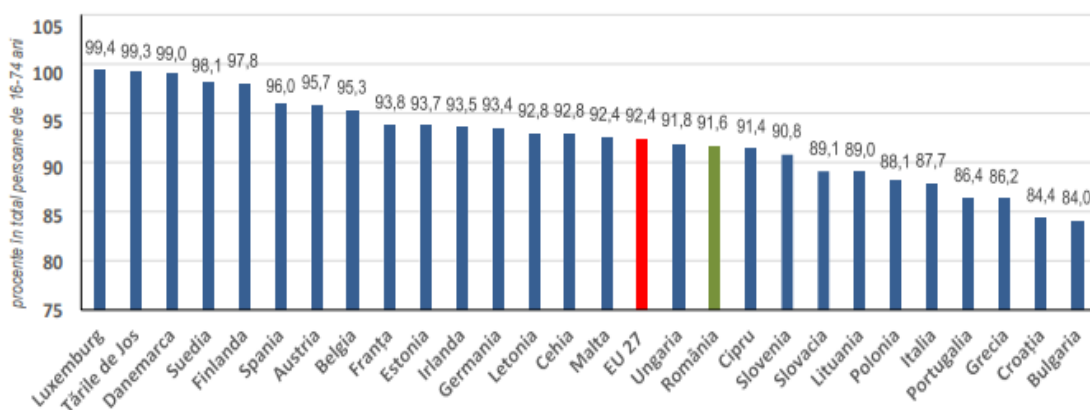


Fig. 3. Ponderea persoanelor în vârstă de 16-74 ani care au utilizat internetul în ultimele 12 luni, în Uniunea Europeană, în anul 2023

Sursa: https://insse.ro/cms/sites/default/files/com_presa/com_pdf/tic_r2024.pdf

2.3. Atacuri cibernetice și securitatea datelor

Conform C. Vrabie, în cercetarea IT&C, securitatea reprezintă un sector restrâns, deși în prezent include concepte frecvent întâlnite în mass-media, cum ar fi atacurile cibernetice asupra informațiilor și canalelor de comunicare sau furturile de identitate. Este evident că ceea ce se întâmplă acum în lumea electronică, în special în domeniul securității digitale, va avea un impact semnificativ asupra vieții noastre viitoare, un impact despre care adesea nu suntem pe deplin conștienți. Un argument solid în sprijinul acestei ipoteze este că multe dintre tehnologiile de care ne folosim astăzi au fost dezvoltate ca parte a cercetărilor finanțate de guvernele lumii, în scopuri

militare. Tehnologii precum calculatoarele, comunicațiile prin satelit și chiar Internetul au fost concepute inițial în perioadele războaielor mondiale și ale Războiului Rece, fiind astăzi parte integrantă din viața noastră cotidiană. În prezent, aceste inovații sunt atât de prezente încât nu ne putem imagina viața fără ele, iar impactul lor asupra viitorului devine tot mai greu de anticipat [34].

Având în vedere frecvența și severitatea crescută a atacurilor cibernetice, încorporarea inteligenței artificiale (AI) introduce un strat suplimentar de complexitate în ecosistemul digital, oferind în același timp strategii inovatoare pentru îmbunătățirea măsurilor de securitate cibernetică. Apariția tehnologiilor precum AI, învățarea automată și cloud computing este din ce în ce mai amestecată în cadre corporative pentru a spori eficacitatea operațională și a atenua amenințările cibernetice. Deoarece piața AI de securitate cibernetică înregistrează o creștere semnificativă, proiectată să escaladeze de la 24 de miliarde de dolari în 2023 la aproximativ 134 miliarde de dolari până în 2030, asimilarea acestor progrese tehnologice este recunoscută ca un element critic în transformarea digitală a întreprinderilor. Aplicarea AI pentru identificarea și remedierea amenințărilor cibernetice, alături de automatizarea proceselor de recrutare și personalizarea experiențelor clienților, exemplifică impactul profund al digitalizării asupra diferitelor industrii. Această transformare tehnologică nu este lipsită de pericole potențiale; cu toate acestea, perspectivele de avansare și inovare sunt considerabile, iar aplicarea inteligenței artificiale în domeniul securității cibernetice va persista ca un obiectiv critic al cercetării și dezvoltării în următorii ani [35].

Un atac cibernetic este un incident în care atacatorii vizează să deterioreze, să obțină controlul asupra sau să acceseze documente și sisteme critice dintr-o rețea de calculatoare, fie că este vorba despre o rețea de firmă sau una personală. Aceste atacuri sunt desfășurate de persoane sau organizații, având diverse motivații, inclusiv politice, infracționale sau personale, pentru a obține acces la informații sensibile sau pentru a le distruge [36].

Conform Microsoft printre tipurile de atacuri cibernetice se numără [36]:

1. **Malware:** Software-ul malițios, care include viruși, troieni, spyware și alte programe care, sub aparența unui fișier sau atașament inofensiv (de exemplu, documente criptate), permit hackerilor să pătrundă într-o rețea de computere. Aceste atacuri pot perturba grav rețelele IT și pot cauza daune considerabile în funcționarea unui sistem.
2. **Atacul distribuit de refuzare a serviciilor (DDoS):** Acest tip de atac are loc atunci când multiple sisteme compromise sunt utilizate simultan pentru a copleși un server sau o rețea, făcându-le inaccesibile pentru utilizatori. Un exemplu de astfel de atac poate include mii de feronerie pop-up sau reclame care copleșesc site-ul atacat.
3. **Phishing:** Hackerii folosesc mesaje de e-mail frauduloase care par a veni din partea unor companii de încredere, cu scopul de a obține acces la datele confidențiale ale utilizatorilor, cum ar fi parolele și informațiile bancare, pentru a le utiliza în scopuri rău intenționate.
4. **Atacuri de injectare SQL:** Acest atac exploatează vulnerabilitățile software-ului bazat pe SQL, pentru a fura, șterge sau a obține control asupra bazelor de date de la diverse aplicații sau site-uri. Infractorii cibernetici pot exploata această metodă pentru a accesa informații sensibile ale utilizatorilor, cum ar fi datele de carduri sau informațiile de autentificare ale conturilor online.
5. **Ransomware:** O formă de atac în care hackerii criptează fișierele unui utilizator sau ale unei organizații și cer o sumă de bani pentru a le decripta. Acest tip de atac a devenit din ce în ce mai frecvent și adesea se dovedește a fi extrem de costisitor pentru victime.

Într-o lume din ce în ce mai conectată, în care economia globală depinde de comunicarea și

accesarea informațiilor de oriunde și în orice moment, **securitatea cibernetică** devine esențială pentru menținerea stabilității și siguranței activităților online. Oferind protecție împotriva atacurilor cibernetice, securitatea cibernetică contribuie la menținerea confidențialității și integrității datelor, permițând oamenilor și organizațiilor să colaboreze și să inoveze fără teama de a fi expuși la riscuri semnificative. Aceasta este fundamentală nu doar pentru protejarea datelor sensibile, dar și pentru încurajarea încrederii în utilizarea tehnologiei. Soluțiile de securitate potrivite permit organizațiilor și guvernelor să adopte tehnologii avansate, îmbunătățind în acest fel comunicarea și livrarea de servicii, fără a crește riscurile de atacuri cibernetice [37].

Conform Microsoft patru din cele mai bune practici privind securitatea cibernetică sunt [37]:

1. Adoptarea unui model de securitate Zero Trust:

Pe măsură ce multe organizații implementează modele de muncă hibride, care permit angajaților să lucreze atât de acasă cât și de la birou, un model de securitate precum **Zero Trust** devine din ce în ce mai necesar. Acesta presupune că nici o solicitare de acces nu trebuie considerată implicit sigură, indiferent dacă provine din interiorul rețelei sau nu. În acest sens, este important ca fiecare acces să fie verificat riguros, iar utilizatorilor să li se acorde doar permisiuni minime pentru a accesa resursele necesare activității lor.

2. Instruirea continuă a angajaților în domeniul securității cibernetice:

În cadrul unei organizații, protecția cibernetică nu este responsabilitatea exclusivă a echipelor IT, ci a întregului personal. Multe atacuri de tip **phishing** se adresează angajaților, astfel încât educarea acestora cu privire la riscurile de securitate cibernetică este esențială. Angajații trebuie să fie capabili să identifice potențialele atacuri și să adopte măsuri preventive. Simulările periodice de phishing sunt un mod eficient de a evalua și îmbunătăți nivelul de pregătire al echipei.

3. Crearea și implementarea unor procese de securitate clare:

Reducerea riscurilor de atacuri cibernetice presupune implementarea unor proceduri standardizate care să asigure prevenirea, detectarea și gestionarea incidentelor de securitate. Aceste procese trebuie să includă actualizări regulate ale sistemelor software și hardware, astfel încât vulnerabilitățile să fie minimizate, și să ofere angajaților un set clar de instrucțiuni în caz de atac. Ghiduri internaționale, cum ar fi cele oferite de ISO 27001 sau NIST, pot fi folosite pentru a crea un cadru eficient de securitate.

4. Investiții în soluții de securitate integrate:

Tehnologia de securitate cibernetică avansează rapid, iar multe dintre soluțiile de securitate actuale includ instrumente de inteligență artificială și automatizare pentru detectarea și oprirea atacurilor fără intervenție umană. De asemenea, aceste soluții sunt concepute pentru a oferi o imagine completă a activităților din rețea, facilitând reacțiile rapide și eficiente. Este esențial ca organizațiile să implementeze soluții care protejează toate aspectele mediului IT, de la identitățile utilizatorilor, la aplicații, puncte finale și infrastructuri cloud.

Securitatea informațională este un concept care a apărut odată cu dezvoltarea tehnologiilor moderne ce permit transferul și procesarea informațiilor. În contextul actual, atât instituțiile publice, cât și companiile au conștientizat că informațiile reprezintă un bun valoros, adesea mai important decât bunurile materiale. Furtul, distrugerea, alterarea sau blocarea accesului la aceste informații pot avea consecințe grave. Cu toate acestea, în mediul informatic de astăzi, atacurile cibernetice sunt încă frecvente, iar legislația existentă nu oferă o protecție suficientă împotriva acestora. De multe ori, atacatorii rămân neidentificați, iar prejudiciile produse sunt greu de descoperit sau cuantificat [38].

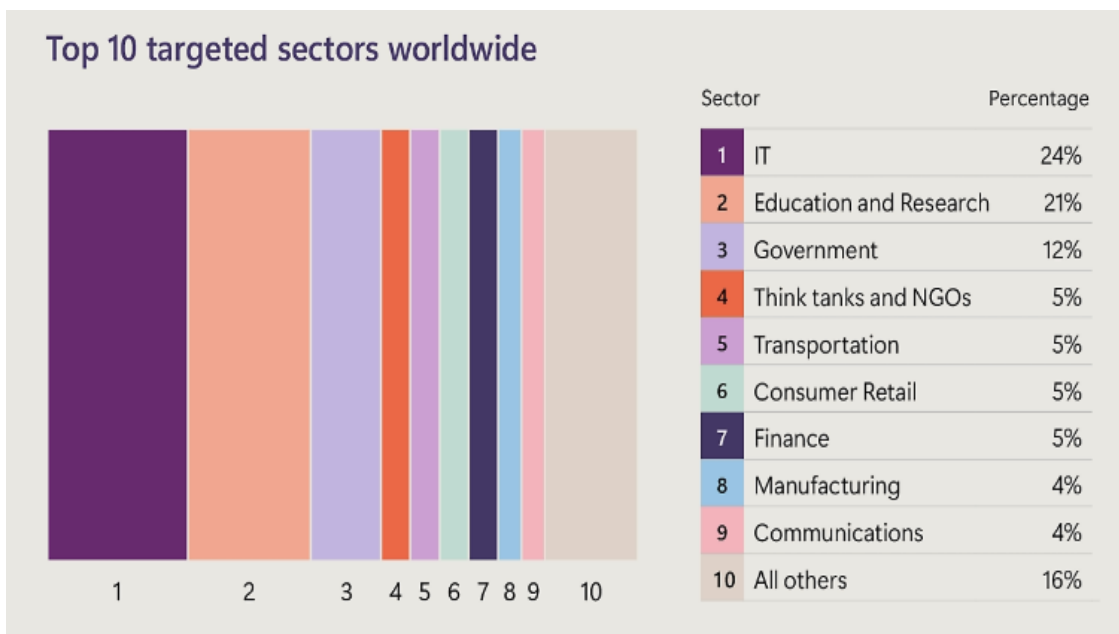


Fig. 4. Cele mai vizate 10 sectoare la nivel mondial

Sursa: <https://www.microsoft.com/ro-ro/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024#Nation-state-threat-actors>

2.3.1. Exemple de atacuri cibernetice

Phishing-ul reprezintă o tehnică de atac cibernetic în care infractorii informatici induc în eroare victimele, determinându-le să divulge date sensibile, cum ar fi informațiile personale, financiare sau de securitate. De obicei, atacatorii se bazează pe faptul că utilizatorii sunt ocupați și nu verifică cu atenție sursa mesajelor. La prima vedere, e-mail-urile de tip phishing pot părea legitime. Este esențial ca utilizatorii să își actualizeze constant programele și sistemul de operare al dispozitivelor pentru a se proteja de astfel de atacuri.

În mod special, este important să fii extrem de atent atunci când primești mesaje ce pretind a veni din partea unor instituții oficiale, cum ar fi băncile, și care solicită date sensibile (precum datele de cont sau parolele). Este recomandat să citești cu atenție mesajele și să compari adresa expeditorului cu cele din corespondențele anterioare, pentru a verifica eventuale greșeli de exprimare sau adrese suspecte. De asemenea, nu este recomandat să răspunzi la mesaje dubioase; dacă ai îndoieli, le poți redirecționa instituțiilor oficiale, folosind canalele oficiale de contact.

Un exemplu semnificativ de atac cibernetic este cazul în care atacatorii au utilizat identitatea Agenției Naționale de Administrare Fiscală (ANAF) [39] pentru a derula o campanie de phishing. Aceasta a fost raportată de către DNSC (Directoratul Național de Securitate Cibernetică) [40] și a implicat trimiterea de e-mailuri false, care păreau a proveni de la Serviciul Clienți ANAF. Mesajele includeau un link care redirecționa victimele către un site fraudulos ce imita portalul oficial ANAF. Scopul atacului era de a colecta informații personale, cum ar fi CNP-ul, numărul de telefon și datele cardului bancar, sub pretextul procesării unei rambursări fiscale.

Impactul acestui atac a fost considerabil, având atât consecințe financiare – prin furtul direct al fondurilor și posibile tranzacții recurente – cât și asupra securității datelor personale, victimele fiind expuse riscului de furt de identitate. În plus, există pericolul ca datele furate să fie utilizate în atacuri viitoare, inclusiv prin phishing direcționat [41].



Fig. 5. E-mail de tip phishing

Sursa: <https://dnsc.ro/vezi/document/scam-phishing-vishing>

2.3.2. Proiect de digitalizare a atacurilor cibernetice în sectorul de sănătate

La data de 26 martie 2025, a avut loc, la Hotel The Marmorosch din București, conferința finală a proiectului „Romanian Cyber Care Health” (RO-CCH), organizată de Directoratul Național de Securitate Cibernetică (DNSC) [40]. Evenimentul a fost dedicat consolidării securității cibernetice în sectorul medical din România și a reunit o diversitate de profesioniști din domeniul sănătății, experți în securitate cibernetică și parteneri ai proiectului. Conferința a oferit un cadru optim pentru schimbul de idei, analize și perspective asupra provocărilor cu care se confruntă sistemul medical românesc în fața amenințărilor cibernetice, precum și pentru discutarea soluțiilor necesare pentru protejarea sănătății digitale în România.

Proiectul RO-CCH a urmărit crearea unui ecosistem medical rezilient din punct de vedere cibernetic. Obiectivul central al inițiativei a fost acela de a dezvolta infrastructuri și procese care să protejeze sistemele informatice din instituțiile de sănătate, pregătind sectorul medical să răspundă eficient riscurilor cibernetice tot mai sofisticate. Prin acest proiect, s-a dorit nu doar consolidarea securității cibernetice, ci și îmbunătățirea capacității instituțiilor medicale de a preveni, identifica și răspunde rapid la posibilele atacuri cibernetice, contribuind astfel la protejarea datelor sensibile ale pacienților [42].

Principalele subiecte abordate în cadrul proiectului RO-CCH au fost dezvoltarea unor modele organizaționale eficiente pentru creșterea maturității și rezilienței cibernetice în cadrul instituțiilor medicale; strategii specifice pentru identificarea și gestionarea vulnerabilităților cibernetice care afectează acest sector esențial, alături de soluții inovative pentru formarea continuă a personalului și pentru creșterea nivelului de conștientizare în privința riscurilor legate de securitatea datelor pacienților. Experții implicați în proiect au subliniat importanța implementării unor măsuri sustenabile și eficiente pentru protejarea sănătății digitale, iar livrabilele proiectului includ instrumente și materiale de suport care pot fi folosite pentru a întări securitatea cibernetică în

instituțiile medicale din România.

În deschiderea conferinței, domnul Dan Cîmpean, Directorul DNSC, a evidențiat importanța unui parteneriat solid între sectorul public, mediul privat și instituțiile academice pentru asigurarea unui sistem medical digitalizat, sigur și rezilient la noile provocări tehnologice. În contextul unui peisaj global marcat de instabilitate geopolitică și de atacuri cibernetice tot mai sofisticate, securitatea cibernetică în domeniul sănătății trebuie să fie tratată nu doar ca o problemă tehnică, ci și ca un risc strategic. Proiectul RO-CCH a avut un rol crucial în crearea unui cadru organizațional adecvat pentru acțiuni viitoare, contribuind la formarea unei noi generații de specialiști în securitatea cibernetică și promovând o cultură organizațională bazată pe prevenirea și gestionarea rapidă a incidentelor de securitate [42].

Finalizarea proiectului RO-CCH reprezintă o realizare importantă în eforturile de creștere a rezilienței cibernetice în sectorul medical din România. Prin livrabilele sale, proiectul a furnizat instrumente specifice care răspund nevoilor curente ale instituțiilor medicale, sprijinindu-le în protejarea infrastructurii digitale și în gestionarea eficientă a riscurilor cibernetice. Toate materialele și instrumentele dezvoltate în cadrul proiectului sunt disponibile publicului pe site-ul oficial al proiectului, la secțiunea „Livrabile”, www.rocch.ro [43].

Proiectul „Romanian Cyber Care Health” (RO-CCH) a fost implementat cu sprijinul unei finanțări nerambursabile, obținută în baza contractului de finanțare nr. 101101522. Acesta a fost finanțat de Comisia Europeană prin CNECT.H – Digital Society, Trust, and Cybersecurity, în cadrul apelului DIGITAL-2022-CYBER-02-SUPPORTHEALTH, tipul de acțiune: Digital SME Support Actions, pe o perioadă cuprinsă între ianuarie 2023 și martie 2025 [42].

2.4. Dezvoltarea competențelor digitale ale funcționarilor publici

Proiectul „Competențele Digitale Avansate pentru Funcționari Publici” este o componentă esențială a Investiției 16 din Planul Național de Redresare și Reziliență (PNRR) [44] al României, având ca scop sprijinirea procesului de digitalizare a serviciilor publice. Acest proiect se concentrează pe dezvoltarea competențelor digitale avansate ale funcționarilor publici, un demers necesar pentru îmbunătățirea operațiunilor interne din administrația publică și pentru implementarea e-guvernării. Scopul principal al inițiativei este de a instrui aproximativ 30.000 de funcționari publici până în anul 2026, ceea ce reprezintă aproximativ 20% din totalul acestora. De asemenea, 2.500 de funcționari publici de conducere vor beneficia de formare în leadership și management în contextul noilor tehnologii și al transformării digitale.

Proiectul este structurat în mai multe etape și tipuri de programe de formare, ce vizează atât formarea generală a funcționarilor publici, cât și programe specializate. Printre acestea se numără cursuri de management al digitalizării administrației publice, instruire în utilizarea instrumentelor digitale pentru munca la distanță și telemuncă, colectarea și interpretarea avansată a datelor, precum și administrarea rețelelor TIC și dezvoltarea aplicațiilor web. Aceste cursuri sunt esențiale pentru adaptarea funcționarilor la cerințele impuse de transformările tehnologice din sectorul public.

Până în prezent, proiectul a înregistrat realizări semnificative, inclusiv 1.173 de protocoale de colaborare interinstituțională, ceea ce reprezintă 27% din totalul autorităților și instituțiilor publice din România gestionate prin sistemul informatic al ANFP, incluzând instituții coordonate sau aflate în subordonare.

Proiectul contribuie semnificativ la digitalizarea administrației publice, sprijinind nu doar implementarea e-guvernării, dar și reformele PNRR care includ componente de digitalizare. În plus, instruirea funcționarilor publici va reduce dependența de terți și va accelera procesul de digitalizare al instituțiilor publice. Funcționarii publici instruiți vor fi mai bine pregătiți pentru a înfrunta provocările aduse de era digitală, devenind agenți ai schimbării în mediul lor de lucru și

capabili să transmită cunoștințele dobândite colegilor lor [45].

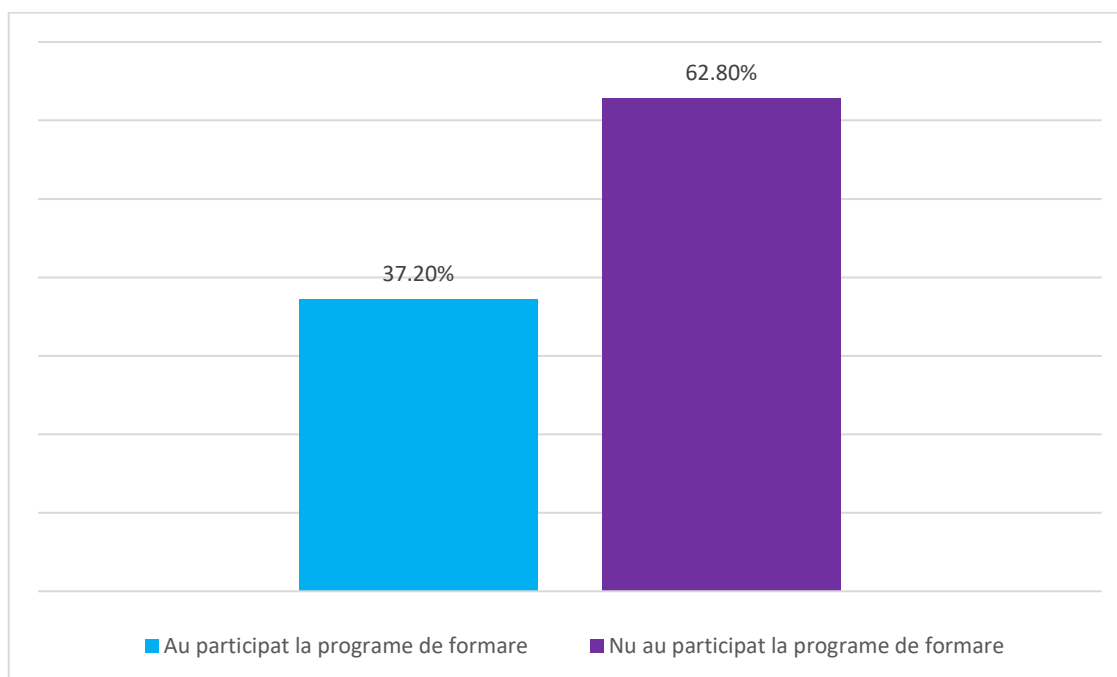


Fig. 6. Participarea funcționarilor publici la programe de formare pentru dezvoltarea competențelor digitale (ANFP, 2022)

Sursa: <https://www.anfp.gov.ro/R/Doc/2023/PNRR/Anexa%20nr.%201%20-%20Analiza%20competente%20digitale.pdf>

2.5. Beneficiile e-guvernării

Unul dintre avantajele e-guvernării este reducerea semnificativă a timpilor de așteptare și a birocrăției. În prezent, cetățenii sunt adesea nevoiți să se deplaseze la diferite ghișee, să stea la cozi și să depună personal documente pentru a obține acte sau servicii publice. Cu ajutorul tehnologiilor de informație, aceste procese devin mai rapide și mai eficiente. Documentele electronice pot circula între diverse instituții guvernamentale și pot fi validate rapid de autoritățile competente, astfel că cetățeanul poate obține documentele solicitate fără a mai fi necesar să se deplaseze repetat la ghișee. În plus, multe dintre aceste documente pot fi obținute direct în format electronic. Tehnologia informației permite ca serviciile publice să fie disponibile online 24 de ore din 24. Astfel, cetățenii pot accesa informațiile sau efectua tranzacțiile necesare de oriunde din lume, la orice oră, printr-o simplă conexiune la internet. Aceasta oferă un grad ridicat de accesibilitate pentru persoane din zone mai îndepărtate sau cu program încărcat, care nu ar fi putut altfel să ajungă la ghișeele instituțiilor publice [8].

E-guvernarea poate contribui semnificativ la reducerea impactului asupra mediului. Prin digitalizarea proceselor administrative, se reduce dependența de hârtie și se elimină necesitatea transportului fizic al documentelor sau al persoanelor către instituțiile publice. Aceasta nu doar că economisește resurse naturale, dar reduce și emisiile de carbon asociate cu transportul, având un impact pozitiv asupra sustenabilității mediului înconjurător.

Implementarea soluțiilor de e-guvernare determină o reducere semnificativă a costurilor administrative, atât pentru instituțiile publice, cât și pentru cetățeni. Digitalizarea proceselor birocratice elimină necesitatea tipăririi și gestionării documentelor fizice, reducând astfel cheltuielile asociate cu hârtia, imprimarea și arhivarea. De asemenea, utilizarea platformelor online pentru depunerea și procesarea cererilor administrative optimizează alocarea resurselor umane, permițând redistribuirea personalului către activități cu valoare adăugată mai mare. În plus, costurile indirecte, precum cele generate de deplasările la ghișee sau de timpul pierdut în așteptare, sunt considerabil diminuate, sporind eficiența administrativă și contribuind la

sustenabilitatea financiară a sectorului public [8].

Utilizarea serviciilor de e-guvernare elimină necesitatea deplasărilor frecvente la instituțiile publice, oferind cetățenilor posibilitatea de a accesa servicii administrative rapid și eficient, direct din mediul online. Un aspect esențial este reducerea timpului necesar pentru realizarea formalităților, deoarece interacțiunile cu administrația pot avea loc oricând, fără a fi condiționate de programul de lucru al instituțiilor. De asemenea, digitalizarea documentelor și posibilitatea transmiterii acestora în format electronic simplifică procesele birocratice, reducând disconfortul cauzat de manipularea documentelor fizice. În plus, prin evitarea cozilor și a timpului de așteptare, cetățenii beneficiază de o experiență mai comodă și mai eficientă în relația cu administrația publică [8].

Un alt avantaj important al e-guvernării este îmbunătățirea experienței cetățeanului în interacțiunile cu administrația publică. Platformele digitale permit cetățenilor să acceseze servicii și informații fără a mai întâmpina obstacolele birocratice tradiționale. Astfel, aceștia pot rezolva multiple aspecte administrative într-un singur loc, cu un timp de așteptare redus și o mai bună transparență. De asemenea, interfața digitală poate fi optimizată pentru a fi prietenoasă și ușor de utilizat, facilitând accesul unui public larg.

Unul dintre principalele avantaje ale e-guvernării este reducerea corupției în administrația publică, prin digitalizarea proceselor și eliminarea interacțiunii directe dintre cetățeni și funcționari. Implementarea unui sistem informatic permite depunerea documentelor și completarea solicitărilor exclusiv în format electronic, ceea ce asigură transparența și obiectivitatea procedurilor. De asemenea, identificarea electronică a utilizatorilor și păstrarea automată a înregistrărilor contribuie la aplicarea corectă a reglementărilor legale. În România, birocrăția reprezintă un factor care favorizează corupția, iar lipsa unor reguli clare privind gestionarea cazurilor poate duce la întârzieri și practici abuzive. Digitalizarea serviciilor publice combate aceste probleme prin standardizarea proceselor și prin monitorizarea acestora, astfel încât cererile să fie soluționate în mod echitabil, fără influențe externe [8].

Capitolul 3. Studiu de caz comparativ: România vs. Estonia în implementarea e-guvernării

În ultimele două decenii, digitalizarea administrației publice a devenit o prioritate majoră la nivel global și european, iar e-guvernarea s-a impus ca un element esențial pentru modernizarea statului. În contextul actual, în care accesul rapid la servicii publice eficiente, transparente și centrate pe cetățean este o cerință fundamentală, transformarea digitală nu mai reprezintă doar o opțiune, ci o necesitate strategică. Statele membre ale Uniunii Europene sunt îndemnate să implementeze politici coerente de digitalizare, astfel încât să asigure o guvernare deschisă, participativă și eficientă, în conformitate cu principiile consacrate în tratatele europene și documentele de politici publice la nivel comunitar.

În acest context, România a făcut pași importanți în direcția digitalizării administrației publice, însă procesul rămâne fragmentat, cu provocări persistente legate de infrastructura tehnologică, interoperabilitatea sistemelor, nivelul de alfabetizare digitală al funcționarilor și gradul de utilizare efectivă a platformelor de e-servicii de către cetățeni. De cealaltă parte, Estonia este considerată un model de bune practici în domeniul e-guvernării, fiind una dintre primele țări europene care a integrat digitalizarea profund în structura administrației sale. Proiecte precum e-Residency, X-Road sau votul online au plasat Estonia în topul clasamentelor privind maturitatea digitală și eficiența administrației publice.

Pornind de la aceste diferențe semnificative, capitolul de față propune o analiză comparativă între România și Estonia în ceea ce privește nivelul de implementare al e-guvernării. Studiul urmărește testarea ipotezelor formulate în prima parte a lucrării, în special cea conform căreia e-guvernarea contribuie la îmbunătățirea eficienței instituționale și la creșterea încrederii cetățenilor în

administrație. Astfel, analiza se va concentra atât pe aspectele tehnice și instituționale ale digitalizării serviciilor publice, cât și pe impactul asupra relației dintre stat și cetățeni.

Un alt aspect important în această comparație îl reprezintă gradul de maturitate digitală al fiecărui stat, analizat prin prisma indicatorilor internaționali (DESI – Digital Economy and Society Index), dar și a capacității administrative interne de a dezvolta și gestiona infrastructuri digitale eficiente. În timp ce Estonia a reușit să își construiască un ecosistem digital integrat, susținut de politici coerente și un angajament guvernamental constant, România se confruntă încă cu o lipsă de viziune pe termen lung și o implementare inegală a inițiativelor digitale la nivel național și local.

Prin această abordare comparativă, capitolul își propune nu doar să evidențieze decalajele existente între cele două state, ci și să contribuie la conturarea unor direcții strategice de dezvoltare a e-guvernării în România, în vederea eficientizării serviciilor publice, creșterii transparenței și consolidării încrederii cetățenilor în administrația publică. Totodată, lucrarea oferă un cadru analitic pentru înțelegerea modului în care bunele practici europene pot fi adaptate contextului românesc, contribuind astfel la o administrație mai modernă, mai accesibilă și mai apropiată de cetățeni.

3.1. E-guvernarea în Estonia

Estonia este adesea citată drept exemplul ideal al unei transformări digitale reușite, fiind una dintre primele țări din lume care a reușit să integreze complet tehnologia în administrația publică și în viața cotidiană a cetățenilor săi. Ceea ce face cazul Estoniei atât de interesant este contextul în care s-a produs această transformare: o țară mică, proaspăt ieșită din perioada sovietică, cu resurse financiare limitate, dar cu o voință politică fermă de a inova și de a construi un stat eficient, transparent și aproape complet digitalizat.

Estonia a devenit una dintre cele mai avansate societăți digitale din lume, datorită unei serii de evenimente cheie care au marcat dezvoltarea sa. Deși drumul parcurs nu poate fi copiat în totalitate, provocările întâmpinate și lecțiile învățate pot inspira alte națiuni să își creeze propriile soluții. În acest context, e-Estonia a transformat societatea într-una caracterizată de transparență, încredere și eficiență. Printre provocările inițiale s-a numărat construirea unui stat funcțional de la zero, fără a putea adopta birocrăția tradițională. Primul proiect major în acest sens a fost „principiile politicii informaționale estoniene”, iar un contur strategic pentru dezvoltarea IT a fost ratificat de parlament câțiva ani mai târziu. În ciuda vremurilor politice dificile, guvernul a decis să aloce 1% din PIB pentru susținerea IT-ului, stabilind astfel tehnologia ca pilon esențial în rezolvarea problemelor societale [46].

3.1.1. Transformarea digitală în Estonia prin programul Tiger Leap

După 1991, când și-a recâștigat independența, Estonia a început un proces ambițios de reconstrucție a instituțiilor și a sistemului administrativ. Lipsa infrastructurii tradiționale s-a transformat rapid într-un avantaj: autoritățile nu erau blocate de sisteme învechite, iar decizia de a "sări peste" anumite etape convenționale a permis dezvoltarea rapidă a unei guvernări digitale moderne. În acest context a apărut programul Tiigrihüpe („Leap Tiger”), lansat în 1996, care viza conectarea tuturor școlilor la internet și alfabetizarea digitală timpurie a populației. Acesta a fost primul pas dintr-o strategie pe termen lung ce a pus digitalizarea în centrul politicilor publice estoniene.

Programul Tiger Leap, a avut un rol esențial în dezvoltarea educației și digitalizării statului post-sovietic. După recâștigarea independenței, Estonia s-a confruntat cu provocări semnificative în modernizarea infrastructurii educaționale și în integrarea tehnologiei în procesul de învățământ. Programul a fost gândit să răspundă acestor nevoi, având ca scop integrarea tehnologiei în școlile

din întreaga țară și asigurarea unui acces larg la internet și la calculatoare pentru profesori și elevi.

În 1997, Ministerul Educației din Estonia a lansat programul Tiger Leap, care s-a concentrat pe trei piloni principali: distribuirea de computere și internet în școli, formarea cadrelor didactice și dezvoltarea de software educațional în limba estonă. Până la sfârșitul anului 1997, au fost distribuite 743 de calculatoare, iar școlile au primit acces la internet prin conexiuni de dial-up, fiind implementate inițiative pentru a îmbunătăți viteza și accesul online.

Pentru a sprijini cadrele didactice, Tiger Leap a organizat cursuri de formare pentru profesori, iar în anul 1997, peste 3.800 de profesori au participat la sesiuni de instruire în domeniul TIC, organizate pe parcursul a 40 de ore. Aceste cursuri au fost esențiale pentru a asigura utilizarea eficientă a tehnologiei în sălile de clasă și pentru a sprijini dezvoltarea competențelor digitale ale cadrelor didactice.

Un alt obiectiv major al programului a fost dezvoltarea de software educațional care să fie compatibil cu limba estonă, astfel încât elevii să poată învăța în mod eficient folosind resurse digitale. În acest sens, Tiger Leap a lansat proiecte de traducere și adaptare a materialelor educaționale existente și a organizat concursuri pentru dezvoltarea unor noi programe educaționale. Printre proiectele notabile se numără dezvoltarea unor manuale electronice pentru discipline precum geografia, literatura și biologia, în scopul de a facilita accesul elevilor din întreaga țară la informații educaționale actualizate și de calitate [47].

3.1.2. Transformarea guvernării digitale în Estonia prin X-Road

În contextul transformării digitale a administrațiilor publice, interoperabilitatea între instituții a devenit o condiție esențială pentru furnizarea rapidă, sigură și eficientă a serviciilor electronice. O infrastructură digitală solidă, care să permită conectarea sistemelor informatice disparate, este crucială pentru construirea unei guvernări electronice moderne. În acest sens, Estonia a dezvoltat și implementat încă din 2001 sistemul X-Road, o platformă care permite schimbul securizat de date între instituțiile publice și private.

X-Road este o soluție software open-source care permite schimbul unificat, securizat și standardizat de date între diferite organizații dintr-un ecosistem digital colaborativ. Prin facilitarea interoperabilității și prin creșterea nivelului de securitate, X-Road contribuie la optimizarea utilizării resurselor informaționale ale instituțiilor publice și private [48]. Acesta economisește anual 1345 de ani de muncă pentru cetățenii Estoniei, reducând semnificativ volumul de muncă birocratică și optimizând procesul de furnizare a serviciilor publice [49].

Proiectul X-Road a început să fie discutat în Estonia încă din 1998, în contextul provocărilor economice și sociale cu care se confrunta țara. În acea perioadă, bazele de date ale administrației publice erau izolate și schimbul de date între agenții, ministere și organizații era lent și ineficient, afectând serios eficiența guvernamentală. Problema era agravată de faptul că majoritatea registrelor publice foloseau baze de date diferite și nu existau interfețe standardizate pentru a facilita transferul de informații.

În 2000, sub inițiativa consilierului Prim-ministrului, Linnar Viik, și cu finanțare din partea Ministerului Transporturilor și Comunicațiilor, Ministerului de Interne și Biroului Guvernamental, a fost lansat proiectul pilot X-tee. Acest proiect a avut ca scop interconectarea a trei baze de date guvernamentale, folosind protocolul XML-RPC pentru schimbul de informații. Echipa de dezvoltatori, condusă de Tanel Tammet, Hannu Krosing și Vello Kadarpiik, a întâmpinat provocări tehnice legate de alegerea între tehnologia proprietară și utilizarea software-ului open-source. Un punct important în dezvoltarea X-Road a fost utilizarea tehnologiilor XML și XML-RPC, care au fost promovate de profesioniștii din domeniu, ca Vello Kadarpiik, care a lucrat în domeniul financiar și care a contribuit la integrarea aplicațiilor XML în sectorul public. Inițial, tehnologia SOAP a fost luată în considerare, dar a fost preferată tehnologia RPC datorită faptului

că SOAP nu era suficient de matură la acel moment [50].

În Estonia, organizațiile publice au propriile lor sisteme informatice pentru a procesa informații relevante pentru stat și cetățeni, în vederea furnizării serviciilor publice. Acestea funcționează adesea pe sisteme diferite, potrivite funcției fiecărei organizații. X-Road este o platformă distribuită de schimb de informații care permite acestor sisteme diferite să comunice între ele în întreg sectorul guvernamental. De exemplu, poliția poate accesa date din sistemul de sănătate, de la autoritatea fiscală sau din registrul comerțului, și invers. Dar pentru a face acest lucru, trebuie să îndeplinească trei criterii fundamentale: interoperabilitate tehnică, protecția integrității datelor în timpul transferului și confidențialitatea datelor. X-Road permite transferuri sigure, toate datele ieșite fiind semnate digital și criptate, iar datele primite sunt autentificate și înregistrate. De asemenea, a fost conceput cu gândul la extindere, astfel încât poate fi scalat pe măsură ce apar noi servicii și platforme digitale. În prezent, evoluează într-un instrument care poate scrie în mai multe sisteme informatice, poate transmite seturi mari de date și poate efectua căutări simultane în diverse baze de date [49].

3.1.3. Transformarea identității digitale în Estonia prin e-Identity

Într-o eră în care tehnologia digitală transformă rapid modul în care interacționăm cu instituțiile publice și private, e-Identitatea a devenit un element esențial al statului digital. Conform site-ului oficial E-Estonia acest sistem inovativ este reprezentat de e-ID, un instrument care facilitează accesul sigur și eficient al cetățenilor la o gamă largă de servicii digitale, indiferent de locația acestora. Introducerea e-ID-ului a fost un pas important, contribuind semnificativ la digitalizarea administrației publice și la îmbunătățirea interacțiunilor dintre cetățeni și instituțiile statului.

e-Identitate (e-ID) reprezintă un sistem de identitate digitală emis de statul estonian, care permite cetățenilor săi, indiferent de locul în care trăiesc, să acceseze servicii digitale în mod sigur și eficient. Acesta a fost implementat de mai bine de 20 de ani și este un pilon esențial al statului digital. E-ID este utilizat pentru o gamă largă de activități, inclusiv plata facturilor, votul online, semnătura digitală și accesul la informațiile de sănătate, contribuind la eficientizarea administrării și tranzacțiilor atât în sectorul public, cât și în cel privat. Sistemul este disponibil sub diferite forme, inclusiv prin cardul de identitate, Mobile-ID și Smart-ID, oferind un nivel înalt de securitate și conveniență.

Începând cu 2014, Estonia a extins utilizarea identității digitale prin programul e-Residency, care permite cetățenilor din întreaga lume să acceseze serviciile digitale ale Estoniei, fără a fi necesar să fie fizic în țară. De asemenea, Estonia a influențat dezvoltarea politicii europene în domeniu, prin contribuția la Directiva eIDAS, care asigură interoperabilitatea identităților electronice în Uniunea Europeană.

Un element important al acestui sistem este portofelul digital de identitate, care permite utilizatorilor să stocheze documente și să efectueze tranzacții digitale sigure. Pe măsură ce Europa progresează, Estonia continuă să joace un rol de lider în implementarea identităților digitale și în dezvoltarea soluțiilor interoperabile pentru guvernarea digitală globală [51].

Conform site-ului oficial E-Estonia ID-card-ul este un document de identitate obligatoriu emis de Poliția și Biroul de Gardă de Frontieră din Estonia pentru cetățenii săi și pentru cetățenii Uniunii Europene care locuiesc permanent în țară. În plus față de rolul său de identificare, acest card poate fi folosit și în format electronic prin integrarea unui ID digital care poate fi utilizat în combinație cu ID-card-ul fizic. Acesta permite cetățenilor să efectueze tranzacții online, să semneze documente, să acceseze servicii de sănătate și să participe la votul electronic.

Pentru utilizarea ID-card-ului în format digital, utilizatorii trebuie să instaleze aplicațiile necesare, precum DigiDoc4, care le permit verificarea funcționalității cititorului de carduri inteligente și gestionarea documentelor semnate electronic. În plus, instrucțiunile pentru utilizarea ID-card-ului

sunt valabile și pentru utilizarea ID-ului digital e-Residency sau a cardurilor diplomatice.

Estonia a facilitat și utilizarea acestui card și în context internațional. Cetățenii pot utiliza ID-card-ul pentru a călători în alte state membre ale Uniunii Europene sau ale Spațiului Economic European, fără a fi necesar un pașaport. ID-card-ul poate fi folosit și ca un card de client în diverse programe de loialitate, fiind o soluție practică pentru reducerea numărului de carduri fizice necesare.

Pentru a facilita utilizarea acestor funcționalități, Portalul MyID oferă informații despre ID-card-uri, Mobile-ID, Digi-ID și Smart-ID, ajutând cetățenii să gestioneze certificatele digitale și tranzacțiile electronice [52].



Fig. 7. ID-card

Mobile-ID reprezintă o formă de identificare digitală securizată, integrată în telefonul mobil al utilizatorului, care oferă funcționalități similare cardului de identitate electronic. Acest sistem se bazează pe o cartelă SIM specială, emisă de operatorii de telefonie mobilă, care stochează chei criptografice și rulează o aplicație dedicată pentru autentificare și semnătură digitală. Prin eliminarea necesității unor echipamente suplimentare, cum ar fi cititoarele de carduri, Mobile-ID facilitează accesul rapid și sigur la servicii digitale diverse, precum cele bancare, administrative sau comerciale. Popularitatea acestui sistem este în continuă creștere, în special datorită accesibilității smartphone-urilor și nevoii tot mai accentuate de soluții de identificare mobilă [53].

În completarea acestei perspective funcționale, Mobile-ID poate fi înțeles și ca un „document de identitate digital portabil”, recunoscut oficial de autoritățile naționale, precum Poliția și Paza de Frontieră. Această tehnologie permite utilizatorilor să se autentifice online, să semneze electronic documente, să acceseze registre naționale sau să participe la votul electronic, într-un mod echivalent utilizării unui act de identitate fizic. Prin integrarea acestor funcții critice într-un dispozitiv aflat permanent în posesia utilizatorului, Mobile-ID devine un instrument esențial în arhitectura identității digitale moderne, contribuind semnificativ la digitalizarea interacțiunilor cu instituțiile publice și private [54].

Programul e-Residency a fost lansat în 2014 de guvernul estonian cu scopul de a oferi persoanelor din afacerea Estoniei o identitate digitală, permițându-le să acceseze servicii guvernamentale electronice și să gestioneze afaceri într-un mediu transparent și sigur. Această inițiativă inovativă a fost prima de acest tip în lume, Estonia fiind un pionier în guvernanța electronică. Deși a început cu un buget modest și o echipă mică, programul a crescut rapid, având un impact semnificativ asupra antreprenoriatului global. Astăzi, e-Residency permite antreprenorilor din întreaga lume să înființeze și să administreze afaceri în Estonia complet digital, fără a fi necesar să se afle fizic în țară. Acesta facilitează gestionarea afacerilor prin semnătura digitală și servicii electronice, economisind timp și reducând birocrăția. Pentru Estonia, programul a adus beneficii economice și de promovare a inovației, contribuind la creșterea sectorului de afaceri și atragerea de investiții și turiști. Totodată, a consolidat reputația Estoniei ca lider global în domeniul tehnologiilor digitale și al guvernanței electronice [55].

Smart-ID este o aplicație mobilă destinată identificării digitale, care oferă o alternativă practică pentru utilizatorii ce nu dispun de o cartelă SIM specială, dar care au nevoie să își dovedească identitatea online în mod securizat. Soluția este frecvent utilizată în sectorul financiar pentru autentificare și aprobarea tranzacțiilor, remarcându-se prin simplitate și accesibilitate. Din 2018, Smart-ID este recunoscut oficial ca dispozitiv calificat de creare a semnăturii electronice (QSCD), ceea ce permite utilizatorilor să semneze documente la nivelul semnăturii electronice calificate (QES), cu valoare juridică deplină în toate statele membre ale Uniunii Europene. Aplicația este compatibilă cu o gamă largă de dispozitive smart, inclusiv telefoane, tablete și ceasuri inteligente, funcționând prin conexiune Wi-Fi sau internet mobil, fără a necesita SIM special sau roaming. Utilizarea sa este gratuită, nelimitată și transfrontalieră, fiind adoptată la scară largă, unde cetățenii o folosesc pentru a interacționa cu serviciile digitale ale statului și ale sectorului privat [56].

Bazată pe tehnologii avansate de criptografie și infrastructură PKI, aplicația oferă un nivel ridicat de securitate și protecție împotriva tentativelor de fraudă, inclusiv mecanisme de nerepudiare și detecție a clonării. Printre avantajele sale se numără ușurința în utilizare, posibilitatea instalării pe mai multe dispozitive inteligente, compatibilitatea și respectarea cerințelor reglementărilor europene eIDAS, PSD2 și EBA. În plus, utilizatorii beneficiază de o metodă inovatoare de înregistrare la distanță prin verificare biometrică automată (ABIV), disponibilă prin dispozitive cu funcție NFC și un document de identitate electronic. De la lansare, Smart-ID s-a bucurat de o adopție rapidă, depășind pragul de un milion de utilizatori în țările baltice într-un interval scurt [57].

3.1.4. Transformarea sistemului de sănătate în Estonia prin e-Health

Estonia este un lider în domeniul sănătății digitale, având un sistem complet integrat de e-Sănătate, exemplificat prin National Health Information System (HIS), care conectează furnizorii de servicii medicale din întreaga țară și stochează datele pacientului într-o bază centralizată, cu peste 40 de milioane de documente medicale. Acest sistem permite accesul rapid și eficient la informațiile necesare, iar utilizarea datelor genomice colectate de la peste 200.000 de persoane promovează medicina personalizată, îmbunătățind eficiența tratamentelor. Confidențialitatea și dreptul de proprietate asupra datelor sunt protejate, pacienții având dreptul de a vizualiza propriile fișe medicale și de a restricționa accesul la datele lor. Accesibilitatea la informațiile de sănătate este facilitată prin portalul pacientului, iar implementarea tehnologiei KSI Blockchain în HIS garantează integritatea datelor și protejează sistemul împotriva amenințărilor interne. Sistemul de carduri de identitate electronice asigură securitatea accesului la dosarele medicale ale pacienților, iar inițiativa e-Sănătate din Estonia oferă un model valoros pentru alte țări care doresc să îmbunătățească sistemele lor de sănătate digitale. Prin combinarea tehnologiilor inovative, Estonia demonstrează impactul pozitiv al digitalizării asupra îngrijirii medicale și eficienței sistemelor de sănătate [58].

Dosarul Electronic de Sănătate (e-Health Record) este un sistem național integrat care centralizează datele medicale ale pacienților din diverse unități de sănătate, permițând accesul online și securizat la istoricul medical al acestora. Acesta stochează informații standardizate despre vizitele la medic, tratamentele și testele efectuate, accesibile atât pentru medici, cât și pentru pacienți, prin portalul e-Pacientului. Tehnologia KSI Blockchain este utilizată pentru a asigura integritatea și securitatea datelor, iar pacienții pot vizualiza propriile dosare sau cele ale persoanelor pentru care au obținut permisiunea [58].

E-Prescription este un sistem centralizat, digitalizat, care permite emiterea și gestionarea prescripțiilor medicale fără utilizarea hârtiei. Medicul prescrie medicamentele printr-un formular online, iar pacientul doar prezintă un card de identitate la farmacie pentru a ridica medicamentele, farmacistul accesând datele pacientului din sistem. Acesta include și subvențiile medicale acordate de stat, fiind afișate automat în sistem. e-Rețeta elimină necesitatea vizitelor fizice pentru reînnoirea rețetelor, acestea putând fi emise prin contactul la distanță cu medicul. Implementarea completă a acestui sistem economisește timp și reduce sarcina administrativă atât pentru pacienți,

cât și pentru medici [59].

E-Ambulance reprezintă un sistem digitalizat de intervenție rapidă, care permite localizarea precisă a apelurilor de urgență într-un interval de maximum 30 de secunde, facilitând astfel trimiterea imediată a unei ambulanțe către locul necesar. În caz de urgență, medicii pot utiliza codul de ID al pacientului pentru a obține informații esențiale, precum grupa sanguină, alergii, tratamentele recente, medicamentele în curs de administrare sau statutul de sarcină, asigurând astfel un răspuns rapid și corect la nevoile pacientului [60].

3.2. E-guvernarea în România

România se află într-un proces continuu de adaptare la cerințele unei administrații publice moderne, în care digitalizarea joacă un rol esențial. În ultimele două decenii, autoritățile române au inițiat o serie de măsuri pentru implementarea e-guvernării, cu scopul de a îmbunătăți eficiența instituțiilor publice, de a facilita accesul cetățenilor la servicii și de a spori transparența administrativă. Deși procesul a cunoscut perioade de stagnare și provocări legate de infrastructură, voința politică fragmentată sau nivelul scăzut de alfabetizare digitală, România a reușit să dezvolte câteva instrumente importante în domeniul guvernării electronice. Sistemul național de identitate electronică, gestionat prin platforma Ghiseul.ro și, mai recent, prin proiectul ROeID, reprezintă pași importanți în direcția consolidării e-guvernării.

ROeID este o aplicație mobilă lansată în 2023, care permite cetățenilor din România și din diaspora să acceseze serviciile publice digitale printr-un singur set de credențiale. Aplicația facilitează autentificarea în platformele guvernamentale naționale și europene, folosind o identitate digitală validată prin încărcarea cărții de identitate, un selfie și un video scurt. Proiectul contribuie la digitalizarea administrației publice, simplificând accesul la servicii precum plata taxelor și obținerea documentelor oficiale, fără a mai fi necesară deplasarea la ghișee [61].

3.2.1. Implementarea Cardului Național de Sănătate în România

Cardul național de sănătate (CEAS) este un proiect de interes național implementat de Casa Națională de Asigurări de Sănătate (CNAS), cu scopul de a eficientiza și transparentiza utilizarea fondurilor publice în sistemul de asigurări sociale de sănătate. Cardul conține datele personale ale asiguratului, precum numele, prenumele, codul unic de identificare, numărul cardului și data nașterii, iar valabilitatea sa este de 5 ani. Acesta funcționează ca un cod de acces unic pentru toate platformele informatice ale CNAS și reprezintă dovada că un asigurat a beneficiat efectiv de servicii medicale. Cardul conține datele de identificare ale persoanei asigurate, iar activarea lui se face la prima vizită la un furnizor de servicii medicale, prin introducerea unui cod PIN personal. Utilizarea sa este obligatorie începând cu 1 mai 2015, cu excepția urgențelor medicale, unde nu este necesar. Prin intermediul cardului, furnizorii medicali pot valida rapid serviciile acordate, iar CNAS poate urmări în timp real fluxurile financiare și corectitudinea decontărilor. În cazul pierderii sau deteriorării, se poate solicita un duplicat, iar până la emiterea acestuia, asiguratul poate beneficia de servicii în baza unei adeverințe temporare. Cardul aduce beneficii atât pentru sistemul de sănătate, prin reducerea fraudei și a birocrăției, cât și pentru pacient, prin simplificarea accesului la servicii și asigurarea unei evidențe clare a istoricului medical [62].

Casa Națională de Asigurări de Sănătate este o instituție publică autonomă, cu personalitate juridică, care coordonează și administrează sistemul asigurărilor sociale de sănătate din România. Principalul său rol este de a asigura funcționarea unitară și eficientă a sistemului, prin gestionarea fondurilor destinate serviciilor medicale, elaborarea politicilor de sănătate în domeniul asigurărilor și monitorizarea furnizorilor de servicii medicale. CNAS colaborează cu Ministerul Sănătății și alte instituții pentru a asigura accesul echitabil la servicii medicale de calitate, iar prin intermediul unui sistem informatic integrat, urmărește evidența asiguraților și controlul utilizării fondurilor publice din sănătate [63].

Legea nr. 95/2006 privind reforma în domeniul sănătății reglementează procesul de implementare a cardului național de sănătate în cadrul sistemului de asigurări sociale de sănătate din România. Unul dintre aspectele centrale ale legii este integrarea cardului în sistemul informatic unic gestionat de Casa Națională de Asigurări de Sănătate, ceea ce permite o mai bună validare a serviciilor medicale și o monitorizare mai eficientă a decontărilor. Legea stabilește cadrul legal pentru distribuirea cardului, pentru activarea acestuia și pentru utilizarea sa obligatorie începând cu data de 1 mai 2015. De asemenea, sunt reglementate măsurile de protecție a datelor personale ale asiguraților și se prevede responsabilitatea furnizorilor de servicii de sănătate de a utiliza cardul pentru verificarea statutului de asigurat și decontarea serviciilor prestate. În cazul în care cardul este pierdut sau deteriorat, asigurații au dreptul să solicite un duplicat, iar legea asigură continuarea serviciilor medicale prin eliberarea unei adeverințe temporare până la primirea unui nou card [64].

În sistemul asigurărilor sociale de sănătate, scopul principal este protejarea asiguraților împotriva costurilor serviciilor medicale în caz de boală sau accident, prin finanțarea acestora din fonduri colectate de la persoanele asigurate. Asigurările sociale de sănătate sunt reglementate de Legea nr. 95/2006, care stabilește un pachet minim de servicii medicale, inclusiv prevenirea bolilor, tratamente curative, medicamente și dispozitive medicale, ce sunt acordate asiguraților în mod universal, echitabil și nediscriminatoriu. Finanțarea acestui sistem se realizează prin Fondul Național Unic de Asigurări de Sănătate (FNUASS), gestionat de Casa Națională de Asigurări de Sănătate, iar colectarea contribuțiilor de asigurări sociale de sănătate se face de Ministerul Finanțelor Publice prin ANAF. CNAS administrează și implementează politicile publice de sănătate, în timp ce casele județene de asigurări de sănătate încheie contracte directe cu furnizorii de servicii medicale, asigurând accesul asiguraților la servicii decontate din FNUASS [65].

Conform Codului Fiscal, persoanele care au calitatea de asigurat în sistemul de asigurări sociale de sănătate trebuie să plătească o contribuție de 10% din veniturile realizate, iar acest lucru se aplică atât angajaților, cât și celor care realizează venituri care implică plata acestei contribuții. De asemenea, există persoane care sunt asigurate fără a fi necesar să plătească această contribuție, printre care se numără copiii sub 18 ani, tinerii între 18 și 26 de ani care sunt elevi, studenți sau ucenici, persoanele cu dizabilități, femeile însărcinate și lăuzele, pensionarii, persoanele aflate în concediu pentru creșterea copilului sau beneficiare de indemnizație de șomaj, printre altele. Aceste categorii beneficiază de asigurare medicală gratuită, având dreptul la serviciile de sănătate prevăzute de lege fără a contribui financiar la FNUASS [65].



Fig. 8. Cardul național de sănătate

3.2.2. E-Factura și digitalizarea procesului fiscal în România

Conform Hotărârii nr. 520 din 24 iulie 2013, Agenția Națională de Administrare Fiscală (ANAF) este autoritatea centrală responsabilă cu administrarea și colectarea veniturilor publice, gestionând impozitele, taxele și contribuțiile conform legislației fiscale din România. ANAF are ca scop implementarea și monitorizarea respectării legislației fiscale, prin activități precum controlul

fiscal, inspecția fiscală și executarea silită. De asemenea, ANAF gestionează sistemele informatice necesare colectării taxelor și impozitelor, având ca obiectiv asigurarea transparenței și eficienței procesului fiscal [66].

Sistemul național RO e-Factura este destinat operatorilor economici pentru emiterea și primirea facturilor electronice. Acesta utilizează fișiere XML și respectă standardul european EN 16931-1+A1, precum și regulile naționale RO-CIUS impuse de legislația românească. În Monitorul Oficial nr. 977 din 27 octombrie 2023, a fost publicată Legea nr. 296/2023 [67], care aduce modificări în ceea ce privește facturarea electronică. Aceste modificări sunt implementate în conformitate cu Decizia de punere în aplicare (UE) 2023/1553 a Consiliului Uniunii Europene, ce autorizează România să implementeze facturarea electronică obligatorie pentru toate tranzacțiile efectuate între persoanele impozabile pe teritoriul României, începând cu 1 ianuarie 2024.

Pentru utilizarea sistemului RO e-Factura, operatorii economici trebuie să se înregistreze în Spațiul Privat Virtual (SPV). Înregistrarea poate fi realizată prin accesarea site-ului ANAF, iar pentru a primi atenționări, trebuie să fie exprimată opțiunea corespunzătoare. Facturile electronice pot fi emise și transmise în două moduri: prin servicii web, utilizând aplicații proprii care se conectează la sistemul RO e-Factura prin API-uri, sau prin încărcarea fișierelor XML folosind aplicația pusă la dispoziție de Ministerul Finanțelor. Mai multe informații pot fi accesate prin ghidurile și documentația tehnică disponibile pe site-urile ANAF și Ministerul Finanțelor [68].

3.2.3. Platforma e-guvernare.ro și digitalizarea serviciilor publice

Sistemul Electronic Național (SEN) al României a fost lansat în septembrie 2003, în cadrul ședinței Grupului de Promovare a Tehnologiei Informației, având ca scop principal facilitarea accesului cetățenilor și al operatorilor economici la informații și servicii publice prin intermediul platformei online www.e-guvernare.ro [11].

Conform lui C. Vrabie, platforma www.e-guvernare.ro reprezintă un portal unic de acces la serviciile publice electronice din România, având rolul de a facilita interacțiunea dintre cetățeni și instituțiile statului prin mijloace digitale. Acest sistem informatic are la bază o serie de principii esențiale, precum egalitatea de șanse, nediscriminarea, respectarea confidențialității datelor cu caracter personal, precum și asigurarea securității informațiilor și a accesului liber la informațiile de interes public. Totodată, platforma promovează transparența administrativă și utilizarea tehnologiilor moderne în procesul decizional.

Obiectivele urmărite prin implementarea acestei platforme vizează în mod direct reducerea costurilor administrative, limitarea birocrăției, combaterea corupției, precum și creșterea calității serviciilor publice oferite cetățenilor. De asemenea, se urmărește „îmbunătățirea relației dintre cetățeni și administrația publică, prin accesibilitate crescută și eliminarea barierelor fizice și birocratice”.

Prin intermediul portalurilor electronice, cetățenii pot accesa diverse tipuri de servicii, precum depunerea de formulare administrative sau solicitarea de informații publice, fără a fi necesară deplasarea fizică la ghișee. Serviciile sunt organizate pe secțiuni tematice și sunt disponibile continuu (24/7). De asemenea, e-guvernarea contribuie la protejarea datelor personale și la îmbunătățirea calității serviciilor publice prin automatizare și digitalizare [8].

3.2.4. Transformarea procesului administrativ prin platforma Ghișeul.ro

Platforma Ghișeul.ro este un sistem electronic prin intermediul căruia cetățenii pot efectua plăți către instituțiile publice înrolate, precum taxe, impozite sau amenzi contravenționale, beneficiind de reducerile prevăzute în cazul achitării acestora în termenul legal de 15 zile. De asemenea, platforma permite plata pentru diverse servicii publice, inclusiv cele comunitare de utilitate

publică. Accesibilă non-stop, cu excepția intervalelor de mentenanță, Ghișeul.ro se remarcă prin implementarea unor standarde înalte de securitate pentru tranzacțiile online, prin criptarea datelor bancare conform protocolului SSL și respectarea cerințelor impuse de standardul PCI-DSS. Procesarea plăților este gestionată de entități externe specializate, iar datele cardurilor nu sunt colectate sau stocate de platformă ori de instituțiile beneficiare. În plus, utilizatorii sunt avertizați să acceseze platforma doar prin introducerea directă a adresei oficiale, ca măsură suplimentară de prevenire a fraudelor informatice. Astfel, Ghișeul.ro contribuie semnificativ la modernizarea administrației publice prin digitalizare, oferind un canal sigur, rapid și transparent de interacțiune între cetățeni și stat [69].

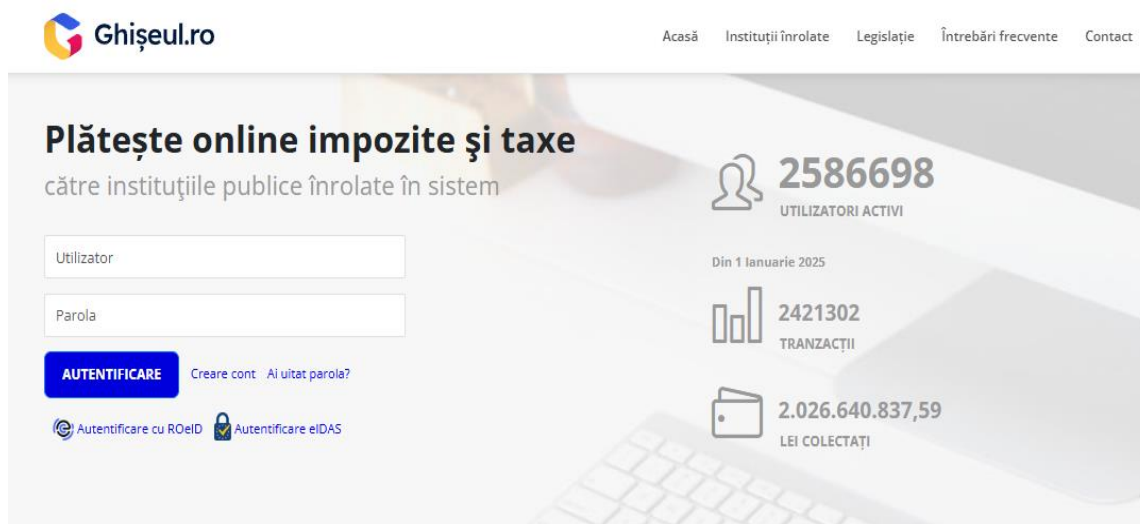


Fig. 9. Platforma Ghișeul.ro
sursa: <https://www.ghiseul.ro/ghiseul/public/#>

3.2.5. E-licitație și digitalizarea procesului de achiziții publice în România

Conform Sistemul Electronic de Achiziții Publice (SEAP), accesibil prin intermediul platformei e-licitatie.ro, constituie un pilon esențial în procesul de digitalizare a administrației publice din România. Acesta este conceput ca un instrument digital modern, gestionat sub coordonarea Autorității pentru Digitalizarea României, care facilitează desfășurarea în format electronic a întregului ciclu de achiziții publice. Prin intermediul SEAP, autoritățile contractante pot iniția, derula și finaliza proceduri de achiziție într-un cadru transparent și standardizat, asigurând, totodată, accesul echitabil al operatorilor economici la contractele finanțate din fonduri publice. Astfel, platforma contribuie activ la consolidarea unui mediu concurențial sănătos și la eficientizarea procesului decizional în administrația publică [70].

În acest context, obiectivele principale ale SEAP reflectă o viziune orientată spre modernizarea administrației și utilizarea responsabilă a resurselor publice. Platforma își propune să asigure transparență deplină asupra procesului de achiziții, să promoveze concurența loială și să reducă riscurile de fraudă sau favoritism în alocarea contractelor publice. Prin digitalizarea fluxurilor de lucru și simplificarea accesului la licitații, SEAP contribuie la reducerea costurilor administrative și la creșterea eficienței instituționale. De asemenea, implementarea unor măsuri avansate de securitate cibernetică garantează un mediu sigur pentru desfășurarea procedurilor, oferind un cadru predictibil și controlat pentru toate părțile implicate în procesul de achiziție publică [70].

În vederea menținerii integrității și bunei funcționări a platformei, Autoritatea pentru Serviciile Societății Informaționale ASSI are dreptul de a suspenda utilizatorii care încalcă prevederile legale sau regulamentele interne ale SEAP. Printre faptele sancționabile se numără transmiterea de informații false, conținut malițios, încălcarea drepturilor de autor sau interferențele neautorizate cu sistemul. Totodată, operatorul își rezervă dreptul de a modifica regulile de utilizare și

informațiile disponibile în platformă, cu informarea prealabilă a utilizatorilor. Aceste măsuri contribuie la asigurarea unui proces transparent, sigur și eficient de gestionare a achizițiilor publice prin mijloace electronice [71].

Funcționalitatea extinsă a platformei SEAP este reflectată și de diversitatea tipurilor de proceduri și anunțuri disponibile, adaptate în funcție de complexitatea achiziției și valoarea estimată a contractului. Printre cele mai utilizate proceduri se numără licitația deschisă, care permite participarea oricărui operator economic interesat, și licitația restrânsă, ce presupune o selecție prealabilă a candidaților eligibili. În cadrul platformei, interacțiunea dintre autoritățile contractante și ofertanți se realizează printr-o serie de instrumente digitale, precum anunțurile de participare (CN), anunțurile simplificate (SCN), invitațiile de participare (RFQ), sau anunțurile de concesiune (PC). SEAP oferă, de asemenea, acces la date privind achizițiile directe, sistemele dinamice de achiziții și cataloagele electronice, demonstrând astfel capacitatea sa de a susține un sistem public de achiziții flexibil, transparent și adaptabil la nevoile pieței actuale [70].

3.3. Comparație între România și Estonia în domeniul e-guvernării

Digitalizarea administrației publice reprezintă una dintre cele mai complexe și necesare reforme pentru statele europene, iar diferențele dintre țări reflectă atât contextul istoric, cât și viziunea strategică a guvernelor asupra transformării digitale. Compararea sistemelor de e-guvernare din România și Estonia evidențiază diferențe semnificative în ceea ce privește viziunea strategică, nivelul de integrare digitală și maturitatea infrastructurii tehnologice. Estonia este adesea considerată un model de referință la nivel european și global în domeniul digitalizării administrației publice, datorită unei abordări coerente și bine planificate.

Estonia, recunoscută pentru viziunea sa digitală, a integrat tehnologia în structura guvernamentală încă din anii 2000. Prin inițiative precum e-Residency, e-ID și e-Health, Estonia a creat un ecosistem digital coerent, în care cetățenii și rezidenții pot interacționa cu statul într-un mod fluid și securizat. De exemplu, e-Residency permite antreprenorilor din întreaga lume să înființeze și să administreze companii în Estonia, având acces la infrastructura digitală a statului. În plus, e-Residency oferă posibilitatea persoanelor din afara Estoniei să acceseze digital servicii guvernamentale, ceea ce demonstrează deschiderea Estoniei către inovație și internaționalizare. În domeniul sănătății, sistemul e-Health permite accesul la istoricul medical personal, programări și prescripții electronice, reducând semnificativ timpul de așteptare și erorile medicale.

Prin contrast, România a demarat procesul de digitalizare a administrației publice într-un ritm mai lent și fragmentat, cu inițiative disparate care au evoluat în paralel, fără o integrare funcțională completă între ele. Platforme precum e-guvernare.ro, Ghișeul.ro și e-licitatie.ro (SEAP) acoperă diverse domenii ale interacțiunii cetățeanului cu statul – de la plăți online pentru taxe și impozite, până la achiziții publice sau depunerea de formulare administrative – însă lipsa unei infrastructuri de tip back-office integrat, precum X-Road, limitează coerența și eficiența sistemului. De exemplu, utilizarea serviciilor digitale în România necesită de multe ori autentificări separate, completarea repetitivă a datelor și interacțiuni redundante între cetățean și multiple instituții, ceea ce descurajează utilizarea pe scară largă. În plus, deși România a făcut progrese notabile în domeniul plăților electronice prin Ghișeul.ro și în transparentizarea achizițiilor publice prin SEAP, lipsa unei identități digitale unificate, echivalente e-ID-ului estonian, rămâne un obstacol major în calea unei digitalizări reale și eficiente.

Un alt aspect important al diferenței dintre cele două modele este abordarea strategică. Estonia a avut încă de la început o viziune unitară, susținută de voință politică și investiții constante în infrastructură digitală, securitate cibernetică și educație digitală. În schimb, România a adoptat o strategie de digitalizare adesea reactivă, bazată pe proiecte punctuale sau dictate de obligații europene, precum cele prevăzute în Planul Național de Redresare și Reziliență. Astfel, deși România dispune de infrastructură tehnologică și expertiză, eforturile de digitalizare sunt fragmentate, ceea ce afectează eficiența și încrederea cetățenilor în aceste sisteme.

România poate învăța din experiența Estoniei importanța unei strategii naționale integrate de digitalizare, care să asigure coerența între diferitele platforme și servicii publice. Estonia a reușit să construiască un sistem digitalizat bazat pe interoperabilitate și accesibilitate, prin implementarea unui cadru legislativ solid și infrastructură tehnologică avansată, esențial pentru fluidizarea procesului administrativ. De asemenea, este necesar ca România să adopte o identitate digitală unificată, similară cu sistemul e-ID din Estonia, care să permită cetățenilor să acceseze toate serviciile guvernamentale într-un mod simplu și securizat. Un alt punct esențial este crearea unui mediu de încredere, prin investiții în securitate cibernetică și educație digitală, astfel încât cetățenii să se simtă confortabil să adopte și să utilizeze aceste platforme. România ar trebui să își concentreze eforturile pe eliminarea fragmentării administrative și pe crearea unei infrastructuri interconectate, care să reducă birocrăția și să îmbunătățească eficiența serviciilor publice.

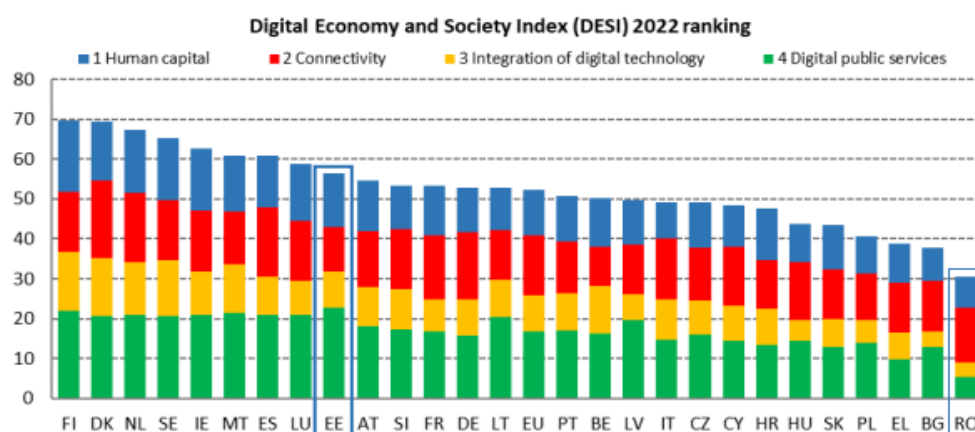


Fig. 10. Digital Economy and Society Index

Sursa:

9file:///C:/Users/denis/Downloads/DESI_2022__Estonia__eng_LELKUDOD0NI4pnkf8S4QICVSA_88701%20(1).pdf

Capitolul 4. Analiza rezultatelor chestionarului

În vederea realizării unei analize relevante asupra percepției cetățenilor români privind serviciile de e-guvernare, a fost aplicat un chestionar online care a urmărit aspecte precum gradul de utilizare a platformelor digitale, dificultățile întâmpinate, nivelul de încredere în aceste soluții și competențele digitale ale utilizatorilor. Chestionarul a fost completat de un număr de 81 de respondenți, proveniți din medii socio-demografice diferite. Deși eșantionul nu este reprezentativ la nivel național, datele colectate oferă o imagine generală asupra modului în care cetățenii se raportează la digitalizarea administrației publice. În continuare, vor fi prezentate rezultatele obținute, sub formă de tabele grafice, însoțite de interpretări corespunzătoare.

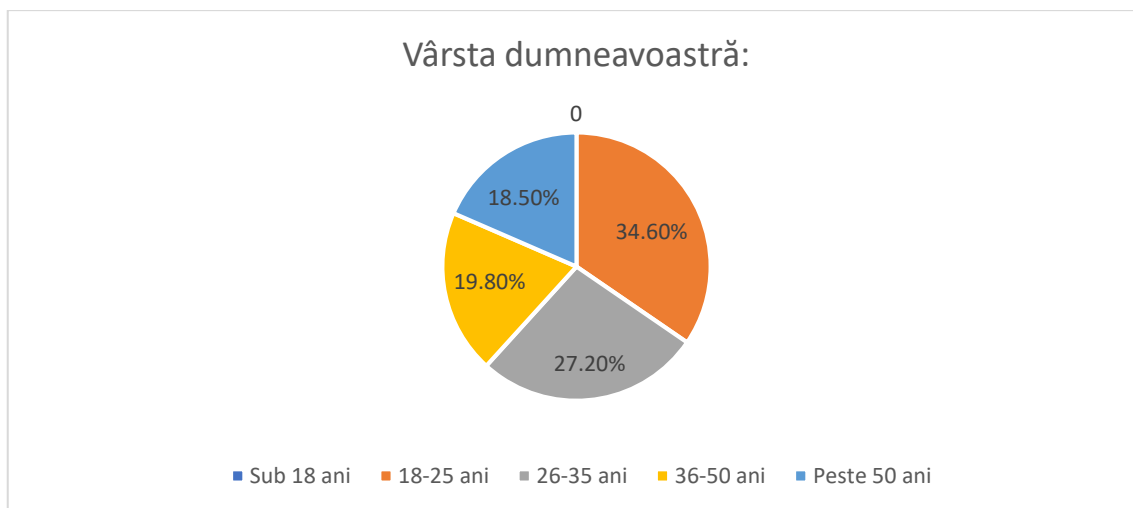


Fig. 11. Distribuția respondenților în funcție de vârstă

Majoritatea respondenților la chestionar se încadrează în categoria de vârstă 18–25 de ani (34,6%), urmată de grupa 26–35 de ani (27,2%). Procentul celor cu vârste între 36–50 de ani este de 19,8%, iar cei peste 50 de ani reprezintă 18,5% din totalul eșantionului. Nu au existat respondenți sub 18 ani.

Distribuția respondenților în funcție de gen:

Din totalul de 80 de respondenți, 53,1% (43 de persoane) au declarat că sunt de gen masculin, iar 50,9% (38 de persoane) de gen feminin. Niciunul dintre participanți nu a ales opțiunea „Prefer să nu spun”.

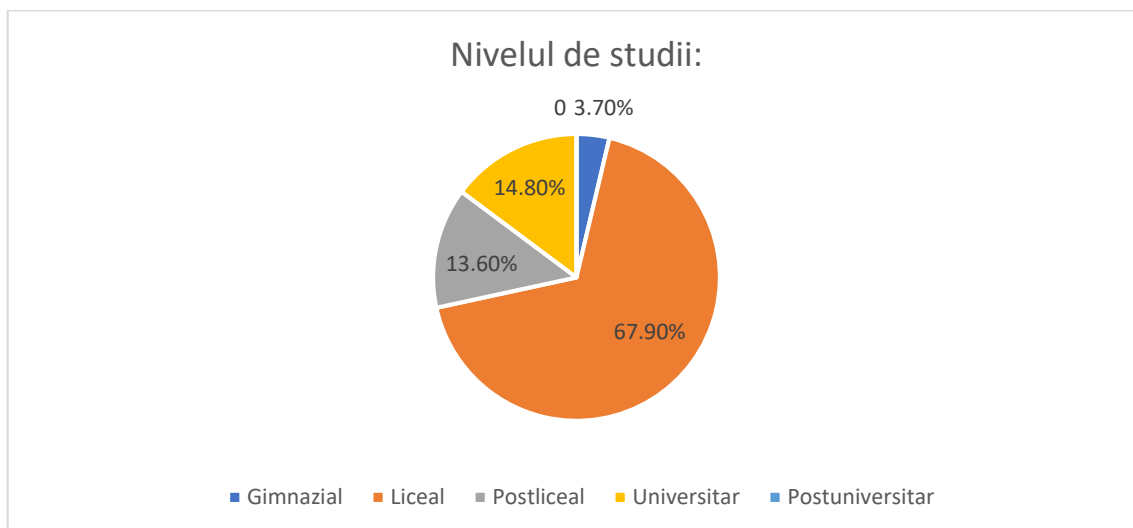


Fig. 12. Distribuția respondenților în funcție de nivelul de studii

Cea mai mare pondere a respondenților provine din categoria liceală, cu 67,9% (55 de persoane). În continuare, 14,8% dintre respondenți (12 persoane) au studii universitare, iar 13,6% (11 persoane) au studii postliceale. Doar 3,7% (3 persoane) dintre respondenți au absolvit ciclul gimnazial. Niciun respondent nu a indicat un nivel de studii postuniversitar.

Distribuția respondenților în funcție de locul de rezidență:

Din totalul respondenților, 64,2% (52 de persoane) locuiesc în mediul urban, iar 35,8% (29 de

persoane) trăiesc în mediul rural.

Accesul regulat la internet:

Majoritatea respondenților (97,5%, adică 79 de persoane) au declarat că au acces regulat la internet atât acasă, cât și pe mobil. Doar 1,2% dintre respondenți (1 persoană) au acces la internet doar acasă, iar aceeași pondere (1,2%, 1 persoană) utilizează internetul doar pe mobil. Niciun respondent nu a menționat că nu are acces la internet.

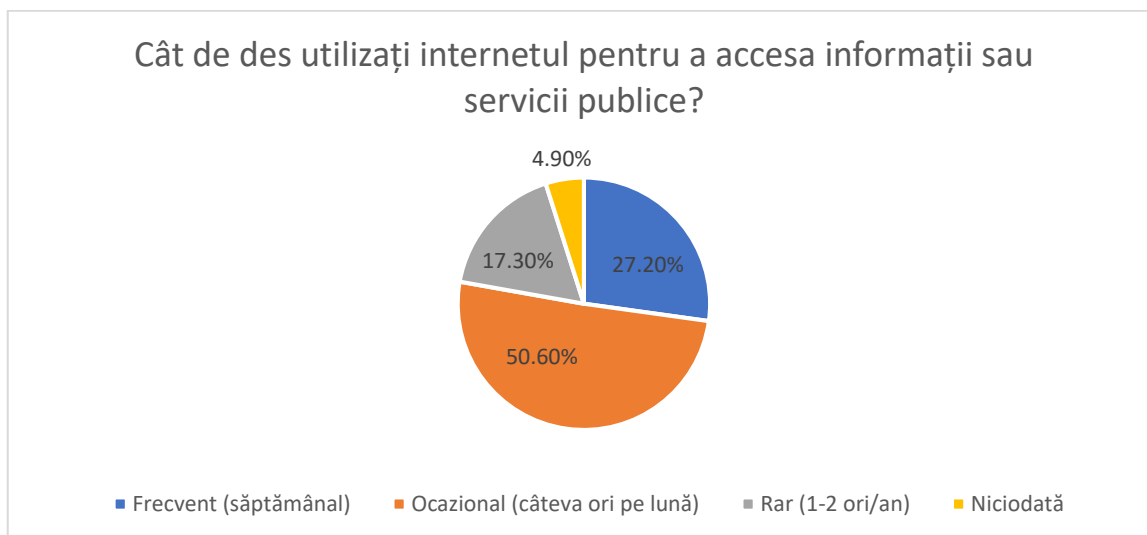


Fig. 13. Frecvența utilizării internetului pentru accesarea informațiilor sau serviciilor publice

Majoritatea respondenților (50,6%, adică 41 de persoane) utilizează internetul pentru a accesa informații sau servicii publice ocazional, de câteva ori pe lună. 27,2% dintre respondenți (22 de persoane) accesează aceste servicii frecvent, săptămânal, în timp ce 17,3% (14 persoane) le utilizează rar, doar 1-2 ori pe an. Un mic procent (4,9%, 4 persoane) nu utilizează deloc internetul pentru a accesa astfel de informații sau servicii.

Evaluarea competențelor digitale ale respondenților:

Majoritatea respondenților își evaluează competențele digitale ca fiind bune (55,6%, adică 45 de persoane). 30,9% dintre respondenți (25 de persoane) consideră că au competențe digitale foarte bune. Un procent mai mic (9,9%, 8 persoane) se autoevaluează cu competențe digitale medii, iar 3,7% dintre respondenți (3 persoane) le consideră slabe.

Utilizarea platformelor de e-guvernare:

Majoritatea respondenților (87,7%, adică 71 de persoane) au utilizat până acum platforme de e-guvernare, precum ghișeul.ro, platforma ROeID, e-guvernare.ro, SPV etc. În schimb, 12,3% dintre respondenți (10 persoane) nu au utilizat aceste platforme.

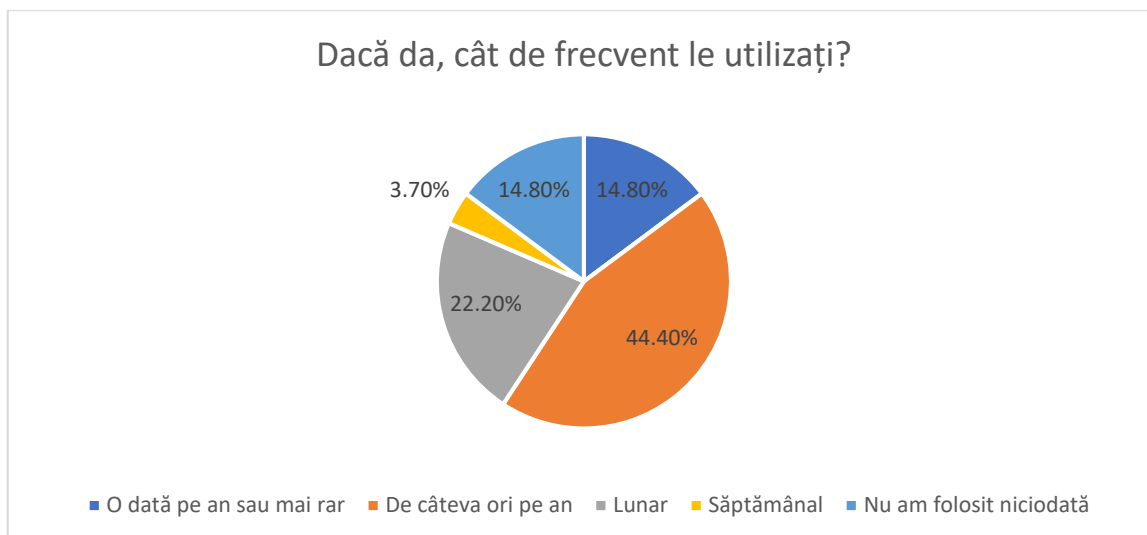


Fig. 14. Frecvența utilizării platformelor de e-guvernare

Dintre respondenții care au utilizat platforme de e-guvernare, 44,4% (36 de persoane) le utilizează de câteva ori pe an, iar 22,2% (18 persoane) le accesează lunar. 14,8% dintre respondenți (12 persoane) folosesc aceste platforme o dată pe an sau mai rar, iar 3,7% (3 persoane) le utilizează săptămânal. În același timp, 14,8% dintre respondenți (12 persoane) nu au folosit niciodată aceste platforme, chiar dacă anterior au răspuns că le-au utilizat.

Tipuri de servicii accesate prin platformele de e-guvernare:

Întrebarea a permis alegerea mai multor tipuri de servicii, iar cei mai mulți respondenți (59,3%, adică 48 de persoane) au utilizat platformele de e-guvernare pentru plata taxelor și impozitelor, iar un număr similar (59,3%, 48 de persoane) le-au accesat pentru a solicita documente administrative (certificate, adeverințe etc.). 37% dintre respondenți (30 de persoane) au utilizat platformele pentru obținerea cazierului judiciar sau fiscal, în timp ce 34,6% (28 de persoane) au folosit serviciile pentru depunerea declarațiilor fiscale. 9,9% dintre respondenți (8 persoane) au accesat platformele pentru înregistrarea unei firme sau PFA. 23,5% dintre respondenți (19 persoane) nu au accesat niciun serviciu prin platformele de e-guvernare.

Ușurința de utilizare a platformelor de e-guvernare:

Majoritatea respondenților consideră platformele de e-guvernare ușor de utilizat. 43,2% dintre aceștia (35 de persoane) le-au evaluat ca fiind "foarte ușor" de utilizat, iar 23,5% (19 persoane) le consideră "ușor" de utilizat. Un procent semnificativ de respondenți (30,9%, 25 de persoane) a menționat că platformele sunt "nici ușor, nici greu" de utilizat. Doar 2,5% dintre respondenți (2 persoane) au spus că platformele sunt "greu" de utilizat, iar niciun respondent nu a considerat că utilizarea acestora este "foarte greu" de realizat.

Dificultăți întâmpinate la utilizarea platformelor de e-guvernare:

Majoritatea respondenților (92,6%, 75 de persoane) nu au întâmpinat dificultăți în utilizarea platformelor de e-guvernare. Cu toate acestea, o mică parte dintre aceștia au semnalat anumite probleme. 3,7% dintre respondenți (3 persoane) au întâmpinat probleme tehnice sau erori frecvente, iar 2,5% (2 persoane) au menționat lipsa de informații clare. În plus, 1,2% dintre respondenți (1 persoană) au considerat că autentificarea pe platformă era prea complicată. Nu au fost raportate dificultăți legate de o interfață complicată.

Impactul platformelor de e-guvernare asupra timpului petrecut pentru rezolvarea problemelor administrative:

Majoritatea respondenților consideră că utilizarea platformelor de e-guvernare a redus semnificativ timpul necesar pentru rezolvarea problemelor administrative. 58% dintre aceștia (47 de persoane) au afirmat că timpul a fost redus semnificativ, iar 37% (30 de persoane) consideră că reducerea a fost într-o oarecare măsură. Doar o mică parte dintre respondenți au spus că impactul asupra timpului a fost minor: 1,2% dintre respondenți (1 persoană) au considerat că timpul petrecut nu a fost prea mult redus, iar 3,7% (3 persoane) au afirmat că nu au observat nicio reducere a timpului petrecut pentru rezolvarea problemelor administrative.

Încrederea în securitatea datelor personale furnizate platformelor de e-guvernare:

Majoritatea respondenților au exprimat un nivel ridicat de încredere în securitatea datelor personale furnizate pe platformele de e-guvernare. 50,6% dintre respondenți (41 persoane) au declarat că au foarte multă încredere în securitatea acestor platforme, iar 44,4% (36 persoane) au afirmat că au destul de multă încredere. O mică parte dintre respondenți au exprimat o încredere mai scăzută: 3,7% dintre respondenți (3 persoane) au indicat că au puțină încredere, iar 1,2% (1 persoană) au spus că nu au nicio încredere în securitatea platformelor.

Preferința între rezolvarea problemelor administrative online și la ghișeu fizic:

Majoritatea respondenților preferă să rezolve problemele administrative online, 51,9% dintre aceștia (42 persoane) optând pentru această variantă. Un procent semnificativ, de 34,6% (28 persoane), a menționat că depinde de situație, indicând o preferință flexibilă în funcție de tipul problemei administrative. În schimb, 13,6% dintre respondenți (11 persoane) preferă să rezolve problemele la ghișeu fizic, ceea ce sugerează o deschidere limitată față de digitalizarea completă a acestui tip de servicii.

Nivelul de informare privind riscurile online:

Rezultatele arată că majoritatea respondenților (60,5%, adică 49 de persoane) se consideră foarte bine informați cu privire la riscurile online, cum ar fi furtul de date sau atacurile cibernetice. Un procent important, de 29,6% (24 de persoane), se declară destul de bine informați, ceea ce indică un grad bun de conștientizare în rândul populației chestionate. Pe de altă parte, doar 7,4% (6 persoane) se consideră puțin informați, iar 2,5% (2 persoane) afirmă că nu sunt deloc informați în acest sens.

Impactul dezinformării asupra încrederii în platformele de e-guvernare:

În ceea ce privește influența dezinformării asupra încrederii în serviciile de e-guvernare, rezultatele chestionarului indică faptul că majoritatea respondenților (91,4%, adică 74 de persoane) consideră că fenomenul dezinformării afectează negativ percepția publicului asupra acestor platforme. Doar 1,2% (1 respondent) nu vede o legătură directă între cele două, în timp ce 7,4% (6 respondenți) nu pot aprecia impactul sau nu au o opinie clară în acest sens.

Concluzii

Lucrarea de față a avut ca obiectiv principal evaluarea impactului implementării e-guvernării asupra administrației publice din România, concentrându-se atât asupra gradului de digitalizare a serviciilor publice, cât și asupra percepției cetățenilor și a dificultăților întâmpinate de instituțiile statului în acest proces complex. Rezultatele cercetării confirmă faptul că e-guvernarea, deși încă aflată într-un stadiu de dezvoltare inegal, are potențialul de a transforma profund modul în care administrația publică interacționează cu cetățenii și își desfășoară activitatea internă.

Pe parcursul investigației au fost formulate și testate trei ipoteze centrale. Prima dintre acestea, care susține că e-guvernarea contribuie la creșterea eficienței administrației publice, a fost validată

prin analiza unor platforme digitale deja operaționale, precum ghișeul.ro și e-guvernare.ro. Aceste instrumente informatice au demonstrat capacitatea de a reduce semnificativ timpii de procesare a solicitărilor, de a diminua volumul birocrăției și de a facilita accesul cetățenilor la servicii esențiale, contribuind astfel la o administrare mai rapidă și mai transparentă.

Cea de-a doua ipoteză a vizat identificarea obstacolelor majore care frânează implementarea eficientă a e-guvernării. Cercetarea a relevat faptul că infrastructura tehnologică insuficient dezvoltată, în special în mediul rural sau în instituțiile subfinanțate, precum și nivelul scăzut de competențe digitale în rândul personalului administrativ, constituie bariere semnificative. Diferențele marcante între regiunile țării și între instituțiile publice în ceea ce privește capacitatea de a adopta noile tehnologii confirmă existența unei fragmentări în aplicarea politicilor de digitalizare.

În ceea ce privește a treia ipoteză, care presupune un impact pozitiv al e-guvernării asupra încrederii cetățenilor în instituțiile publice, analiza a evidențiat un rezultat nuanțat. Deși există premise favorabile unei creșteri a încrederii, acest efect este condiționat de factori precum gradul de transparență a platformelor digitale, ușurința de utilizare a acestora și calitatea interacțiunii cu administrația. În absența unei experiențe digitale coerente și accesibile, riscul de alienare și neîncredere din partea cetățenilor rămâne ridicat.

Obiectivele lucrării au fost atinse în mod sistematic, după cum urmează:

1. Gradul de implementare al soluțiilor de e-guvernare a fost evaluat prin examinarea funcționării unor platforme digitale și a cadrului legislativ și strategic care le reglementează. S-a constatat o tendință generală pozitivă de extindere a digitalizării, cu progrese notabile în mediul urban, dar și cu persistența unor dezechilibre semnificative între diverse unități administrative.
2. Beneficiile și provocările asociate procesului de e-guvernare au fost analizate la nivel național și local. Printre avantajele constatate se numără sporirea eficienței instituționale, reducerea interacțiunii birocratice și accesul mai facil la informații publice. În contrapondere, deficiențele infrastructurale și lipsa unei culturi organizaționale digitale adecvate se dovedesc a fi principalele obstacole în calea progresului.
3. În privința soluțiilor propuse, s-a subliniat necesitatea unor investiții consistente în infrastructura digitală, a formării continue a angajaților din administrația publică, precum și a simplificării interfețelor platformelor pentru a asigura incluziunea digitală. De asemenea, este esențială formularea unor politici publice coerente și adaptate nevoilor regionale, care să reducă disparitățile existente și să susțină o dezvoltare echilibrată.

În concluzie, e-guvernarea se conturează drept un vector esențial în procesul de modernizare și eficientizare a administrației publice din România. Cu toate acestea, succesul său pe termen lung este condiționat de un angajament politic real, de alocarea strategică a resurselor, dar și de implicarea activă și constantă a cetățenilor și funcționarilor în procesul de digitalizare. Lucrarea de față contribuie astfel la o mai bună înțelegere a dinamicii actuale a e-guvernării în România și oferă o bază argumentativă solidă pentru conturarea unor direcții viitoare de acțiune, menite să sprijine o transformare digitală sustenabilă și incluzivă.

Anexa

Chestionar – Percepția cetățenilor asupra e-guvernării în România

Bună ziua! Numele meu este Nițulescu Ionela-Denisa, studentă în anul III la Facultatea de Administrație Publică din cadrul Școlii Naționale de Studii Politice și Administrative (SNSPA). Acest chestionar face parte din cercetarea pentru lucrarea mea de licență, având ca temă „E-

guvernarea în România”.

Scopul cercetării este de a înțelege mai bine percepția cetățenilor asupra serviciilor publice digitalizate, gradul de utilizare a platformelor de e-guvernare, dificultățile întâmpinate și nivelul de încredere în aceste soluții digitale.

Confidențialitate:

Toate răspunsurile sunt anonime și vor fi utilizate doar în scop academic. Nu sunt colectate date personale, iar răspunsurile vor fi analizate în mod general, ca parte a unui studiu statistic. Nu vor exista referiri la persoane individuale.

Vă mulțumesc pentru timpul acordat și pentru sprijinul în realizarea acestei cercetări!

1. *Vârsta dumneavoastră:*

- Sub 18 ani
- 18–25 ani
- 26–35 ani
- 36–50 ani
- Peste 50 ani

2. *Gen:*

- Feminin
- Masculin
- Prefer să nu spun

3. *Nivelul de studii:*

- Liceal
- Postliceal
- Universitar
- Postuniversitar

4. *Locuiți în:*

- Mediul urban
- Mediul rural

5. *Aveți acces regulat la internet?*

- Da, acasă și pe mobil
- Doar acasă
- Doar pe mobil
- Nu

6. *Cât de des utilizați internetul pentru a accesa informații sau servicii publice?*

- Frecvent (săptămânal)
- Ocazional (câteva ori pe lună)
- Rar (1-2 ori/an)
- Niciodată

7. *Cum v-ați evalua competențele digitale?*

- Foarte bune

- Bune
 - Medii
 - Slabe
8. *Ați utilizat până acum platforme de e-guvernare (ex: ghișeul.ro, platforma ROeID, e-guvernare.ro, SPV etc.)?*
- Da
 - Nu
9. *Dacă da, cât de frecvent le utilizați?*
- O dată pe an sau mai rar
 - De câteva ori pe an
 - Lunar
 - Săptămânal
 - Nu am folosit niciodată
10. *Ce tipuri de servicii ați accesat prin aceste platforme? (puteți selecta mai multe variante)*
- Plata taxelor și impozitelor
 - Obținerea cazierului judiciar/fiscal
 - Înregistrarea unei firme sau PFA
 - Depunerea declarațiilor fiscale
 - Solicitarea unor documente administrative (certificate, adeverințe etc.)
 - Altceva (vă rugăm să specificați): _____
 - Nu am accesat niciodată
11. *Cât de ușor de utilizat vi se par aceste platforme?*
- Foarte ușor
 - Ușor
 - Nici ușor, nici greu
 - Greu
 - Foarte greu
12. *Ce dificultăți ați întâmpinat (dacă ați întâmpinat)?*
- Interfață complicată
 - Probleme tehnice / erori frecvente
 - Lipsa de informații clare
 - Necesitatea autentificării complicate
 - Alte probleme: _____
 - Nu am întâmpinat dificultăți
13. *Considerați că utilizarea platformelor de e-guvernare a redus timpul petrecut pentru rezolvarea problemelor administrative?*
- Da, semnificativ
 - Da, într-o oarecare măsură
 - Nu prea
 - Deloc
14. *Cât de mult aveți încredere în securitatea datelor personale furnizate acestor platforme?*

- Foarte multă încredere
- Destul de multă încredere
- Puțină încredere
- Nicio încredere

15. *Ați prefera să rezolvați probleme administrative online sau la ghișeu fizic, dacă ați avea de ales?*

- Online
- La ghișeu
- Depinde de situație

16. *Cât de informat(ă) considerați că sunteți în legătură cu riscurile online (ex: furtul de date, atacuri cibernetice)?*

- Foarte bine informat(ă)
- Destul de informat(ă)
- Puțin informat(ă)
- Deloc

17. *Credeți că dezinformarea afectează încrederea oamenilor în platformele de e-guvernare?*

- Da
- Nu
- Nu știu

References

- [1] Comisia Europeană, „Guvernarea electronică și serviciile publice digitale,” [Interactiv]. Available: <https://digital-strategy.ec.europa.eu/ro/policies/egovernment>. [Accesat 2025 februarie 23].
- [2] HOTĂRÂRE nr. 20 din 4 ianuarie 2001, „organizarea și funcționarea Ministerului Comunicațiilor și Tehnologiei Informatiei,” [Interactiv]. Available: <https://legislatie.just.ro/Public/DetaliiDocumentAfis/25961>. [Accesat 4 mai 2025].
- [3] Sistemul Electronic de Achiziții Publice, [Interactiv]. Available: <https://www.e-licitatie.ro>. [Accesat 26 februarie 2025].
- [4] Sistemul Electronic Național, [Interactiv]. Available: <https://www.romania.gov.ro>. [Accesat 26 februarie 2025].
- [5] Ministerul Finanțelor Publice, „Portalul serviciilor publice de plată,” [Interactiv]. Available: <https://www.ghiseul.ro>. [Accesat 26 februarie 2025].
- [6] Guvernul României, „Strategia Națională de E-guvernare 2014-2020,” [Interactiv]. Available: <https://www.gov.ro>. [Accesat 26 februarie 2025].
- [7] C. Vrabie, „Promisiunile Inteligenței Artificiale (AI) Administrației Publice și Orașelor Inteligente,” *SCIC*, vol. 11, 2024.
- [8] C. Vrabie, *Elemente de e-guvernare*, București: Editura Pro Universitaria, 2016.
- [9] C. Vrabie, C. Antonie, L. Iordache și L. Brosner, „E-guvernarea în municipiile din România,” *SCIC*, vol. 1, 2023.
- [10] C. C. MANDA, „Digitalizarea administrației publice din Romania – între nevoile și aspirațiile unei societăți moderne a secolului XXI.,” *SCIC*, vol. 9, 2023.
- [11] M. G. MIHĂILĂ, „E-guvernarea, Romania 2000-2030. Orașe inteligente și dezvoltare urbană,” *SCIC*, vol. 6, 2023.
- [12] E. I. Constantin și D. Ș. Voinea, „Transformarea digitală în administrația publică – Soluții informatice și rolul formării profesionale,” 2023. [Interactiv]. Available: https://ina.gov.ro/wp-content/uploads/2024/01/Transformare-digitala-in-administratia-publica_Solutii-informactice-si-rolul-formarii-profesionale.pdf. [Accesat 27 februarie 2025].
- [13] MINISTERUL CERCETĂRII, INOVĂRII ȘI DIGITALIZĂRII, „GHIDUL DIGITALIZĂRII”.
- [14] C. Săvulescu, „Tendințe ale e-guvernării în context național și internațional,” *SCIC*, vol. 1, 2023.
- [15] Ministerul Afacerilor Externe, „Organizația pentru Cooperare și Dezvoltare Economică (OCDE),” [Interactiv]. Available: <https://www.mae.ro/node/1481>. [Accesat 28 februarie 2025].
- [16] C. Vrabie, „Rețelele sociale și rolul lor în societatea de astăzi,” *SCIC*, vol. 2, 2023.

- [17] Comisia Europeană, „Abordarea europeană a inteligenței artificiale,” [Interactiv]. Available: <https://digital-strategy.ec.europa.eu/ro/policies/european-approach-artificial-intelligence>. [Accesat 01 martie 2025].
- [18] NASA, „What is Artificial Intelligence?,” [Interactiv]. Available: <https://www.nasa.gov/what-is-artificial-intelligence/>. [Accesat 01 martie 2025].
- [19] Legea nr. 161/2003 , „privind măsurile necesare pentru accelerarea reformei economice și modernizarea administrației publice,” [Interactiv]. Available: <https://legislatie.just.ro/public/detaliidocument/43323>. [Accesat 01 martie 2025].
- [20] Comisia Europeană, „Semnături electronice,” [Interactiv]. Available: <https://digital-strategy.ec.europa.eu/ro/policies/esignatures>. [Accesat 02 martie 2025].
- [21] Legea nr. 455/2001, „privind semnătura electronică,” [Interactiv]. Available: <https://legislatie.just.ro/Public/DetaliiDocument/29903>. [Accesat 02 martie 2025].
- [22] „Protecția datelor în conformitate cu RGPD,” [Interactiv]. Available: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_ro.htm. [Accesat 03 martie 2025].
- [23] Microsoft, „Ce este protecția datelor?,” [Interactiv]. Available: <https://www.microsoft.com/ro-ro/security/business/security-101/what-is-data-protection>. [Accesat 03 martie 2025].
- [24] „Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal,” [Interactiv]. Available: <https://www.dataprotection.ro>. [Accesat 04 martie 2025].
- [25] Comisia Europeană, „Descoperiți eIDAS,” [Interactiv]. Available: <https://digital-strategy.ec.europa.eu/ro/policies/discover-eidas>. [Accesat 04 martie 2025].
- [26] World Health Organization, „WHO-convened global study of origins of SARS-CoV-2: China Part”.
- [27] World Health Organization, [Interactiv]. Available: <https://www.who.int>. [Accesat 06 martie 2025].
- [28] World Health Organization, „COVID-19 Cases, World,” [Interactiv]. Available: <https://data.who.int/dashboards/covid19/cases?n=c>. [Accesat 06 martie 2025].
- [29] Comisia Europeană, „Soluții digitale în timpul pandemiei,” [Interactiv]. Available: https://commission.europa.eu/strategy-and-policy/coronavirus-response/digital-solutions-during-pandemic_ro#soluții-inovatoare. [Accesat 06 martie 2025].
- [30] Comisia Europeană, „Rolul aplicațiilor de depistare și de avertizare a contactilor în timpul pandemiei de COVID-19,” [Interactiv]. Available: https://commission.europa.eu/strategy-and-policy/coronavirus-response/travel-during-coronavirus-pandemic/contact-tracing-and-warning-apps-during-covid-19_ro. [Accesat 07 martie 2025].
- [31] Consiliul European, „Certificatul digital al UE privind COVID,” [Interactiv]. Available: <https://www.consilium.europa.eu/ro/infographics/eu-digital-covid-certificate/>. [Accesat 07 martie 2025].

- [32] I. Petcu și A. F. Radu, „The education system, the way to fight fake news,” *TRUST*, vol. 1, 2024.
- [33] Institutul Național de Statistică, [Interactiv]. Available: https://insse.ro/cms/sites/default/files/com_presa/com_pdf/tic_r2024.pdf. [Accesat 20 martie 2025].
- [34] C. VRABIE, „Convergenta securitatii digitale,” *SCIC*, vol. 3, 2023.
- [35] O. A. Sarcea (Manea), „AI & Cybersecurity – connection, impacts, way ahead,” *TRUST*, vol. 1, 2024.
- [36] Microsoft, „Ce este un atac cibernetic?,” [Interactiv]. Available: <https://www.microsoft.com/ro-ro/security/business/security-101/what-is-a-cyberattack>. [Accesat 25 martie 2025].
- [37] Microsoft, „Ce este securitatea cibernetică?,” [Interactiv]. Available: <https://www.microsoft.com/ro-ro/security/business/security-101/what-is-cybersecurity>. [Accesat 25 martie 2025].
- [38] A. M. Tîrziu și A. Ciuperca, „Protectia si securitatea informatiilor la nivelul autoritatilor publice nationale din Romania,” *SCIC*, vol. 2, 2023.
- [39] Agenția Națională de Administrare Fiscală (ANAF), [Interactiv]. Available: anaf.ro/anaf/internet/ANAF. [Accesat 26 martie 2025].
- [40] Directoratul Național de Securitate Cibernetică (DNSC), [Interactiv]. Available: <https://dnsc.ro>. [Accesat 26 martie 2025].
- [41] Directoratul Național de Securitate Cibernetică, „ALERTĂ: Phishing E-mail ANAF,” [Interactiv]. Available: <https://dnsc.ro/citeste/alerta-phishing-e-mail-anaf>. [Accesat 27 martie 2025].
- [42] Cibernetică, Directoratul Național de Securitate, „DNSC marchează finalizarea proiectului Romanian Cyber Care Health,” [Interactiv]. Available: <https://dnsc.ro/citeste/dnsc-marcheaza-finalizarea-proiectului-romanian-cyber-care-health-ro-cch-sanatate-digital-mai-sigur-prin-colaborare-si-inovatie-strategica>. [Accesat 28 martie 2025].
- [43] Romanian Cyber Care Health (RO-CCH), [Interactiv]. Available: <https://www.rocch.ro>. [Accesat 28 martie 2025].
- [44] Planul Național de Redresare și Reziliență, [Interactiv]. Available: <https://proiecte.pnrr.gov.ro/#/home>. [Accesat 29 martie 2025].
- [45] Planul Național de Redresare și Reziliență, „Dezvoltarea competențelor digitale: prezentarea proiectului și a principalelor rezultate,” [Interactiv]. Available: <https://www.anfp.gov.ro/media/3qaeydtk/dezvoltarea-competențelor-digitale-prezentarea-proiectului-și-a-rezultatelor.pdf>. [Accesat 30 martie 2025].
- [46] This is the story of the world's most advanced digital society, „E-Estonia,” [Interactiv]. Available: <https://digiexpo.e-estonia.com/story-of-e-estonia/>. [Accesat 9 aprilie 2025].
- [47] M. Lauristin, „Tiger Leap,” [Interactiv]. Available: https://www.educationestonia.org/wp-content/uploads/2023/01/tigrihype2007ENG_standard.pdf. [Accesat 09 aprilie 2025].

- [48] „X-Road,” [Interactiv]. Available: <https://x-road.global>. [Accesat 10 aprilie 2025].
- [49] E-Estonia, „X-Road – interoperability services,” [Interactiv]. Available: <https://e-estonia.com/solutions/x-road-interoperability-services/x-road/>. [Accesat 10 aprilie 2025].
- [50] „X-Road History,” [Interactiv]. Available: <https://x-road.global/xroad-history>. [Accesat 10 aprilie 2025].
- [51] E-estonia, „E-Identity,” [Interactiv]. Available: <https://e-estonia.com/solutions/estonian-e-identity/id-card/>. [Accesat 11 aprilie 2025].
- [52] „Introduction,” [Interactiv]. Available: <https://www.id.ee/en/rubriik/introduction/>. [Accesat 11 aprilie 2025].
- [53] E-Estonia, „Mobile ID,” [Interactiv]. Available: <https://e-estonia.com/solutions/estonian-e-identity/mobile-id/>. [Accesat 11 aprilie 2025].
- [54] „Mobile-ID: digital identity document on smart phone,” [Interactiv]. Available: <https://www.id.ee/en/article/mobile-id-digital-identity-document-on-smart-phone/>. [Accesat 11 aprilie 2025].
- [55] „The story,” [Interactiv]. Available: <https://www.e-resident.gov.ee/the-story/>. [Accesat 11 aprilie 2025].
- [56] „Smart-ID,” [Interactiv]. Available: <https://digiexpo.e-estonia.com/all-solutions/smart-id/>. [Accesat 11 aprilie 2025].
- [57] E-Estonia, „Smart ID,” [Interactiv]. Available: <https://e-estonia.com/solutions/estonian-e-identity/smart-id/>. [Accesat 11 aprilie 2025].
- [58] E-Estonia, „e-Health,” [Interactiv]. Available: <https://e-estonia.com/solutions/e-health-2/e-health-records/>. [Accesat 11 aprilie 2025].
- [59] E-Estonia, „e-Prescription,” [Interactiv]. Available: <https://e-estonia.com/solutions/e-health-2/e-prescription/>. [Accesat 11 aprilie 2025].
- [60] E-estonia, „e-Ambulance,” [Interactiv]. Available: <https://e-estonia.com/solutions/e-health-2/e-ambulance/>. [Accesat 11 aprilie 2025].
- [61] Autoritatea Națională pentru Cercetare, „Lansarea aplicației ROeID – centralizarea tuturor serviciilor publice, accesibile cu un singur login al identității digitale,” [Interactiv]. Available: <https://www.mcid.gov.ro/lansarea-aplicatiei-roeid-centralizarea-tuturor-serviciilor-publice-accesibile-cu-un-singur-login-al-identitatii-digitale-11441/>. [Accesat 21 mai 2025].
- [62] CNAS, „Cardul național de asigurări de sănătate,” [Interactiv]. Available: <https://cnas.ro/cardul-national-de-asigurari-de-sanatate/>. [Accesat 12 aprilie 2025].
- [63] CNAS, „Informații generale,” [Interactiv]. Available: <https://cnas.ro/informatii-generale/>. [Accesat 12 aprilie 2025].

- [64] Lege 95/2006, „Cardul național de asigurări sociale de sănătate,” [Interactiv]. Available: <https://lege5.ro/gratuit/g42tmnjsgi/cardul-national-de-asigurari-sociale-de-sanatate-lege-95-2006?dp=hazdanbzha4dc>. [Accesat 12 aprilie 2025].
- [65] CNAS, „Ghidul asiguratului,” [Interactiv]. Available: <https://cnas.ro/wp-content/uploads/2025/01/Ghidul-asiguratului-editia-3.pdf> . [Accesat 12 aprilie 2025].
- [66] HOTĂRÂRE nr. 520 din 24 iulie 2013, [Interactiv]. Available: <https://legislatie.just.ro/Public/DetaliiDocument/150246>. [Accesat 13 aprilie 2025].
- [67] LEGE nr. 296 din 26 octombrie 2023, [Interactiv]. Available: <https://legislatie.just.ro/Public/DetaliiDocumentAfis/275745>. [Accesat 13 aprilie 2025].
- [68] E-Factura, „Ghid privind utilizarea sistemului național de facturare electronică RO e-Factura,” [Interactiv]. Available: https://static.anaf.ro/static/10/Anaf/AsistentaContribuabili_r/Ghid_RO_eFactura.pdf. [Accesat 13 aprilie 2025].
- [69] Ghiseul.ro, [Interactiv]. Available: <https://www.ghiseul.ro/ghiseul/public/informatii/intrebari-frecvente>. [Accesat 14 aprilie 2025].
- [70] Licitatii.SEAP, [Interactiv]. Available: <https://licitatiiseap.ro/seap/>. [Accesat 14 aprilie 2025].
- [71] Ghiseul.ro, „Sistemul Național Electronic de Plată Online cu Cardul Bancar,” [Interactiv]. Available: <https://www.ghiseul.ro/ghiseul/public/help/Manual%20de%20utilizare%20-%20Contribuabili.pdf>. [Accesat 14 aprilie 2025].
- [72] Ministerul Cercetării, Inovării și Digitalizării, [Interactiv]. Available: <https://www.mcid.gov.ro>. [Accesat 2025 februarie 2025].