Școala Națională de Studii Politice și Administrative
Facultatea de Administrație Publică

CONTRIBUȚIA DIGITALIZĂRII INSTITUȚIILOR DE NIVEL CENTRAL LA CREȘTEREA CALITĂȚII GUVERNĂRII STATALE

- lucrare de licență, specializarea Administrație Publică -

Coordonator

Conf. Univ. Dr. Cătălin VRABIE

Absolvent

Sabadiș Gabriel

București
2024

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

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

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

6. Trimiteți profesorului coordonator lucrarea doar în format **Microsoft Word** – alte formate nu vor fi procesate;
7. **Nu ștergeți 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: Sabadiș Gabriel

Data și semnătura: 06.12.2023

Cuprins

Abstract

Prin această lucrare, se urmărește investigarea și analizarea procesului de digitalizare în instituțiile de nivel central ale administrației publice din România. **Obiectivele** includ definirea și evidențierea importanței digitalizării în contextul administrației publice, evaluarea progresului și evoluției digitalizării în aceste instituții, precum și examinarea conceptelor asociate calității guvernării în era digitalizării, evidențiate în cadrul Agenției Naționale de Administrare Fiscală prin analiza eficienței și transparenței acesteia. **Studii prealabile:** Cercetarea își propune să exploreze concepte fundamentale, cum ar fi digitalizarea, administrarea eficientă și buna guvernare, bazându-se pe o **abordare** descriptivă, ce are la bază cercetarea cantitativă, folosind ca instrument de cercetare chestionarul. **Rezultate:** Lucrarea anticipează ca și rezultat principal, în urma studiului de caz, posibilitatea existenței unui cadru tehnologic necesar tranziției către o administrație fiscală digitală, în care să existe atât transparența corespunzătoare, cât și eficiența adecvată în relația cu cetățenii. **Implicații:** Studiul propune implicații semnificative pentru practicienții din domeniul administrației publice, care pot valorifica exemplul de bune practici, contribuind astfel la optimizarea și implementarea proceselor digitale. **Valoarea** acestei lucrări constă în contribuția sa la înțelegerea procesului de digitalizare în administrația publică românească și la sublinierea impactului acestui fenomen asupra calității guvernării statale. Lucrarea adaugă o perspectivă detaliată și relevanță practică la discuția generală despre digitalizarea instituțiilor publice, prin aducerea în prim plan a analizei privind eficiența și transparența în cadrul Agenției Naționale de Administrare Fiscală

Cuvinte cheie: eficiență, transparență, securitate, modernizare digitală

Introducere

Cu toții facem parte, cu sau fără voia noastră, din această eră a digitalizării, fără a realiza cât de ancorați suntem în tot acest proces. Noile generații au avut parte involuntar de implicare în lumea digitală, încă din primele momente ale vieții și până în prezent, urmând să contribuie la dezvoltarea nesfârșită a digitalizării. De la modul în care ne gestionăm agenda zilnică, până la modalitățile de divertisment și cumpărături, tehnologia digitală a facilitat experiențele noastre. Accesul rapid la informații, serviciile online și interconectivitatea continuă să redefinească modul în care experimentăm și navigăm prin lumea din jurul nostru. Acest fenomen nu doar că ne-a modificat comportamentele, ci și a contribuit la modelarea societății într-un mod inedit, aducând cu sine atât oportunități, cât și provocări. Deși filosofii afirmă că totul are un început și un sfârșit, tehnologia a dovedit contrariul. Ne situăm astfel într-un secol în care impactul tehnologic, cât și nivelul la care a ajuns să fie dezvoltată întreaga ramură digitală, a continuat să evolueze, fără momente de plafonare, atingând praguri mai mari ca niciodată.

Înainte de a enumera multitudinea inovațiilor tehnologice din prezent, să ne amintim de piatra de temelie care a dat startul lumii digitale. Astfel, ne reamintim de unul dintre primele dispozitive din domeniul digital, și anume calculatorul. Termenul „calculator", conform Dicționarului explicativ al limbii române, se referă la „*maşină sau instalaţie cu care se efectuează automat operaţii matematice şi logice*" [1]. Începând cu anii 1940-1950, au apărut primele calculatoare electronice digitale, cu tuburi electronice, a căror putere de procesare era net inferioară calculatoarelor din prezent, având o viteză de calcul de numai 50 de operații pe secundă. Cincizeci de ani mai târziu, conform legii lui Moore[1], s-a ajuns la apariția unor noi dispozitive precum cele create de „Apple"[2], având o putere echivalentă a 200 de miliarde de tuburi electronice, iar asta era doar începutul tehnologiilor dezvoltate de către marile companii. [2]. Amintim astăzi de noi inovații tehnologice, precum inteligența artificială (AI[3]), realitatea virtuală (VR[4]) sau sistemele de tip „blockchain"[5], care continuă să redefinească limitele, fiind uneori de neînțeles pentru cetățeanul de rând, datorită mecanismelor din spatele funcționării acestora.

[1] această lege presupune că densitatea de tranzistori într-un circuit integrat se dublează la fiecare 2 ani
[2] referință la compania de electronice
[3] acronim pentru „Artificial Intelligence"
[4] acronim pentru „Virtual Reality"
[5] registru al datelor descentralizate, partajate în mod securizat, prin care permite unui grup colectiv de participanți să partajeze date.

Vasile Baltac afirmă despre lumea digitală că aceasta „*Este o lume nouă, apărută pe parcursul unei singure generații umane și care ne confruntă cu oportunități și pericole, ne împarte în nativi digitali și non-nativi, ne obligă să ne adaptăm la schimbări radicale în modurile de comunicare și relaționare interumane.*" [3]. Observăm cum, în urma evoluției dispozitivelor tehnologice care au ajuns să își facă simțită prezența în viața fiecăruia, dezvoltarea aplicațiilor creează nevoia de a ne îngloba tot mai mult în folosirea acestor „device-uri"[6]. De aceea este important să avem o societate digitalizată, ce are la bază cetățeni bine informați și pregătiți să utilizeze tehnologia în mod eficient. Alfabetizarea digitală[7] devine astfel esențială pentru a ne asigura că toți indivizii pot beneficia de oportunitățile oferite de lumea digitală.

Odată ce o parte a statului, reprezentată de cetățeni, atinge un anumit nivel de digitalizare, ne punem întrebarea cu privire la cealaltă parte distinctă, reprezentată de către organizațiile publice, în vederea atingerii nivelului de digitalizare, care să satisfacă nevoile ambelor părți, în ceea ce privește buna guvernare a statului. Apare astfel, guvernarea electronică, pe care o putem defini drept „*utilizarea tehnologiei informației de către agențiile guvernamentale (organizațiile publice) în relațiile cu cetățenii, întreprinderile și alte corpuri guvernate [...]. Beneficiile rezultate putând fi reducerea corupției, creșterea transparenței, mai mult confort, creșterea veniturilor și/sau reducerea costurilor*." [4]. O altă perspectivă poate fi aceea de a livra serviciile publice într-un mod eficient și favorabil cetățeanului prin folosirea tehnologiilor digitale, fiind o modalitate mult mai practică. [5].

Se creează astfel o „rețea" de inter-comunicații între instituțiile publice și cetățeni, prin care se încearcă, pe de o parte, să se faciliteze fluxul birocratic, iar pe de altă parte, aceste sisteme oferă o relație mai puternică între stat și cetățean. Apar astfel numeroase servicii și sisteme de tipul comerțului electronic, al documentelor electronice, al programării electronice la una dintre instituțiile guvernamentale, serviciul de plată online a taxelor și impozitelor, servicii de obținere a autorizațiilor prin intermediul platformelor online, precum și sisteme implementate recent, de tipul alertelor electronice (ro-alert), folosite de către guvern pentru informarea cetățenilor cu privire la eventuale situații de urgență.

Dam astfel naștere unor orașe de tip „smart cities", asociate cu orașe ale viitorului, prin care se dorește creșterea sustenabilității și rezolvarea multitudinii de probleme, atât de tipul economic, de mediu sau chiar social, prin intermediul tehnologiilor digitale [6]. Prin oferirea unor servicii de calitate, prin care creștem eficiența și transparența în relația stat-cetățean, diminuând pe cât posibil costurile prin soluții avantajoase, ajungem în final la atingerea principalului scop, acela de a îmbunătăți calitatea vieții la nivelul întregii societăți.

În cadrul primului capitol al acestei lucrări, vom defini mai pe larg importanța digitalizării în administrația publică din România, urmărind procesul și evoluția digitalizării în cadrul instituțiilor de nivel central, abordând de asemenea concepte cu privire la calitatea guvernării în era digitalizării. Totodată, relația dintre cetățeni și organizațiile publice se va regăsi în capitolul al doilea, urmând ca în cel de-al treilea capitol să descoperim dacă instituțiile de nivel central se pot adapta în contextul noilor realități digitale.

Context

În contextul în care instituțiile publice de nivel central se confruntă cu evoluția accelerată a noilor tehnologii digitale în era contemporană, este necesar ca digitalizarea să vină în ajutorul acestora pentru a le sprijini în procesul unei guvernări calitative. Astfel, transformarea digitală în cadrul instituțiilor publice reprezintă o etapă esențială în procesul de adaptare a administrației publice, odată cu evoluția societății.

[6] se referă la un obiect sau instrument care poate fi utilizat într-un anumit context sau domeniu pentru a realiza anumite activități sau pentru a furniza anumite servicii.
[7] face referire la aptitudinile, cunoștințele și înțelegerea necesară pentru a utiliza noi tehnologii

Totodată, această necesitate de digitalizare a instituțiilor publice de nivel central, este constrânsă de numarul mare de cereri din partea cetățenilor la adresa instituțiilor de nivel central (fie prin apeluri telefonice, prin sesiuni chat, formulare sau alte metode), a căror numar este în continuă creștere [7]. Astfel, dezvoltarea capacității societății de a adaptare a noilor cerințe în ceea ce privește întregul proces digital, atrage de la sine exigențe asupra instituțiilor de a se ridica la standardele noilor tehnologii.

Numeroase proiecte au venit în sprijinul contextului actual, încercând să sprijine instituțiile publice în acest demers. Amintim astfel, de sistemul național privind factura electronică „RO e-Factură", ce a fost creat pentru a facilita operatorii economici printr-un serviciu electronic de primire și emitere a facturilor, având un puternic impact în domeniul administrativ, dar și pe plan economic și de mediu, intrând în vigoare la data de 01.01.2024 [8]. Totodată, amintim de platforme precum cea a „Sistemului electronic de achiziții publice" sau „Ghișeul.ro" ce au un scop comum , alături de cea menționată anterior, acela de a încuraja procesul de digitalizare în rândul instituțiilor publice, oferind o mai bună guvernare și o relație mai strânsă cu cetățenii, în contextul evoluției rapide a tehnologiilor care sunt nelipsite în rândul societății moderne.

Astfel, tendințele imediate ale tehnologiilor digitale în societatea contemporană, precum și necesitatea adaptării instituțiilor publice de nivel central la această transformare digitală, accentuează procesul de digitalizare în administrația publică românească și reflecta impactul acestui fenomen asupra calității guvernării statale.

Capitolul 1. Principii ale digitalizării instituțiilor de nivel central

Într-o eră dominată de tehnologie și schimbări accelerate, digitalizarea devine un element primordial pentru modernizarea și eficientizarea administrației publice din România. În contextul unei societăți tot mai conectate și a unei economii în plină transformare digitală, administrația publică se confruntă cu presiuni, și totodată oportunități, pentru a-și adapta procesele și serviciile la noile cerințe și nevoi ale cetățenilor.

În continuare, vom încerca să definim și să transpunem importanța digitalizării în administrația publică din România, arătând procesul și evoluția acestui fenomen în cadrul instituțiilor de nivel central, precum și conceptele cheie legate de calitatea guvernării în era digitalizării.

1.1. Definirea si importanța digitalizării în administrația publică din România

Deși poate fi la îndemâna oricui de a se avânta prezumției că digitalizarea în administrația publică reprezintă simpla conversie a documentelor în format electronic, tehnologiile digitale au demonstrat contrariul. Acestea nu sunt doar un mijloc de implementare a unei strategii pentru modernizare a societății și furnizarea de servicii către cetățeni, ci determină, în mare măsură, direcția schimbării pe care un stat sau o întreagă societate urmează să o ia.

Evoluția tehnologiilor digitale a schimbat fundamental felul în care interacționăm cu informația și cum ne desfășurăm activitățile cotidiene. Digitalizarea în administrația publică nu se rezumă doar la conversia documentelor fizice în formate electronice, ci reprezintă o transformare profundă a întregului sistem. Această transformare include optimizarea proceselor administrative, facilitarea accesului la serviciile publice, și crearea unui mediu propice pentru inovare și colaborare.

Un aspect esențial al digitalizării este capacitatea de a colecta, analiza și utiliza datele în mod eficient. Prin intermediul tehnologiilor digitale avansate, administrația publică poate să obțină o înțelegere mai profundă a nevoilor și preferințelor cetățenilor, ceea ce poate duce la servicii mai personalizate și eficiente. De exemplu, implementarea sistemelor de analiză a datelor poate ajuta la identificarea tendințelor și problemelor în diverse domenii, de la educație și sănătate, până la infrastructură și mediu înconjurător [9].

În plus, digitalizarea oferă oportunități inedite pentru îmbunătățirea transparenței și responsabilității în administrația publică. Prin publicarea online a informațiilor despre bugete, decizii și proiecte de lege, cetățenii pot urmări mai ușor activitățile guvernamentale și pot participa activ la procesele decizionale. Această transparență sporită poate contribui la construirea unei relații de încredere între cetățeni și instituțiile publice.

De asemenea, digitalizarea poate juca un rol important în promovarea integrării sociale. Prin facilitarea accesului la serviciile publice online, precum și prin dezvoltarea competențelor digitale în rândul populației, administrația publică poate reduce barierele în accesarea resurselor și informațiilor. Acest lucru poate avea un impact pozitiv în special în comunitățile marginalizate sau mai puțin dezvoltate, oferindu-le șanse egale în societatea digitală.

Instituțiile administrației publice își schimbă modul de lucru pentru a îmbunătăți furnizarea de servicii, pentru a fi mai eficace, iar acest proces implică și digitalizarea. Digitalizarea în sectorul public implică noi modalități de lucru cu părțile interesate, noi servicii, noi cadre de furnizare a serviciilor, precum și noi forme de relații [10]. Considerăm că aceste relații formate prin intermediul digitalizării în administrația publică au ca prim obiectiv orientarea către cetățeni și către nevoile lor. Procesele digitale ar trebui să fie concepute și implementate având în vedere experiența utilizatorului, pentru a le face mai ușor de accesat și utilizat. Acest lucru poate implica dezvoltarea de platforme online intuitive, crearea de aplicații pentru servicii publice sau facilitarea accesului la informații și documente prin intermediul portalurilor web.

Odată ce această relație, instituție – cetățean, este consolidată, se va da naștere unei mai bune colaborări. Posibilitatea de a trimite cereri, documente sau rapoarte online poate simplifica și accelera procesele administrative, reducând în același timp birocrația și timpul pierdut pentru deplasări, acesta fiind doar unul dintre factorii care favorizează ambele capete care relaționează, fiind o situație de tipul „win-win”[8].

Implementarea de soluții digitale poate sprijini transparența și responsabilitatea în administrația publică. Accesul la informații și decizii guvernamentale poate fi facilitat prin publicarea acestora online, oferind cetățenilor posibilitatea de a fi mai bine informați și implicați în procesele decizionale.

Cu toate acestea, pentru a asigura succesul transformării digitale în administrația publică, este esențial să existe investiții corespunzătoare în infrastructura digitală și în formarea personalului. Astfel, digitalizarea poate deveni un factor important al modernizării și eficientizării administrației publice în România, având un impact semnificativ asupra serviciilor oferite cetățenilor și asupra modului în care aceștia interacționează cu instituțiile guvernamentale.

1.2. Procesul și evoluția digitalizării în cadrul instituțiilor de nivel central

Așa cum am menționat și în introducerea acestei lucrări, întreg progresul tehnologic a apărut treptat, însă evoluția acestuia a fost una foarte accelerată, într-un timp foarte scurt, cu o anvergură majoră, atât pentru instituțiile statului, cât și pentru cetățeni. Într-o eră în care tehnologia digitală a devenit parte integrantă a vieții noastre cotidiene, procesul de digitalizare în instituțiile publice reprezintă un element cheie în evoluția modului în care administrația interacționează cu cetățenii și își desfășoară activitățile. De-a lungul istoriei, digitalizarea în sectorul public a parcurs un drum fascinant, cu transformări semnificative și impact profund asupra modului în care se realizează comunicarea și gestionarea informațiilor.

Deși am făcut precizarea clară că digitalizarea reprezintă mai mult decât conversia documentelor fizice în format electronic, și această etapă a constituit un prim pas în apariția digitalizării în sectorul public. În trecut, corespondența oficială între instituțiile publice și

[8] conform dicționarului „Oxford Languages” acest termen denotă o situație în care ambele părți beneficiază într-un anume fel

cetățeni, precum și între instituțiile publice între ele, se realiza predominant prin intermediul scrisorilor trimise prin poștă. Acest proces era adesea îngreunat de expedierea lentă, costurile asociate cu aceasta și necesitatea gestionării și arhivării fizice a documentelor. Amintim totodată de apariția telegrafului în sectorul public și impactul său revoluționar asupra comunicării, transformând corespondența și schimbul de informații într-un proces mult mai rapid și eficient [11].

Odată cu avansul tehnologic și cu adoptarea e-mailului în administrația publică, peisajul comunicării s-a schimbat radical. E-mailul a câştigat în faţa poştei obişnuite, datorită vitezei și costurilor reduse [12]. Acesta a facilizat si eficientizat comunicarea atât între departamentele unei instituții publice, cât și cu cetățenii. E-mailul a devenit un instrument esențial pentru corespondența oficială, notificări, comunicări interne și externe. Prin simpla apăsare a unui buton, informațiile puteau fi transmise instantaneu, eliminând astfel barierele asociate cu timpul de livrare al scrisorilor și reducând considerabil costurile de expediere [13]. Această tranziție către utilizarea e-mailului a reprezentat un prim pas important în adaptarea instituțiilor publice la noile tehnologii digitale și a pregătit terenul pentru etapele ulterioare ale digitalizării. Mai mult decât atât, a deschis calea către o comunicare mai transparentă, accesibilă și eficientă între cetățeni și administrația publică. Astfel, cetățenii au început să aibă posibilitatea de a trimite solicitări, sugestii sau reclamații online, primind în schimb un răspuns rapid și precis.

Unul dintre primele proiecte notabile de digitalizare a fost implementat în cadrul Ministerului Finanțelor Publice (MFP) în 2005, când s-a lansat proiectul „Spațiul Privat Virtual” (SPV). Acesta a fost un pas important în direcția digitalizării administrației publice centrale, oferind contribuabililor și firmelor acces online la informații legate de taxe, impozite, situația conturilor fiscale și alte informații de interes [14]. Proiectul „SPV” a reprezentat o inițiativă întrăzneață în procesul de digitalizare al administrației publice din România. Acest proiect a introdus un nou nivel de accesibilitate și eficiență în relația dintre cetățeni, firme și instituțiile fiscale. Prin intermediul „SPV”, contribuabilii și firmele au beneficiat de posibilitatea de a accesa informații fiscale esențiale într-un mod simplu și rapid. Această schimbare a eliminat impedimentele geografice și temporale, facilitând astfel procesul de conformare la cerințele fiscale. Un alt aspect remarcabil al proiectului „SPV” este reprezentat de transparența sporită în relația cu autoritățile fiscale. Accesul la informații privind taxele, impozitele și situația conturilor fiscale într-un mediu online și securizat a contribuit la creșterea încrederii și înțelegerii în ceea ce privește obligațiile fiscale.

De asemenea, suntem de părere că „SPV” a avut un impact semnificativ în reducerea birocrației și simplificarea procedurilor administrative. Eliminarea necesității deplasării fizice la instituțiile fiscale pentru diverse operațiuni a reprezentat o economie de timp și resurse pentru contribuabili și firme, conducând în final la o eficiență sporită în gestionarea situațiilor fiscale. Prin toate aceste aspecte, proiectul „SPV” a reprezentat un pas important către o administrație publică modernă, adaptată nevoilor și cerințelor unei societăți din ce în ce mai digitalizate. Astfel, acest proiect a schimbat modul în care interacționează cetățenii și firmele cu autoritățile fiscale, încurajând conformarea și simplificând procesele administrative pentru toți cei implicați.

Un alt exemplu de proiect semnificativ de digitalizare a fost lansat de către Agenția Națională de Administrare Fiscală (ANAF), atunci când aceasta a introdus sistemul de declarații electronice. Introducerea sistemului de declarații electronice a adus multiple beneficii atât contribuabililor, cât și autorităților fiscale. Unul dintre cele mai evidente avantaje este facilitarea și simplificarea procesului de declarare a veniturilor și a altor obligații fiscale pentru cetățeni și firme. Prin intermediul acestui sistem, persoanele fizice și juridice au posibilitatea de a completa și transmite declarațiile fiscale online, eliminând astfel necesitatea completării pe hârtie și depunerea fizică la sediile ANAF. Un alt avantaj este reducerea erorilor în completarea declarațiilor fiscale, deoarece sistemul poate oferi asistență în timp real și verificări automatizate pentru anumite date. Acest lucru conduce la creșterea acurateței datelor fiscale și la evitarea unor situații neplăcute pentru contribuabili.

De asemenea, implementarea declarațiilor electronice a dus la o eficientizare a proceselor administrative din cadrul ANAF. Reducerea volumului de documente fizice și trecerea la formatul digital a contribuit la o gestionare mai rapidă și mai eficientă a informațiilor fiscale. Totodată, cetățenii și firmele pot obține informații, pot depune declarații și pot primi răspunsuri la întrebările lor într-un mod mai comod și mai rapid, direct de pe platforma online a ANAF.

În anul 2013, a fost lansat programul guvernamental „Ghișeul.ro", care a reprezentat o altă etapă importantă în digitalizarea serviciilor publice. Prin intermediul acestui portal, cetățenii au acces la o gamă largă de servicii online, precum eliberarea certificatelor de cazier judiciar, adeverințe de venit, certificatul de naștere și altele [15]. Platforma „Ghiseul.ro" a oferit contribuabililor și firmelor posibilitatea de a depune și gestiona declarațiile fiscale într-un mod simplu, eficient și accesibil. Acest lucru a eliminat necesitatea deplasării la sediile fizice ale ANAF pentru a înregistra și actualiza diversele documente fiscale.

Unul dintre cele mai importante aspecte ale sistemului de declarații electronice este comoditatea și economia de timp pe care o aduce contribuabililor și firmelor. Aceștia pot accesa platforma „Ghiseul.ro" de oriunde, cu conexiune stabilă la internet, în orice moment convenabil pentru ei, fără a fi nevoie să aștepte la cozi sau să se confrunte cu programări complicate. De asemenea, introducerea acestui sistem a dus la reducerea erorilor în procesul de completare și înregistrare a declarațiilor fiscale. Fiind un mediu digital, „Ghiseul.ro" poate oferi notificări și alerte pentru a avertiza utilizatorii în cazul unor posibile greșeli sau omisiuni în declarații. Un alt aspect important este transparența sporită pe care o aduce acest sistem. Contribuabilii au acces la istoricul declarațiilor depuse, pot verifica statusul acestora și pot avea o imagine clară asupra situației lor fiscale, totul într-un mediu securizat și protejat.

Observăm cum, treptat, însăși ministerele și instituțiile publice au dezvoltat și implementat propriile proiecte de digitalizare în diferite domenii, cum ar fi sistemul electronic de achiziții publice (SEAP), creat de Agenția pentru Achiziții Publice. Prin intermediul acesteia se desfășoară și se monitorizează achizițiile publice din România [16], în mod transparent și cu acces gratuit atât pentru instituții, dar și mai important, pentru cetățeni. Proiectul reprezintă o inițiativă esențială în direcția modernizării procesului de achiziții publice din România.

Acest sistem a fost introdus pentru a digitaliza și eficientiza întregul proces de achiziții publice, permițând autorităților publice și entităților contractante să deruleze procedurile de achiziții într-un mod conform cu legislația în vigoare. Unul dintre principalele avantaje ale SEAP este accesibilitatea și egalitatea de tratament pentru toți participanții la procesul de achiziții publice. Prin intermediul platformei online, firmele interesate au posibilitatea să acceseze și să participe la licitații publice fără a fi nevoie de prezență fizică, eliminând astfel bariera geografică și facilitând competiția corectă. De asemenea, „SEAP" contribuie la reducerea birocrației și a timpului necesar pentru derularea procedurilor de achiziții publice. Toate documentele și informațiile necesare pot fi încărcate și gestionate electronic, ceea ce duce la economii semnificative de resurse și la o gestionare mai eficientă a timpului. Un alt aspect important este transparența sporită a procesului de achiziții publice. Toate procedurile, anunțurile de participare, documentele aferente licitațiilor sunt publicate pe platformă, oferind astfel o imagine clară și accesibilă a modului în care sunt cheltuiți banii publici.

Este important de menționat că, deși digitalizarea în administrația publică centrală din România a avut parte de o evoluție semnificativă în ultimii ani, există încă multe provocări și nevoi ce las loc îmbunătățirii. Printre principalele nevoi actuale se enumeră dezvoltarea securității cibernetice, dezvoltarea operabilității sistemelor, simplificarea procedurilor și oferirea de servicii online user-friendly[9], iar acestea sunt doar câteva aspecte care necesită atenție continuă pentru a asigura o administrație publică eficientă și modernă.

[9] conform dicționarului Cambridge, reprezintă o manieră (de obicei legată de computere) simplă de utilizat pentru oameni

Istoria digitalizării în instituțiile publice reflectă o evoluție impresionantă în modul în care acestea funcționează și interacționează cu cetățenii. De la conversia documentelor în format electronic, până la implementarea unor sisteme complexe de comunicare și servicii online, digitalizarea a adus o serie de beneficii semnificative.

1.3. Concepte cu privire la calitatea guvernării în era digitalizării

Calitatea guvernării statale este un concept incert ce nu poate fi definit sau măsurat cu exactitate. Considerăm că nu este nevoie să definim guvernarea, însă guvernarea electronică poate reprezenta pentru multi un concept total nou. Astfel, guvernarea electronică este „*o guvernare care aplică forme şi metode de interacţiune dintre administraţii, cetăţeni şi mediul de afaceri, la prestarea serviciilor publice, prin utilizarea mijloacelor electronice*" [17]. Cu toate acestea, guvernarea electronică este un subiect mult mai complex, extrem de ramificat. Cât despre calitatea guvernării, amintim de principii precum cel al tranparenței și eficienței, concepte ce vor fi detaliate în capitolul urmator.

Sistemul guvernamental, încercând să țină pasul cu progresul tehnologic dezvoltă o nouă ramură, cea digitală, născându-se astfel, e-guvernarea. Conceptele cu privire la e-guvernarea în România, au fost amintite în introducere, de menționat este că aceasta se concentrează și pe implicarea cetățenilor, facilitată prin platforme online pentru consultări publice, dezbateri virtuale și alte instrumente ce încurajează participarea activă a cetățenilor în procesul decizional, oferindu-le oportunitatea de a-și exprima opiniile și preocupările în legătură cu deciziile guvernamentale.

Digitalizarea guvernării publice aduce atât angajaților, cât și cetățenilor, numeroase avantaje. Astfel, în cadrul instituțiilor publice, digitalizarea asigură o gestionare eficientă a resurselor și deschide oportunități pentru dezvoltarea de servicii publice inovatoare, contribuind la oferirea unor servicii de calitate pentru cetățeni. Procesul de digitalizare ar trebui să acorde o atenție deosebită nevoilor cetățenilor, pentru o mai bună guvernare și să le definească clar. Realitatea arată că în ultima perioadă, cetățenii au devenit tot mai exigenți în ceea ce privește administrația publică și solicită servicii simple, rapide și transparente. Digitalizarea eficientă trebuie să fie un proces integrat, care să creeze un cadru propice pentru revizuirea procedurilor administrative și simplificarea acestora [18].

În continuare, amintim aspectele cheie ale conceptului de e-guvernare și modul în care acestea transformă calitatea guvernării în era digitalizării. Unul dintre aceste aspecte este participarea cetățenilor. E-guvernarea oferă cetățenilor posibilitatea de a-și exprima opiniile, sugestiile și preocupările cu privire la politicile și deciziile guvernamentale prin intermediul platformelor online. Un alt beneficiu major al e-guvernării este eficiența administrativă. Prin digitalizarea proceselor administrative, instituțiile publice pot reduce birocrația și costurile asociate prestării serviciilor. Implementarea unor sisteme integrate de management al informațiilor și automatizarea unor proceduri pot duce la o mai bună eficiență în funcționarea administrației publice. De asemenea, e-guvernarea contribuie la creșterea incluziunii digitale. Prin oferirea de servicii și informații online, e-guvernarea asigură că toți cetățenii au acces egal la resursele și beneficiile oferite de administrația publică. Aceasta este o abordare importantă într-o societate tot mai digitalizată, unde accesul la internet și la tehnologie este din ce în ce mai important pentru participarea în viața civică și economică. Totodată, crează relații de interdependență atât între guvern si angajații guvernamentali, cât și între guvern și cetățean, guvern și mediul de afaceri, având implicit un impact si asupra relației mediului de afaceri cu cetățeanul, dezvoltând piața de comerț electronic [19].

Considerăm că e-guvernarea reprezintă o evoluție esențială în calitatea guvernării în era digitalizării. Prin participarea cetățenilor și eficiența administrativă, e-guvernarea poate transforma modul în care instituțiile publice funcționează și interacționează cu cetățenii. Este o oportunitate pentru modernizarea și îmbunătățirea serviciilor publice, aducând beneficii atât pentru guverne, cât și pentru societatea în ansamblu.

Guvernul implementează politici și măsuri pentru a asigura securitatea sistemelor și confidențialitatea informațiilor cetățenilor, având în vedere amenințările din mediul online. Astfel e-guvernarea în România aduce serviciile publice mai aproape de era digitală fiind principalul pilon de susținere al întregii mișcări.

Capitolul 2. Impactul digitalizării asupra eficienței si transparenței guvernării statale

Principala componentă în demersul de reducere a birocrației în instituțiile publice este digitalizarea. În cadrul administrației publice, digitalizarea aduce cu sine o serie de beneficii care ar trebui să fie integrate în strategia instituțională și să fie încurajate de către liderii acesteia. Pe de o parte, digitalizarea conduce la o eficientizare a activității instituționale, facilitând utilizarea optimă a resurselor, reducerea costurilor și contribuind la progresul tehnologic și socio-economic. Pe de altă parte, implementarea digitalizării aduce în prim-plan noi oportunități, prin activarea capacităților și competențelor instituționale, ce pot oferi cetățenilor servicii publice inovative și adaptate la nevoile contemporane [20]. Simplificarea procedurilor administrative și reducerea birocrației, atât pentru cetățeni, cât și la nivel inter și intra-instituțional, sunt esențiale pentru a îmbunătăți eficiența administrației publice în ceea ce privește costurile și timpul, și pentru a consolida transparența și integritatea în furnizarea serviciilor. Aceste măsuri contribuie, de asemenea, la creșterea satisfacției cetățenilor și la îmbunătățirea imaginii administrației publice.

Un element fundamental al debirocratizării este accesul facil și rapid la informații și servicii, aspect esențial pentru un stat funcțional, în care cetățenii să nu se simtă intimidați de contactul cu instituțiile publice. În același timp, digitalizarea este un proces esențial pentru a facilita simplificarea eficientă a procedurilor administrative. Simplificarea trebuie să vizeze eliminarea într-o măsură cât mai mare a reglementărilor, în special a celor secundare, care nu sunt necesare, sunt inutile sau sunt menite să complice accesul cetățenilor la drepturile și serviciile de care beneficiază. Un instrument eficient în acest sens este guvernarea electronică, care presupune transformări fundamentale în sistemul de guvernare. Aceasta implică identificarea și implementarea unor instrumente bazate pe tehnologia informației și comunicațiilor, care să promoveze democratizarea societății, debirocratizarea instituțiilor guvernamentale, transparența proceselor decizionale și participarea cetățenilor la guvernare.

Integrarea instrumentelor digitale în societatea actuală a generat în cadrul guvernării statale un proces continuu. Instituțiile publice se folosesc la maximum de instrumentele ce li sunt puse la dispoziție, profitând de beneficiile oferite de această transformare. Observăm astfel, cum într-o lume în care timpul și resursele reprezintă unele dintre cele mai importante valori, adaptarea tehnologiilor digitale permite guvernării să optimizeze procedurile și să eficientizeze serviciile destinate cetățenilor, digitalizarea devenind esențială în reconfigurarea proceselor administrative. Pe de altă parte, digitalizarea oferă oportunități semnificative de a consolida transparența, punând la dispoziția cetățenilor informații mai accesibile și facilitând monitorizarea activităților guvernamentale, transparența guvernamentală fiind un principiu fundamental al unei democrații sănătoase.

Capitolul următor se concentrează pe eficiența și transparența conferite de digitalizare, în cadrul guvernării statale, urmărind rapoartele care reies din acestea și evidențiind atât relația dintre eficiență și digitalizare în procesele administrative, cât și cea dintre transparența guvernamentală și cetățeni.

2.1. Relația dintre digitalizare și eficiență în cadrul proceselor administrative

Realizarea unei guvernări eficiente implică, nu doar formularea clară a obiectivelor pe care sectorul public dorește să le atingă, ci și evaluarea continuă a modului în care serviciile electronice furnizate de guvern contribuie la realizarea acestor obiective. Această evaluare se bazează pe analiza indicatorilor specifici, care pot include eficiența, accesibilitatea, calitatea și

gradul de satisfacție al cetățenilor. Astfel, identificarea discrepanțelor între obiectivele propuse și rezultatele obținute, poate furniza informații valoroase pentru îmbunătățirea continuă a serviciilor guvernamentale și optimizarea proceselor administrative [21].

În cadrul proceselor administrative din instituțiile publice din România, apariția digitalizării a generat o multitudine de factori care au condus spre dezvoltarea eficienței în rândul acestor procese. Un principal factor care susține menținerea eficienței în funcționarea proceselor instituțiilor publice este automatizarea. Aceasta aduce numeroase beneficii și îmbunătățiri, influențând modul în care instituțiile guvernamentale funcționează și interacționează cu publicul.

Un aspect relevant în procesul de automatizare, care clădește calitatea guvernării statale este cel legat de sarcinile repetitive. Procesele administrative care necesită introducerea repetitivă a datelor sau generarea de rapoarte pot fi automatizate cu sisteme software specializate. Un bun exemplu este sistemul software „SAGA", unul dintre cele mai cunoscute și utilizate programe de contabilitate din România. Acest program este folosit de numeroare companii și de numeroși funcționari publici pentru efectuarea gestiunii financiare, oferind o gestionare eficientă a contabilitității și a altor aspecte de natură fiscală. În rândul instituțiilor publice, este folistă o versiune specială al acestui soft, numit „ SAGA B", care spre deosebire de versiunea amintită anterior, acestă versiune este creată special pentru evidența contabilă și fiscală destinate instituțiilor bugerare. Prin acest software, procesele administrative beneficiază de automatizare, reducând timpul necesar pentru administrarea datelor și a tranzacțiilor. Calculul automat generat de sistem și verificarea datelor asigură o precizie mai mare în rapoartele financiare și fiscale, având o interfață intuitivă ce facilitează utilizarea și întelegerea de către utilizator. De asemenea, accesibilitatea online reprezintă un beneficiu prin care se permite accesul la distanță la informații. Programul se actualizează constant pentru a respecta cerințele legale în materie de contabilitate, fiind în conformitate cu legislația fiscală actuală. „SAGA" este eficient datorită multitudinii de funcționalități pe care le oferă, fiind o ustensilă perfectă pentru transmiterea documentelor sau a statelor de salarii direct către client sau firma parteneră. Există posibilitatea de a genera documentele și de a le trimite direct din aplicație către mailul acestora, fie la comun, fie invidual (pentru fiecare angajat în parte), fiind conform cu normele impuse de „GDPR"[10]. În același timp, sistemul gestionează eficient stocurile și facturile, sporind eficiența. Datorită noilor proiecte în vigoare, programul poate să importe documentele de tip "e-factură", fără ca utilizatorul să mai trebuiască să introducă datele manual, fiind mult mai precis și rapid. Astfel, programul reprezintă un avantaj semnificativ în rândul instituțiilor publice și a întreprinderilor, dat fiind faptul că „e-factura" a devenit obligatorie de la 1 ianuarie 2024 [22]. Ca urmare, un program dezvoltat în România, eficientizează substanțial întreg procesul administrativ, atât la nivelul instituțiilor publice, cât și în rândul cetățenilor, având notorietate de-a lungul istoriei, ușurință în utilizare, adaptabilitate (în funcție de volumul și capacitatea întreprinderii sau a instituției), suport tehnic și comunitate mare de utilizatori ce folosesc forumuri ale „SAGA"-ului, precum și costurile accesibile, fiind o opțiune atractivă pentru cei ce vor sa își gestioneze eficient cheltuielile și stocurile.

Astfel de aplicații precum „SAGA", au sprijinit instituțiile publice, în schimbul achiziției unei licențe lunare de folosire a programului, oferindu-le surse autentice, documente electronice și identificare electronică (eID), facilitând comunicarea între instituții, cât și cu clienții prin poșta digitală, direct din aplicație, fără a mai fi necesar mailul. Observăm astfel, cum între anii 2017 și 2018 se înregistrează o creștere a tuturor factorilor menționați la nivelul sectorului public [23].

[10] acronim pentru „General Data Protection Regulation", fiind un regulament european care reglementează protecția datelor cu caracter personal

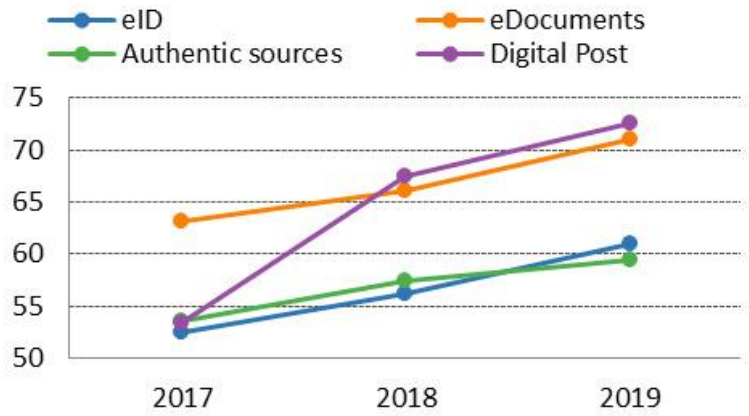


Fig. 1. Factori cheie ai progresului instituțiilor publice prin digitalizare
Sursa: eGovernment Benchmark Capgemini.

Un alt aspect cheie al automatizării în procesul de garantare a eficienței, este acela de reducere a erorilor umane. Utilizarea unor sisteme automate va elimina riscul de erori cauzate de introducerile manuale a datelor, crescând eficiența si reducând semnificativ timpul. De asemenea, documentele vor si gestionate mai eficient prin sistemele automatizate, permițând accesul rapid la orice informație, eliminând ineficiența cauzată de timpul necesar pentru căutarea și distribuirea unui document. Automatizarea prin digitalizare ajută la menținerea conformității cu reglementările și standardele legale, prin implementarea unor procese și controale standardizate. Sistemele digitale pot genera rapoarte și evidențe care demonstrează respectarea cerințelor legislative și a standardelor de securitate și de protecție a datelor.

Tocmai de aceea, numărul de utilizatori al e-guvernării este în continuă creștere, înregistrându-se la nivel european, în anul 2013, un procentaj de 41% din toalitatea utilizatorilor de internet care trebuie să trimită formulare electronice completate către autoritățile publice. Până în anul 2019 se observă o creștere continuă a apelanților la serviciile digitale guvernamentale (cetățenii), numarul crescând cu 26 de procente, ajungând la un cuantum de 67% [24]. Aceste formulare sunt deja preîntocmite, având câmpuri de completat predefinite, pentru a facilita timpul si acuratețea în vederea redactării de către cetățeni, dar și diminuarea duratei de procesare de către instituțiile publice.

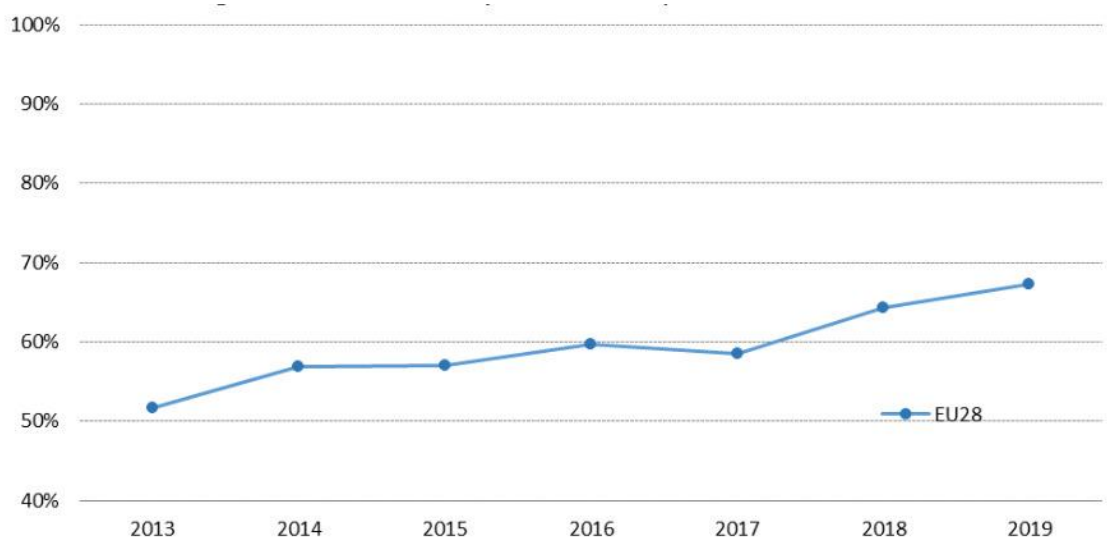


Fig. 2. Raportul utilizatorilor care încarcă documente electronice către instituțiile publice
Sursa: Eurostat, Community survey on ICT usage in Households and by individuals.

Nu în ultimul rând, amintim de eficiența costurilor. Chiar daca nu reducem numărul de angajați, în vederea diminuării costurilor, diminuăm semnificativ volumul de muncă al acestora. Astfel, se crează un flux de lucru optimizat care codnuce la o utilizare mai eficientă a resurselor și la o productivitate mai mare în rândul funcționarilor. Totodată, transpunerea documentelor în format electronic și eliminarea arhivării fizice a acestora, va diminua costurile și va conduce la o accesare mai rapidă și mai eficientă.

De asemenea, suntem de părere că prin digitalizare întreg serviciul public beneficiază de o diminuare a costurilor datorită sistemelor online de acces ale acestor servicii. Nu doar că se va reduce timpul alocat cetățenilor și instituțiilor guvernamentale pentru a putea realiza comunicarea, dar se vor reduce și costurile. Practic, oferirea unor platforme online unde se regăsesc informații utile pentru cetățeni, eficientizează întreg procesul prin care instituțiile publice ar trebui să furnizeze informațiile. Cetățenii nu mai trebuie să se deplaseze fizic la instituții pentru a cere informații, economisind timp și cheltuieli alocate deplasării, iar instituțiile evită necesitatea existenței unui ghișeu public de informații. Pe lângă posibilitatea de furnizare a informațiilor prin intermediul platformelor online, acestea pot eficientiza procesul de furnizare, completate si depunere a documentelor din cadrul instituțiilor guvernamentale. Se va reduce astfel birocrația, costurile aferente hârtiei, timpul alocat fie completării cererilor, fie procesării acestora, precum și nevoia de a avea un spațiu necesar îndosarierii acestor cereri. Astfel, digitalizarea facilitează accesul mai ușor și mai rapid la informații și servicii pentru cetățeni și pentru angajații administrației publice, sporind eficiența comunicării între cei doi, dar și între departamentele administrative.

În rândul factorilor care generează o eficiență ridicată în instituțiile guvernamentale, amintim și de serviciile publice personalizate. Aceste servcii permit administrației publice să ofere ajutor adaptat nevoilor și preferințelor individuale ale cetățenilor. Prin intermediul unor astfel de servicii personalizate, fiecare serviciu în parte își va putea guverna activitățile după bunul plac, iar cetățenilor le va fi mult mai ușor sa acceseze serviciul dorit. Spre exemplu, portalurile personalizate pentru taxe și impozite, pot fi accesate de persoanele care doresc să întreprindă activități în acest sens, cu ușurință, datorită divizării informațiilor în funcție de domeniul de activitate. Imaginați-vă un portal în care toate domeniile de activitate ar fi la comun. În faza incipientă poate părea ușor de utilizat, având tot ceea ce avem nevoie într-un singur loc, însă filtrarea informațiilor si rapiditatea accesării unui anumit serviciu, ne-ar pune în dificultate, fiind ineficient din punct de vedere al economicității timpului. Asfel, aceste servicii publice personalizate vin în ajutorul cetățeanului pentru a îi oferi exact ceea ce are nevoie. Prin intermediul serviciilor personalizate, cetățenii își pot gestiona documentele, plățile, programările sau alte tranzacții administrative.

Observăm cum, între anii 2017 și 2019, se înregistrează o creștere a utilizabilității, a disponibilității online, precum și a accesibilității prietenoase prin device-urile mobile în servicile oferite de către instituțiile publice [23]. În decursul celor 3 ani, utilizabilitatea a crescut cu 3 procente, iar disponibilitatea serviciilor publice în online s-a imbunătățit cu 4,2 procente. Sectorul public a devenit mult mai receptiv în ceea ce privește accesibilitatea pe device-urile mobile, permitându-le utilizatorilor să gasească servicii oricând și oriunde. Din 2017, pâna în 2019, s-a înregistrat o creștere a performanței serviciilor prietenoase mobile oferite de către sectorul public de 15,5%.

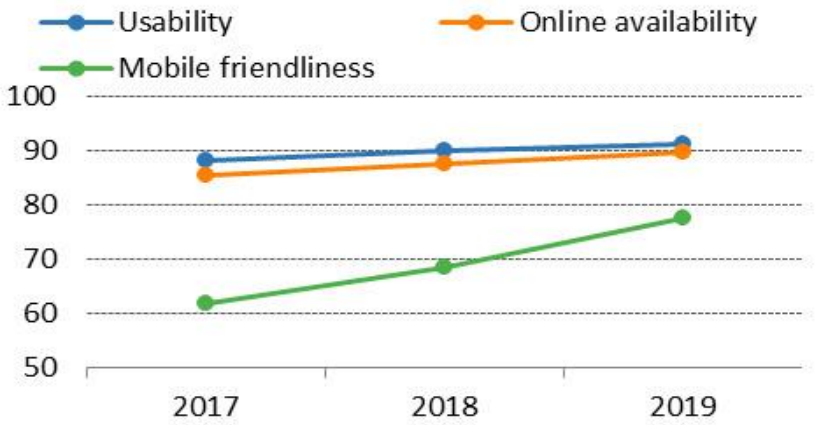


Fig. 3. Defalcare centrată pe utlizator în relație cu sectorul public
Sursa: eGovernment Benchmark Capgemini.

Totodată, digitalizarea permite cetățenilor să completeze și să trimită formulare și cereri online, adaptate în funție de situația lor specifică. Serviciile de asistență virtuală, precum si tehnologiile de tip „chat-bot”[11] de pe site-urile administrației publice pot oferi cetățenilor răspunsuri rapide și personalizate la întrebările și nelămuririle lor. Aceste sisteme pot ghida cetățenii în completatea unui formular, spre exemplu, sau în găsirea unor informații necesare, într-un mod interactiv. Pe lângă asistența virtuală, amintim de alertele și notificările personalizate. Prin intermediul avansului tehnologic actual, cetățenii pot beneficia de alerte și notificări personalizate pentru acestia, în legătura cu expirarea unui document, completarea eronată (sau completarea cu succes) a unui formular și altele. Aceste notificări pot fi trimise atât prin e-mail, sms sau prin aplicații mobile, în funcție de preferințele fiecăruia. Aici intervine și analiza datelor pentru recomandări personalizate, prin intermediul carora administrația publică înțelege mai bine nevoile și preferințele cetățenilor. Prin informațiile colectate, aceste servicii pot utiliza și analiza baza de date colectată de la un cetățean, oferind ulterior recomandări personalizate pentru servicii, programe sau beneficii la care cetățenii ar putea fi eligibili, adaptând astfel, inclusiv notificările personalizate și redirecționate către aceștia. Important de menționat este că această colectare a datelor personalizate, are loc numai cu acordul individului, în limita respectării termenilor și condițiilor, cu privire la regulamentul general de colectare, stocare și gestionare a datelor cu caracter personal.

Impactul pozitiv asupra mediului înconjurător reprezintă un aspect de multe ori ignorat al beneficiilor aduse de digitalizare în administrația publică, având consecințe benefice pentru ecosistem și sustenabilitatea planetei. Prin trecerea de la procese bazate pe folosirea hârtiei și a altor materiale fizice, la soluții digitale, se produc schimbări semnificative în reducerea amprentei de carbon, diminuarea consumului de resurse și limitarea deșeurilor. Aceste beneficii nu sunt doar economice și administrative, ci contribuie și la protecția mediului pentru generațiile viitoare [25]. Una dintre cele mai evidente modalități în care digitalizarea protejează mediul este prin reducerea consumului de hârtie. Într-o administrație publică obișnuită, procesele administrative necesită imprimarea și stocarea unui volum enorm de documente. Acestea nu doar implică utilizarea a numeroase resurse naturale, cum ar fi lemnul și apa, pentru producția de hârtie, dar și generează deșeuri însemnate. Digitalizarea elimină această necesitate. Documentele sunt create, transmise și stocate electronic, fără a mai fi nevoie de hârtie. Astfel, cantitatea de deșeuri provenite din hârtie uzată și documente expirate este redusă drastic.

În urma celei de a 11-a conferințe internaționale de Dezvoltare Stiințifică și Dezvoltare Rurală din anul 2023, s-a analizat consumul de hârtie în urma digitalizării a 25 de instituții publice între anii 2018-2021 [26]. Observăm cum tendințele de a consuma hârtia, scad de la an la an,

[11] numit și bot de conversație, este un program de calculator care utilizează inteligența artificială pentru a simula conversații umane într-un mod natural, interacționând cu utilizatorii prin intermediul textului sau vorbirii și oferind răspunsuri, informații sau suport într-un mod automatizat.

reducându-se cu 67,5% în anul 2021, comparativ cu 2018. Totodată, se înregistrează în rândul utilizării de platforme digitale o creștere semnificativă (Fig.1). Deși între anul 2018 si 2019 creșterea este una de doar 3,4%, între anii 2019 și 2020 avem o creștere de 188,4%, iar între 2020 și 2021 se înregistrează o creștere de 101,6%. Observăm o creștere de la an la an și a echipamentelor de printat, cea mai mare scădere fiind în proporție de 71,1%, intre anii 2020-2021 (Anexa 1).

Indicator / year	2018	2019	2020	2021
paper sheets, number	3 111 500	2 857 500	2 456 000	1 010 000
price of 1 box [1], EUR	14,08	14,18	13,88	14,15
total paper, EUR	17 247,35	16 011,38	13 433,67	5 689,65
printing equipment, EUR	18 476	8 960	8 660	7 162
digital equipment, EUR	179 186	150 315	118 270	202 345
digital platforms, EUR	12 694	13 126	37 862	76 337
number of pupils	10 463	11 297	11 555	11 444
paper, EUR per pupil	1,65	1,42	1,16	0,50
paper, sheets per pupil	297	253	213	88
digital platforms, EUR per pupil	1,21	1,16	3,28	6,67
number of employees	1 671	1 704	1 773	1 795
paper, EUR per employee	10,32	9,40	7,58	3,17
paper, sheets per employee	1 862	1 677	1 385	563

Fig. 4. Comparația consumului de hârtie, a numărului de angajați și a numărului de accesări de platforme digitale în cadrul instituțiilor publice între anii 2018-2021
Sursa: Proceedings of the 11th International Scientific Conference Rural Development 2023 - The Use Of Paper In The Era Of Digitalization.

Digitalizarea în administrația publică nu se limitează doar la eliminarea hârtiei, ci include și trecerea la soluții energetice mai durabile și mai eficiente. Serverele și infrastructura IT necesare pentru stocarea și procesarea datelor sunt optimizate pentru a folosi mai puțină energie și a reduce emisiile de carbon. Aceasta înseamnă că procesele administrative digitale nu doar reduc consumul de energie, ci și contribuie la creșterea cererii pentru surse de energie mai curate, precum energia solară sau eoliană.

Digitalizarea în administrația publică deschide, de asemenea, uși pentru inovație și soluții smart care să contribuie la protejarea mediului înconjurător. Prin utilizarea tehnologiilor precum Internet of Things (IoT)[12] și Big Data[13], administrațiile pot monitoriza și gestiona mai eficient resursele, cum ar fi apa și energia. De exemplu, sistemele de management al deșeurilor pot folosi senzori IoT pentru a colecta și analiza date despre cantitatea deșeurilor generate și nivelurile de reciclare [27]. Acest lucru permite administrației să ia decizii mai bine informate și să implementeze strategii pentru reducerea deșeurilor și creșterea ratei de reciclare.

Drept urmare, digitalizarea în administrația publică reprezintă o necesitate către o guvernare eficientă, optimizând procesele administrative și oferind servicii publice accesibile pentru cetățeni. Această transformare aduce beneficii considerabile, cum ar fi reducerea timpului și costurilor, eliminarea erorilor umane, eficientizarea resurselor și creșterea transparenței în activitatea guvernamentală. Automatizarea și utilizarea unor sisteme specializate amplifică eficientizarea proceselor administrative, iar reducerea sarcinilor repetitive, gestionarea eficientă a datelor și generarea automată a rapoartelor contribuie la îmbunătățirea calității serviciilor oferite și la optimizarea utilizării resurselor. Eficiența costurilor este un alt beneficiu major al

[12] reprezintă rețeaua de obiecte fizice („lucruri") care conțin softuri și alte tehnologii, în scopul conectării și schimbului de date cu alte dispozitive și sisteme de pe internet.
[13] se referă la volumul mare de date structurate și / sau nestructurate care sunt generate, colectate și prelucrate continuu.

digitalizării, prin reducerea volumului de muncă necesar și eliminarea arhivării fizice a documentelor. Aceasta conduce la o administrare mai rapidă și mai eficientă, cu o economie semnificativă de timp și resurse. De asemenea, serviciile publice personalizate și noile tehnologii, cum ar fi asistența virtuală și notificările personalizate, îmbunătățesc experiența cetățenilor în interacțiunea cu instituțiile publice. Accesul simplificat la informații și servicii online contribuie la reducerea birocrației și a cheltuielilor asociate cu deplasările la ghișeele publice. În plus, digitalizarea în administrația publică are un impact pozitiv asupra mediului înconjurător, prin reducerea consumului de hârtie, optimizarea energiei și implementarea unor soluții smart pentru gestionarea resurselor.

Astfel, adoptarea și promovarea soluțiilor digitale în guvernare sunt esențiale pentru construirea unei societăți moderne, eficiente, și sustenabile. Continuarea investițiilor în tehnologie și evaluarea constantă a impactului digitalizării vor contribui la o administrație publică mai eficientă, mai transparentă, mai responsabilă și mai orientată către nevoile cetățenilor.

2.2. Transparența guvernamentală în relația cu cetățenii

Transparența reprezintă un aspect esențial al guvernării moderne, fiind asociată adesea cu conceptul de responsabilitate democratică și eficiența pieței. Această idee își are rădăcinile în accesul la informații guvernamentale și are implicații semnificative pentru economie, politică și societate. În ultimele decenii, transparența a devenit un punct central al discuțiilor despre buna guvernare, fiind văzută ca un element cheie pentru democratizare și pentru îmbunătățirea performanței economice. Odată cu accentuarea importanței transparenței în guvernare, au avut loc schimbări semnificative în legislația privind accesul la informații la nivel global [28]. Aceste legi vizează facilitarea accesului cetățenilor și a altor părți interesate la documente și informații publice, astfel încât procesele decizionale și activitățile guvernamentale să fie mai transparente și mai ușor de înțeles. Transparența nu numai că promovează o mai mare responsabilitate în guvernare, ci este și un pilon al participării publice și al dialogului democratic. Aceasta poate conduce la o creștere a încrederii cetățenilor în instituțiile guvernamentale, dar relația dintre transparență și încredere este complexă și poate fi influențată de mai mulți factori.

Spre finalul secolului al XX-lea, a fost introdus accesul la documentație, respectiv, posibilitatea pentru una sau mai multe părți cu un interes legal direct, real și actual, de a solicita acces la actele pe care administrațiile publice le-au pus în aplicare. Reglementările urmatoare au facut ca transparența decizională să devină obligatorie în România prin adoptarea și implementarea unor legi specifice, care vizează deschiderea și accesibilitatea procesului decizional către cetățeni și alte părți interesate. Amintim astfel de Legea 544/2001 privind liberul acces la informațiile de interes public. Această lege a fost adoptată în anul 2001 și a reprezentat un pas semnificativ în promovarea transparenței decizionale. Ea a stabilit dreptul cetățenilor de a solicita și de a primi informații de interes public de la instituțiile publice. Legea a definit informațiile de interes public, procedurile de solicitare și de furnizare a acestora, precum și sancțiunile pentru refuzul sau întârzierea nejustificată în furnizarea informațiilor. De asemenea, o importanță deosebită o are Legea 52/2003, privind transparența decizională în administrația publică. Aceasta a fost adoptată în 2003, și a stabilit reguli clare privind transparența în procesul decizional al autorităților publice. Ea a impus publicarea în mod obligatoriu a proiectelor de acte normative și a hotărârilor luate de autorități, precum și organizarea de dezbateri publice înainte de adoptarea acestora. Legea a facilitat accesul cetățenilor la informații despre deciziile guvernamentale și a promovat participarea activă a acestora în procesul decizional. Amintim și de adoptarea strategiilor pentru promovarea transparenței, în care Guvernul României a adoptat diverse planuri de acțiune în vederea promovării transparenței și accesului la informație. Acestea includ Planul Național de Acțiune pentru Transparență Guvernamentală, care stabilește obiective specifice și măsuri pentru îmbunătățirea transparenței în activitatea guvernamentală. Un alt factor al consolidării transparenței în România a fost creșterea presiunii din partea societății civile și a organismelor internaționale prin care societatea civilă și organizațiile non-guvernamentale au avut un rol important în promovarea transparenței decizionale, monitorizând activitatea autorităților publice și solicitând transparență și responsabilitate. De asemenea,

organismele internaționale, precum Uniunea Europeană și Organizația pentru Cooperare și Dezvoltare Economică (OCDE), au încurajat și susținut România în implementarea standardelor internaționale privind transparența guvernamentală.

În prezent, transparența guvernamentală are loc în cea mai mare parte în format digital, presupunând accesul la informațiile publice prin intermediul tehnologiilor digitale. Digitalizarea proceselor guvernamentale a pus în centrul atenției disponibilitatea și accesibilitatea informațiilor publice, care devin tot importante în economia bazată pe cunoștințe. Totuși, este important să se sublinieze că transparența poate implica și gestionarea datelor personale ale cetățenilor, ceea ce ridică probleme legate de confidențialitate. Există un echilibru delicat între transparență și protecția datelor personale, iar guvernele trebuie să găsească modalități adecvate de a menține această balanță.

Instituțiile guvernamentale pun la dispoziție resurse publice, baze de date, proiecte legislative, bugete anuale și alte informații de interes public, pentru a facilita o relație strânsă cu cetățenii. Cu toate acestea, nu avem garanția că aceste informații ajung să fie cunoscute de către public. Tocmai de aceea este important ca administrația publică, nu doar să furnizeze informațiile de natură transparentă, ci să se asigure că acestea pe lângă a fi publicate, sunt și promovate și usor de accesat, pentru a ajunge în ochii și în atenția publicului larg. Obvservăm în urma unui chestionar din Argentina, efectuat de către locuitorii orașului Buenos Aires, opinia acestora vizavi de nivelul de transparență al instituțiilor publice. Aceștia au primit o serie de întrebări, de natură subiectivă, întrebări ce au fost împărțite prin prisma a doi factori. Primul factor a fost legat de transparența guvernamentală din punct de vedere al eficienței, iar cel de al doilea factor prevedea transparența din punct de vedere al empatizării pe care cetățeanul o are. Astfel, acțiunile guvernamentale, în termeni de eficiență sau empatie, ar putea afecta încrederea oferită în guvern [29].

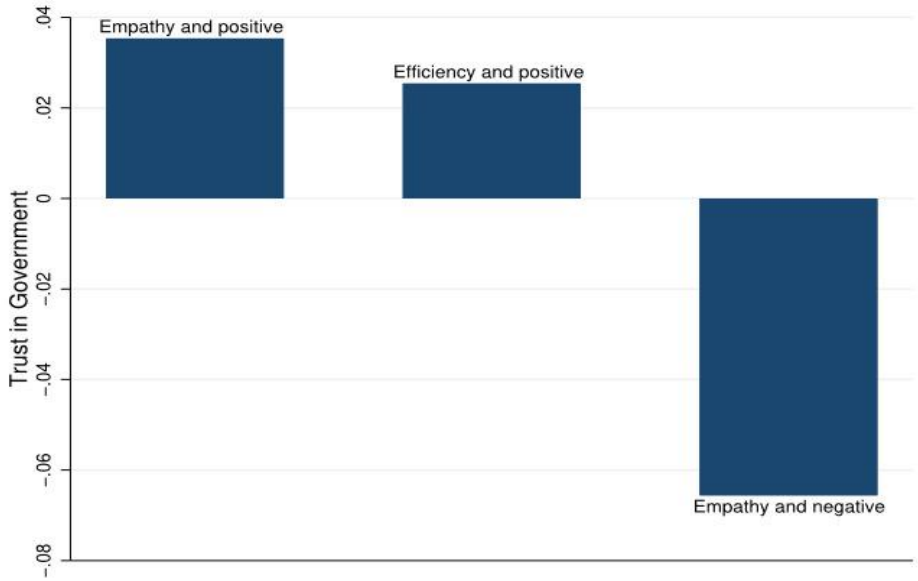


Fig. 5. Încrederea cetățenilor în guvern prin empatie sau eficiță
Sursa: Word Development, Transparency and Trust in Government. Evidence from a Survey Experiment

În urma chestionarului, observăm cum din punct de vedere al factorului eficienței, obținem valori pozitive, întrucât toți participanții consideră transparența guvernamentală importantă. În ceea ce privește chestionarea legată de empatizarea serviciilor transparente puse la dispoziția cetățenilor de către guvern, aproximativ 40% dintre participanți au privit pozitiv transparența guvernului, având încredere în acesta, restul de 60% fiind în opoziție și considerând că nu au suficientă încredere în guvern datorită transparenței oferite. Partea majoritară care consideră că transparența guvernamentală nu este suficient de bine optimizată își arguementează opinia, atragând atenția serviciilor publice. Aceștia menționează că multe dintre site-urile ce își propun

să furnizeze date transparente, de multe ori nu sunt promovate și nu ies la suprafață, astfel cetățenii nu iau cunostință de existența acestora. Un alt factor este aspectul site-urilor, care în unele cazuri, nu se situează la standarde înalte de performanță și nu îndeplinesc măsurile necesare de securitate, pot crea suspiciuni, denaturând încrederea oferită de utilizatori.

Pentru a facilita realizarea unui proces transparent între administrația publică și cetățeni, România a dezvoltat numeroase proiecte cu scopul de a implementa transparența guvernamentală prin intermediul digitalizării. Amintim astfel, de portalul de date deschise al Guvernului României, „data.gov.ro". Acest portal online reprezintă o inițiativă întrăzneață în ceea ce privește promovarea transparenței guvernamentale prin digitalizare în România. Scopul principal al acestui portal este acela de a facilita accesul cetățenilor, mediului academic, organizațiilor non-guvernamentale și sectorului privat la diverse seturi de date deschise, într-o manieră ușor accesibilă. Aceste date deschise reprezintă seturi de informații furnizate de instituțiile publice, care sunt disponibile gratuit și accesibile publicului în format digital, într-un mod liber, putând fi reutilizate si redistribuite de către oricine [30]. Acestea includ informații variate, precum bugetul de stat, cheltuielile publice, statistici economice și sociale, informații despre instituțiile publice, infrastructură, mediu, educație, sănătate, transport și multe altele. Prin intermediul platformei data.gov.ro, utilizatorii pot explora o gamă largă de date deschise, utilizând instrumente de căutare și filtrare pentru a găsi exact informațiile de care au nevoie. Acest lucru permite cercetătorilor să analizeze tendințe, să dezvolte aplicații și instrumente utile, și să realizeze studii pentru a înțelege mai bine contextul social și economic al țării. De exemplu, un cercetător poate accesa seturi de date privind bugetul de stat pentru a analiza alocările financiare către diferite domenii și programe. Un jurnalist poate utiliza datele pentru a investiga cheltuielile publice și pentru a monitoriza modul în care sunt utilizate fondurile publice. Un antreprenor sau dezvoltator de aplicații poate folosi datele pentru a crea instrumente utile pentru cetățeni, cum ar fi aplicații de monitorizare a transportului public sau hărți interactiv. Prin acest portal, guvernul român demonstrează angajamentul său față de transparența și deschiderea în administrație, oferind cetățenilor posibilitatea de a fi informați și implicați în procesele decizionale. De asemenea, „data.gov.ro" promovează o mai mare responsabilitate și eficiență în utilizarea resurselor publice, deoarece informațiile sunt disponibile pentru monitorizare și evaluare publică.

O altă strategie guvernamentală a carei principal scop este transparența față de cetățeni se face simțită prin intermediul platformelor de social media sau alte platforme în care cetățeanul poate oferi „feedback"[14] direct. Guvernele pot folosi platformele de social media pentru a comunica direct cu cetățenii. Acestea pot publica informații despre decizii, politici și programe, oferind cetățenilor acces rapid și ușor la informații de interes public. De asemenea, cetățenii pot pune întrebări, face comentarii și obține răspunsuri direct de la autorități. Platformele de social media oferă cetățenilor posibilitatea de a raporta diverse probleme și de a face sugestii cu privire la serviciile guvernamentale. Acestea pot fi utilizate pentru a semnala probleme în infrastructură, în mediu, în serviciile publice etc. Autoritățile pot monitoriza aceste rapoarte și să acționeze în combaterea problemelor. Instituțiile publice pot folosi platformele de social media pentru a organiza consultări publice și dezbateri online. Acest lucru permite cetățenilor să-și exprime opiniile și să participe la procesul decizional în mod direct, chiar și de la distanță. De exemplu, pot fi organizate sondaje de opinie online sau discuții tematice pe diverse aspecte ale politicilor publice. Tot prin intermediul platformelor menționate anterior se poate dispune de publicarea informațiilor despre cheltuielile guvernamentale și bugetele publice, unde cetățenii pot urmări mai bine modul în care sunt folosiți banii publici. Acest lucru contribuie la o mai mare transparență în activitatea guvernamentală și la o mai mare responsabilitate față de cetățeni.

Un exemplu concret, este reprezentat prin grupurile de „Facebook" ale locatarilor unui anumit sector din București sau chiar site-ul oficial al primăriei de sector. Vom folosi ca și scenariu site-ul primăriei Sectorului 6. Așa cum am observat în studiul de caz efectuat de cetățenii

[14] conform dicționarului „Oxford Languages", semnifică o sugestie, critică sau informație despre cât de bun sau util este ceva sau munca cuiva

orașului Buenos Aires, un factor esențial an transpareței are loc încă dinaintea accesării propriu-zise a site-ului, constând în ușurința prin care acesta este găsit. Adresa site-ului este una ușor de reținut și de găsit „primarie6.ro", fiind întotdeauna primul site găsit de motoarele de cautare atunci când precizăm „sector 6". Site-ul este bine structurat, ușor de accesat, având chiar și un meniu de accesibilitate destinat persoanelor care au deficiențe de vedere, în acest fel informațiile pot fi accesate de către orice utilizator. De asemenea, o transparență eficientă, nu trebuie să fie îngrădită de factori care limitează accesul prin crearea unui cont, acestea denaturând accesul fără bariere. Întâlnim totodată pe site-ul Primăriei Sectorului 6, informații de interes public, precum si o secțiune destinată contactului, care conține informațiile de contact și adresa primăriei, precum și posibilitatea de a apela la o cerere de audie. Cu toate acestea, cea mai importantă ramificație a acestei secțiuni destinate contactului, dupa părerea noastră, este cea prin care se pot face sesizări, petiții sau reclamații online. Amintim pe această cale și de aplicația mobilă „eSector6", aplicație creată de Primăria Sectorului 6, o aplicație de servicii publice unde se regasăsesc și se pun la dispoziție sesizări, plăți, știri locale, se pot întreprinde diverse acțiuni cu privire la salubrizare, reciclare și parcări, având o multitudine de informații utile care consolidează transparența vizavi de cetățenii Sectorului 6. . Am analizat numărul de descărcări, precum si reviewurile utilizatorilor, peste 70% din utilizatori (având peste 10 mii de descărcări) fiind de părere ca aplicația reprezintă cel mai simplu și eficient mod de a face sesizări și plați, catalogând-o drept „simplă și eficientă". În urma analizei activității grupului public de „Facebook" a aceleiași primării, numit „Pentru Sectorul 6", un grup cu peste 30 de mii de membri activi, administrat în prezent de actualul primar al Sectorului 6, observăm transparența activă a acestei instituții și „feedback"-ul pozitiv din partea cetățenilor de sector. Un exemplu concret îl reprezintă propunerea unui membru al grupului, locatar al Sectorului 6, de a accesibiliza intersecțiile și trotoarele pietonale ale sectorului, pentru facilitarea accesului în rândul personelor cu dizabilități, cât și pentru cărucioare. Postarea a acumulat un număr semnificativ de aprecieri și susțineri, urmând ca după o vizita a primarului la „Smart City Expo World Congress" în care s-au adus propuneri de proiecte asemenătoare, ce au avut loc in Barcelona, la mai puțin de un an de la respectiva postare, toate intersecțiile și bulevardele principale ale Sectorului 6 benficiază în prezent de infrastructura menționată anterior.

Un alt proiect care consolidează transparența guvernamentală în România este Sistemul Electronic de Achiziții Publice (SEAP). Considerăm că „SEAP" este una dintre cele mai transparente platforme datorită îndeplinirii urmatoarelor condiții:
a) Accesibilitate: „SEAP" permite accesul facil și gratuit pentru oricine, inclusiv pentru firmele care doresc să participe la licitații publice. Prin intermediul „SEAP", orice persoană sau firmă poate urmări licitațiile deschise, termenele limită, caietul de sarcini și alte informații relevante.
b) Informații Deschise: Toate procedurile de achiziție publică sunt publicate pe „SEAP", oferind transparență cu privire la cheltuielile și deciziile guvernamentale în ceea ce privește achizițiile de bunuri, servicii sau lucrări. Acest lucru îmbunătățește transparența și reduce posibilitatea corupției sau a favoritismului în procesul de achiziție.
c) Monitorizarea și Raportarea: Prin „SEAP", autoritățile publice au posibilitatea de a monitoriza și raporta mai eficient activitățile legate de achizițiile publice. Acest lucru oferă un instrument puternic pentru guvernanță în utilizarea fondurilor publice.
d) Stimularea Competiției și a Inovației: Prin publicarea transparentă a achizițiilor publice, „SEAP" stimulează competiția între furnizorii de bunuri și servicii. Acest lucru poate duce la oferte mai bune, prețuri mai competitive și inovații în domenii precum tehnologia, infrastructura și serviciile publice.
e) Conformitate cu Standardele Europene: „SEAP" este o parte integrantă a eforturilor României de a se conforma standardelor și regulamentelor europene în ceea ce privește achizițiile publice. Acest lucru sporește credibilitatea și accesul la finanțare europeană, contribuind la dezvoltarea economică și socială a țării.

Cu toate acestea, fără o bază legală nimic din cele menționate anterior nu ar fi respectate în totalitate. Tocmai de aceea Sistemul Electronic de Achiziții Publice se află sub temeiul legal al Legii 98/2016 , privind achizițiile publice, cu modificările și completările ulterioare. Potrivit acestei legi, utilizarea „SEAP" este obligatorie pentru toate autoritățile contractante, indiferent

de nivelul de guvernare sau de tipul de achiziție (achiziții de bunuri, servicii sau lucrări). Autoritățile contractante sunt obligate să publice toate procedurile de achiziție publică pe „SEAP", iar comunicarea cu ofertanții și întocmirea documentației se realizează prin intermediul acestui sistem electronic. De asemenea amintim de Legea 99/2016 privind achizițiile sectoriale, Legea 100/2016 privind concesiunile de lucrări și concesiunile de servicii, Legea 101/2016 privind remediile și căile de atac în materie de atribuire a contractelor de achiziție publică, a contractelor sectoriale și a contractelor de concesiune de lucrări și concesiune de servicii, precum și pentru organizarea și funcționarea Consiliului Național de Solutionare a Contestațiilor, HG 394/2016 pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului sectorial/acordului-cadru din Legea nr. 99/2016 privind achizițiile sectoriale, hotărârea de Guvern HG 395/2016 pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziție publică/acordului-cadru din Legea nr. 98/2016 privind achizițiile publice, ordonanța de urgență OUG 114/2011 privind atribuirea anumitor contracte de achiziții publice în domeniile apărării și securității și hotărârea de Guvern HG 89/2020 privind organizarea și funcționarea Autorității pentru Digitalizarea României, toate acestea facând parte din legislație națională și conținând prevederi în vederea desfășurării activității „SEAP". Pe această cale amintim și de prevederile impuse de legislația europeană având Directiva 2014/23/UE a Parlamentului European și a Consiliului/2014 privind atribuirea contractelor de concesiune, Directiva 2014/24/UE a Parlamentului European și a Consiliului/2014 privind achizițiile publice, Directiva 2014/25/UE a Parlamentului European și a Consiliului/2014 privind achizițiile efectuate de entitățile care își desfășoară activitatea în sectoarele apei, energiei, transporturilor și serviciilor poștale și regulamentul de punere în aplicare (UE) 2019/1780 al Comisiei din 23 septembrie 2019 de stabilire a formularelor standard pentru publicarea anunțurilor în domeniul achizițiilor publice și de abrogare a Regulamentului de punere în aplicare (UE) 2015/1986 („formulare electronice") [31]. Prin toate aceste măsuri se impune folosirea unui instrument de natură să prevină corupția și să sporească transparența guvernamentală, facilitând accesul tuturor persoanelor interesate, fie în scop informațional, fie în scop participativ, la acțiunile ce iau loc. În cazul în care prevederile nu sunt conforme, există sancțiuni severe de natură penală, iar în ceea privește procesul de achiziții publice, nerespectarea obligației de utilizare a platformei „SEAP", atrage după sine anularea procedurii de achiziție sau chiar suspendarea dreptului de participare la procedurile următoare.

Astfel, transparența în sectorul public, în contextul digitalizării, reprezintă un aspect vital al guvernării moderne. Aceasta nu numai că promovează responsabilitatea și încrederea în guvern, dar facilitează și participarea cetățenilor în procesul decizional și contribuie la o mai bună înțelegere a activităților și politicilor guvernamentale.

Capitolul 3. Garanții și riscuri în procesul de adaptare la noile realități digitale a instituțiilor de nivel central

Odată cu valul adus de tehnolgie și de noile tendințe digitale ce au loc în cadrul instituțiilor publice, cât și în rândul cetățenilor, numeroase atacuri cibernetice, de natură să fure, modifice sau să distrugă date prețioase, își fac apariția în mod constant, fiind din ce în ce mai puternice. Tocmai de aceea întreaga „gardă", în măsură să protejeze și să asigure securitatea datelor invizilor societății, împotriva atacurilor, sunt însăși instituțiile guvernamentale.

Un aspect negativ al dezvoltării rapide a tehnologiei îl constituie dependența de utilizare a proceselor digitale. Ne situăm astfel într-o societate în care oricine poate avea acces la un dispozitiv sau alte tehnologii ale informației sau mijloace prin care să producă prejudicii întregului sistem guvernamental. Numeroase instituții publice gestionează informații ce au la bază o multitudine de date, fie ele publice ori confidențiale. Aceste date pot prezenta un interes puternic pentru competitori, oferind interese financiare, politice, sau alte asemenea. În opoziție cu protectorii datelor, se află entități considerate actualmente „hackeri", reprezentați prin indivizi sau grupări care încearcă să obțină în mod fraudulos informații ale unui dispozitiv electronic sau ale unei rețele, prin controlul unui sistem de securitate, cu scopul de a avea acces

la informații confidențiale sau avantaje materiale, într-un mod ilegal [32]. Aceștia se folosesc de diverse programe „malware”[15], încercând să denatureze buna funcționare a serviciilor electronice folosite de instituțiile guvernamentale cu scopul de a colecta date și de a crea avantaje sau beneficii proprii, generate în urma amenințărilor cibernetice.

Tocmai de aceea, este extrem de importantă pregătirea personalului din instituțiile publice, pentru a avea cunoștințe ample în vederea combaterii riscurilor generate de digitalizare, dar și prin punerea la dispoziție de către guvern a resurselor digitale necesare pentru a opri eventualele atacuri. După ce se crează întreg sistemul ramificat de garantare împotriva riscurilor noilor realități digitale, trebuie prioritizată actualizarea constantă a metodelor și sistemelor de apărare cibernetice, datorită dezvoltării continue a tehnologiilor. Această dezvoltare ireversibilă este singurul stimulent garant ce poate face față viitoarelor confruntări, datorită apariției rapide și continue de noi tehnologii mai performante decât cele precedente. Ia astfel naștere o luptă continuă a celor două părți, în care cea care posedă cele mai perfomante strategii, precum și cele mai performante tehnologii digitale (fie ele de atac sau de apărare), va învinge. Prin urmare, eventualele riscuri datorate câștigului atacatorilor cibernetici pot crea daune la nivel de stat catastrofale, ce pot denatura întreaga funcționare instituțională.

În cadrul acestui capitol, vom afla care este responsiblitatea instuțiilor guvernamentale în securitatea datelor și în ce măsura se implică acestea când vine vorba de securitatea digitală, care sunt măsurile de securitate luate, dar și care sunt amenințările cibernetice îndreptate către instituțiile guvernamentale, precum și noțiuni cu privire la ce reglementări există în legislația din România privind digitalizarea în administrația publică.

3.1. Responsabilitatea instituțiilor în protejarea și securitatea datelor

Responsabilitatea instituțiilor în protejarea și securitatea datelor poartă o deosebită importanță în era digitală actuală, având în vedere volumul semnificativ de date sensibile cu caracter personal care sunt colectate, stocate și procesate de către organizații. Aceste date pot fi folosite în alte scopuri de către entitățile adverse, astfel că instituțiile guvernamentale trebuie să garanteze protejarea și securitatea unor astfel de date.

Pentru început, sectorul public ar trebui să își însușească o legislație bine pusă la punct care să conțină reglementări și sancțiuni cu privire la protecția datelor. În cazul țărilor membre ale Uniunii Europene există deja numeroase regulamente cu privire la „GDPR”. Aceste prevederi urmăresc pregătirea statelor membre pentru era digitală, în contextul în care peste 90% din europeni își arată dorința de a avea drepturi egale de protecție a datelor peste tot in UE, indiferent de locul în care sunt prelucrate datele [33]. Astfel de regulamente consolidează drepturile fundamentale ale cetățenilor, dint punct de vedere al prevederilor digitale, clarificând totodată normele din piața unică digitală, având beneficii atât pentru întreprinderi, cât și pentru instituțiile publice. Prin reglementări clare, va înceta existența fragmentării diferitelor sisteme naționale și se vor elimina sarcinile administrative redundante, sporind transparența la nivel guvernamental și clădind încrederea cetățenilor.

Un alt aspect important în ceea ce privește responsabilitatea instituțiilor publice de garantare a securității cibernetice îl constituie definirea responsabilităților și a rolurilor. Instituțiile trebuie să definească clar responsabilitățile și rolurile în ceea ce privește protecția datelor. Este nevoie de o echipă de încredere, cu oameni calificați, care sa fie testați atât psihologic, cât și din punct de vedere al cunoștințelor și abilităților de gestionare a datelor cu caracter sensibil, diminuând pe cât de mult posibil riscul de divulgare al unor astfel de informații. De asemenea, ar trebui numit un responsabil desemnat în fiecare instituție care să supravegheze respectarea prevederilor și îndatoririlor fiecărui angajat, precum și asigurarea funcționarii activităților în conformitate cu legislația în vigoare. În România, protecția datelor este reglementată de Legea

[15] reprezintă un soft rău intenționat care afectează și accesează neautorizat un dispozitiv sau o rețea și duce la compromiterea datelor sau blocarea accesului pe dispozitiv

nr. 190/2018 privind măsurile de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, cunoscută sub numele de Regulamentul General privind Protecția Datelor (GDPR). Conform „GDPR", fiecare organizație care prelucrează date cu caracter personal are obligația de a desemna un Responsabil cu Protecția Datelor numit „DPO" (Data Protection Officer), acesta fiind „Responsabilul pentru Protecția Datelor". Acest responsabil cu protecția datelor are rolul de a supraveghea respectarea regulamentelor privind protecția datelor și de a răspunde de aceste aspecte în cadrul organizației. Astfel, în organizațiile care prelucrează date cu caracter personal în România, „Responsabilul pentru Protecția Datelor" este persoana desemnată care se asigură că prelucrarea datelor personale se desfășoară în conformitate cu cerințele legale, inclusiv „GDPR". Acesta poate fi o persoană fizică sau o companie specializată în servicii de protecție a datelor. Astfel de obligații se aplică atât autorităților publice, cât și întreprinderilor private care prelucrează date cu caracter personal.

De asemenea, informarea și consințământul persoanelor afectate reprezintă un aspect cheie în ceea ce privește responsabilitatea instituțiilor publice în protejarea și securitatea datelor. Instituțiile trebuie să informeze persoanele a căror date sunt colectate cu privire la modul în care informațiile lor vor fi utilizate, stocate și protejate. Instituțiile au obligația de a informa persoanele ale căror date sunt colectate cu privire la anumite aspecte esențiale legate de prelucrarea datelor lor. Această informare trebuie să fie clară, concisă și ușor accesibilă pentru persoanele vizate. De obicei, această informare include următoarele elemente:

a) Identitatea și detaliile de contact ale controlorului de date (instituția sau organizația care decide scopul și mijloacele de prelucrare a datelor).
b) Scopurile pentru care sunt colectate și prelucrate datele cu caracter personal.
c) Categoriile de date cu caracter personal care sunt colectate.
d) Destinatarii sau categoriile de destinatari cărora li se pot dezvălui datele.
e) Durata pentru care vor fi stocate datele.
f) Drepturile persoanei vizate, cum ar fi dreptul de acces, rectificare, ștergere sau restricționare a prelucrării datelor.
g) Dreptul de a depune o plângere la o autoritate de supraveghere a protecției datelor.

Conform „GDPR", în unele situații, este necesar consimțământul explicit pentru prelucrarea anumitor categorii sensibile de date (denumite date sensibile sau date speciale). Acestea includ informații privind sănătatea, orientarea sexuală, religia sau apartenența la sindicate. Consimțământul explicit trebuie să fie clar pentru aceste categorii de date. Persoanele afectate au dreptul de a-și retrage consimțământul în orice moment, cu efecte viitoare. Instituțiile sunt obligate să informeze clar persoanele cu privire la acest drept și să ofere modalități ușoare pentru retragerea consimțământului. Instituțiile trebuie să gestioneze și să documenteze în mod corespunzător toate consimțămintele obținute de la persoanele afectate. Acestea ar trebui să fie capabile să demonstreze autorității de supraveghere că au obținut consimțământul în conformitate cu cerințele legale.

Un alt aspect important îl conferă evaluarea riscurilor și implementarea măsurilor de securitate. Instituțiile ar trebui să efectueze evaluări periodice ale riscurilor pentru a identifica potențialele amenințări la adresa securității datelor și a confidențialității. Pe baza acestor evaluări, vor fi implementate măsuri de securitate corespunzătoare pentru a minimiza riscurile. Aceste măsuri pot include criptarea datelor, implementarea unui „firewall"[16] și alte sisteme de detectare a intruziunilor, actualizări regulate de securitate a software-ului și a sistemelor, și alte asemenea. Instituțiile ar trebui să implementeze sisteme de monitorizare a accesului și activității utilizatorilor pentru a urmări și a înregistra cine accesează datele, când și în ce scop. Aceste sisteme ajută la detectarea comportamentelor neobișnuite sau la investigarea activității suspecte.

[16] este un dispozitiv sau soft de securitate în rețea care monitorizează traficul de rețea de intrare și de ieșire și decide dacă să permită sau să blocheze traficul specific pe baza unui set definit de reguli de securitate.

Utilizarea autentificării multi-factor (MFA) este o măsură de securitate puternică pentru a proteja accesul la date. Aceasta necesită, pe lângă parola standard, o altă formă de autentificare, cum ar fi un cod generat dintr-o aplicație, un SMS pe telefonul mobil, amprenta sau scanarea facială a utilizatorului. Totodată, instituțiile ar trebui să definească clar și să limiteze accesul la datele cu caracter personal în funcție de nevoile fiecărui utilizator și de rolul său în organizație. Acest lucru înseamnă că fiecare angajat sau utilizator al sistemului ar trebui să aibă acces limitat la informațiile necesare pentru îndeplinirea sarcinilor sale specifice. De asemenea, instituțiile trebuie să impună politici stricte privind gestionarea parolelor și a conturilor de utilizator. Aceste politici pot include cerințe pentru parole „puternice", expirarea și necesitatea de schimbare periodică a acestora, interzicerea partajării de parole, autentificarea în doi pași, etc. În cazul în care un utilizator nu mai are nevoie de acces sau nu mai lucrează pentru respectiva instituție, accesul acestuia la date ar trebui revocat cât mai repede cu putință, tocmai de aceea este nevoie de revizuiri periodice ale privilegiilor de acces în rândul instituțiilor publice.

Nu în ultimul rând, instruirea și formarea personalului ar trebui prioritizată în rândul sarcinilor efectuate de către sectorul public în vederea protejării și securității datelor. Candidații desemnați să concureze pe unul dintre posturile publice în vederea obținerii unei șanse de a lucra cu date cu caracter personal, ar trebui să treacă mai întâi printr-o serie de factori care vor stabili ulterior dacă este sau nu în măsură persoana desemnată pentru un astfel de post. Aici, desigur, ne raportăm la o multitudine de factori cu privire la verificarea competențelor și a experienței în domeniu a candidatului, urmărind aspecte precum dobândirea anterioară a unui certificat în domeniul protecției datelor sau cursuri de formare relevente. De asemenea, ar trebui îndeplinit cu prioritate consințământul candidatului de a garanta securitatea informațiilor, precum și nedivulgarea acestora sub orice circumstanță, cu excepția prevederile legale în care se cere acest lucru, aducându-i-se la cunostință riscurile asociate cu gestionarea incorectă a informațiilor cu caracter personal, precum și sancțiunile și repercursiunile ulterioare.

Pe lângă datele cu caracter personal, există și alte date care intră în aria responsabilității anumitor instituții publice de a fi protejate și securizate. Există date precum cele de natura informațiilor clasificate guvernamentale. Aceste date, odată ajunse publice pot crea dezastre catastrofale de natura unui război. Tocmai de aceea sunt date cu caracter secret, care trebuie protejate, securizate și criptate într-un mod eficient, având acces limitat și strict doar persoanele desemnate, iar baza de date fizică unde sunt păstrare aceste informații este păzită și securizată pentru a putea garanta protecția datelor clasificate, măsurile specifice regăsindu-se în Hotărârea de Guvern nr. 585/2002 [34], actualizată la 24 martie 2005, privind aprobarea Standardelor naționale de protecție a informațiilor clasificate în România.

3.2. Măsuri de securitate și amenințări cibernetice

Datorită noilor metode și tehnologii actuale care permit atacatorilor cibernetici să se folosească de acestea în scopul obținerii de date, într-un mod fraudulos, a generat factori de natură să împiedice implementarea unui guvern electronic. Astfel, principala preocupare legată de securitate, atât a cetățenilor, cât și a administrației publice este aceea de a implementa măsuri de securitate împotriva atacurilor cibernetice.

Înainte de a stabili care sunt aceste măsuri de securitate luate de guvern în vederea securizării datelor, este important de știut care sunt amenințările cibernetice la care suntem supuși. Până în prezent, conform raportului „Categorii de amințări 2022" al Agenției Uniunii Europene pentru Securitate Cibernetica (ENISA) [35], s-au identificat opt tipuri de amenințări principale (Anexa 2).

Prima amenințare cibernetică este cea de tipul „ransomware" (Anexa 4). Acest tip de amenințare este probabil una dintre cele frauduloase metode prin care atacatorii criptează datele respectivei organizații, urmând să ceară o răscumpărare, de cele mai multe ori sub forma unei remunerații, în vederea decriptării datelor organizației. Entitățile supuse unor astfel de atacuri, riscă fie pierderea datelor cu caracter confidențial, fie publicarea acestora. De aceea, atacatorii profită de

vulnerabilitatea unor astfel de organizații, cerându-le sume considerabile ce pot ajunge la ordinul milioanelor de euro [35], în funcție de importanța datelor și de statutul organizației.

Un ciclu de viață de tipul „ransomware" are în principal cinci etape [36]. Prima etapă reprezintă pătrunderea atacatorului în sistem, datorită vulnerabilității softului folosit de entitatea supusă atacului. După accesul în sistem, urmează etapa executării atacului. Această etapă poate dura de la câteva minute până la săptămâni întregi, în funcție de mărimea fișierelor și a măsurilor de securitate de care dispune „victima". Astfel, atacatorul criptează datele și obține controlul acestora în favoarea sa. Cea de a treia etapă este bazată pe acțiuni și bunuri, fiind numită „acțiune pe obiective". Acțiunile constau în furtul de date, blocarea, criptarea sau ștergerea acestora, iar în ceea ce privește bunurile ne raportăm la foldere, documente, baze de date, etc. Cea de a patra etapă este reprezentată de șantaj. Șantajul are ca mijloc de comunicare de cele mai multe ori șantajul prin email, iar amenințarea are la bază ștergerea fișierelor, redistribuirea datelor și dezvăluirea, fie ea parțială sau totală, a informațiilor. Ca și consecință, atacatorii cer bani, schimbari de soft sau infectarea altor utlizatori. Ultima etapă, presupune negocierea. Aceasta poate avea doua posibile urmări în care cerințele impuse sunt fie îndeplinite, fie respinse de către entitatea supusă atacului. În situația în care nu se acceptă condițiile impuse de atacator, amenințările menționate anterior devin realitate. În situația opusă, în care se respectă cerințele impuse, există două posibile urmări. Una dintre urmări (pe care ne dorim întotdeaună să le întâlnim) înglobează situațiile în care decriptarea are loc cu succes. Cu toate acestea, nu putem avea niciodata garanția că atacatorul va respecta negocierea, chiar daca i se vor îndeplini criteriile. Astfel, în multe situații „victimele" pierd accesul la date și documente, chiar dacă se supun șantajului și se conformează în totalitate, motiv pentru care plata cererii nu este o abordare recomandată deoarece nu se poate garanta a fi eficientă.

În urma studiului efectuat de „ENISA", observăm numărul ridicat de atacaturi de tip „ransonware", focusat în principal pe tările europene, în topul corora se regăsește și România, raportat pe perioada iulie 2021 – iunie 2022 (Anexa 3). Desi în luna iulie a anului 2022, cazurile de „ransonware" au scăzut comparativ cu anul precedent, „ENISA" afirmă că peste jumătate dintre angajații organizațiilor au fost supusi unor astfel de atacuri. Totodată, datele obținute de aceștia sugerează că sumele cerute de atacatori în vederea decriptării datelor au crescut de la an la an. Astfel, în anul 2019 cea mai mare cerere, în umra unui atac „ransonware" a fost de 13 milioane de euro, în 2021 crescând radical, atingând suma de 62 de milioane de euro. Studiul estimează o daună totală la nivel global cauzată de astfel de atacuri, de 18 milioane de euro, înregistrate în anul 2019, fiind de 57 de ori mai mult decât în anul 2015. Totodată, același studiu arată cum între lunile mai 2021 și iunie 2022, raportul comparativ dintre totalul cumulat al numărului de date furate în luna respectivă (reprezentat prin culoarea albastră) și numărul de atacuri de tipul „ransonware" din aceeași lună (reprezentat prin culoarea roșie) (Fig.6).

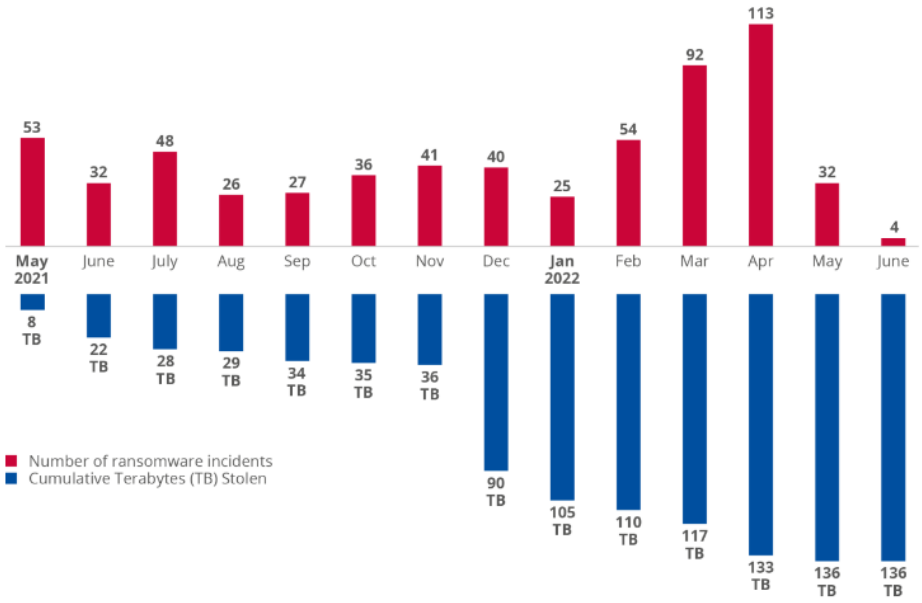


Fig. 6. O serie de incidente „ransomware" raportate între mai 2021 – iunie 2022
Sursa: ENISA - Perspectiva atacaturilor 2022 (iulie 2021 – iulie 2022)

Observăm cum indiferent de numărul de atacuri, care în unele luni este mai mic decât în lunile precedente, cumulul de date furat crește constant de la o lună la alta. Pentru a fi mai specific, în luna mai a anului 2021, 53 de atacuri au condus la un total de 8 TB („terabytes"[17]), iar în luna iunie din 2022, doar 4 atacuri au generat un total de 135 de „terabytes". Raportul arată clar dezvoltarea constantă a atacurilor, precum și slăbiciunea securității organizațiilor, motiv pentru care și sumele în bani cerute de atacatori menționate anterior, au crescut.

Un alt tip de atac este cel de tipul „malware" (Anexa 4). Acest tip de program presupune atacul prin viruși de tipul „viermi" („worms"), „cai troieni" sau programe „spion" [35]. Spre deosebire de alte forme de atac, acesta este distribuit pe piața largă, fiind cumpărat, furat, distribuit și reutilizat, motiv pentru care sursa proveniență lui este necunoscută în totalitate. De asemenea, acest virus poate îmbrăca diverse forme, fiind folosit în moduri diverse în funcție de obiectivele atacatorului, având posibilitatea de a aborda multiple forme de atac. În 2020 și începutul anului 2021, s-a observat o scădere globală a „malware-ului". Această scădere a fost legată de pandemia de „COVID-19" și de faptul că angajații lucrau de acasă, limitând astfel vizibilitatea „malware-ului". Până la sfârșitul anului 2021, când multe persoane au început să se întoarcă la locul de muncă, s-a observat o creștere semnificativă a acestui tip de atac (Fig. 7). Creșterea „malware-ului" se atribuie în principal „crypto-jacking-ului"[18] și „malware-ului" pentru „IoT" [37]. Conform „ENISA", în primele 6 luni din 2022 au avut loc mai multe atacuri țintind „IoT" decât în cei 4 ani precedenți.

[17] este o unitate pentru informații digitale utilizată pentru a desemna capacitatea de stocare pe hard disk, sau memorie USB.
[18] utilizarea în secret a computerului unei victime pentru a crea criptomonede în mod ilegal

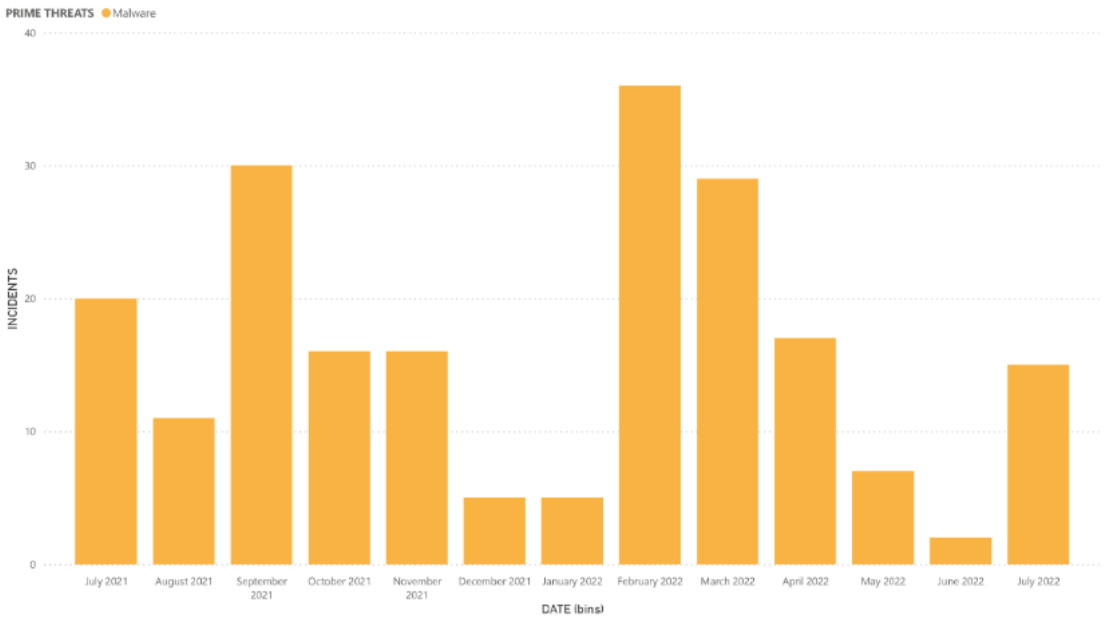


Fig. 7. Serii cronologice ale incidentelor majore observate de ENISA
Sursa: ENISA - Perspectiva atacaturilor 2022 (iulie 2021 – iulie 2022)

Cel de al treilea atac este cel de tipul ingineriei sociale (Anexa 4). Acest atac se bazează pe exploatarea erorilor umane pentru a obține acces la informații sau servicii [35]. Manipularea victimelor pentru a deschide documente, fișiere sau e-mailuri rău intenționate sau pentru a vizita anumite site-uri web, oferind astfel atacatorilor acces neautorizat la sisteme sau servicii, reprezintă o tactică des întâlnită în cadrul atacurilor cibernetice. Cel mai obișnuit tip de astfel de atac este „phishing-ul" (prin e-mail) sau „smishing-ul" (prin mesaje text).

„Phishing-ul" își propune să fure informații importante cu privire la carduri de credit, parole, etc. prin e-mailuri care implică ingineria socială și înșelăciunea. „Spear-phishing-ul" este o versiune mai sofisticată a „phishing-ului" care vizează organizații sau indivizi specifici. Compromiterea e-mailurilor instituționale reprezintă o înșelăciune care vizează acele instituții în care infractorii folosesc tehnici de inginerie socială pentru a obține acces la contul de e-mail al unui angajat, de preferat un superior ierarhic, pentru a inița transferuri bancare în condiții frauduloase. „Whaling-ul" este un atac de tipul „spear-phishing" îndreptat către utilizatori în poziții înalte (executivi, politicieni etc.). „Smishing-ul", un termen derivat dintr-o combinație de „SMS" și „phishing" și apare atunci când informațiile financiare sau personale ale victimelor sunt colectate prin utilizarea mesajelor „SMS". O altă amenințare similară este „vishing-ul", o combinație între „phishing" și voce, care apare atunci când informațiile sunt furnizate prin telefon, unde indivizii folosesc tehnici de inginerie socială pentru a extrage informații importante de la utilizatori [37].

În raportul efectuat de ENISA, s-au înregistrat un număr semnificativ de incidente, focusate în principal pe țările membre ale Uniunii Europene, care se foloseau de ingineria socială (Fig. 8). Se poate observa o creștere în anul 2022, comparativ cu anul precedent. Conform cercetărilor citate de „ENISA", aproape 60% dintre penetrările sistemelor de securitate din Europa, Orientul Mijlociu și Africa implică o componentă de inginerie socială [37]. Atacatorii apelează adesea la replicarea identității vizuale a organizațiilor din sectoarele financiare și tehnologice pentru a păcăli victimele. De asemenea, aceștia vizează tot mai frecvent proprietarii criptomonedelor și schimburile acestora. Conform „Raportului de Investigații al Încălcării Securității Datelor Verizon", aproximativ 82% din atacuri implică o componentă umană, motiv pentru care pregătirea personalului reprezintă un factor cheie împotriva unor astfel de atacuri. Indiferent de cât de performante sunt sitemele de securitate ale organizațiilor, componenta umană poate cădea în capcana unor astfel de atacuri, datorită lipsei vigilenței și a pregătirii în domeniu.

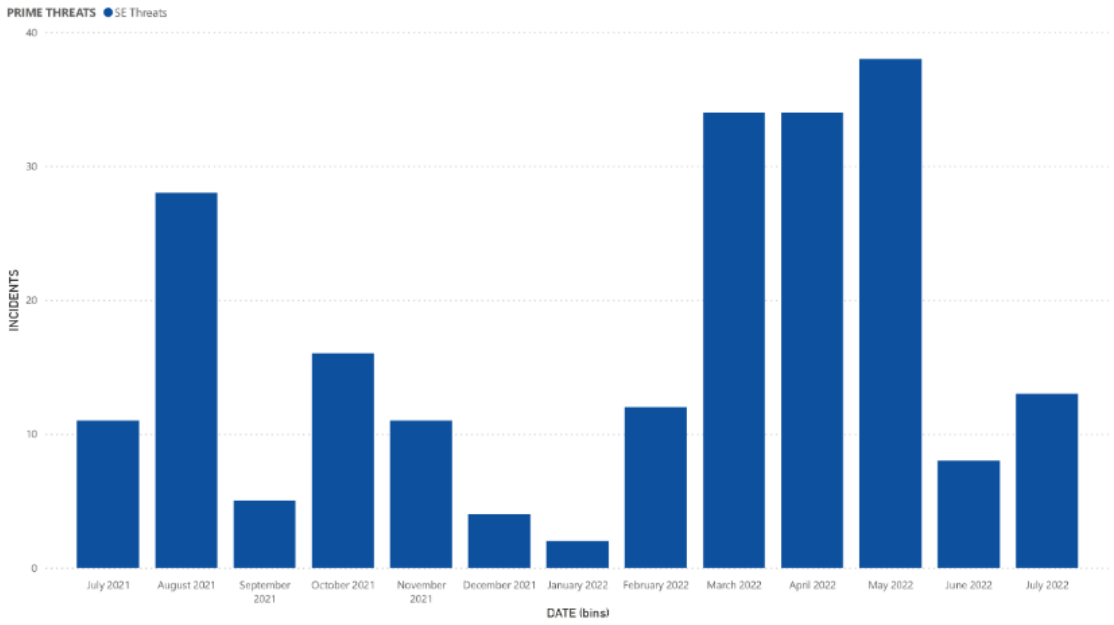


Fig. 8. Incidente majore cauzate de ingineria socială între iulie 2021 și iunie 2022
Sursa: ENISA - Perspectiva atacaturilor 2022 (iulie 2021 – iulie 2022)

Cel de al patrulea atac este reprezentat de amenințările la adresa datelor (Anexa 5), prin care se vizează sursele de date pentru acces neautorizat, întâlnind numeroase scurgeri de date. Într-o economie axată pe date, generăm cantități masive de informații care sunt de o importanță extremă, mai ales pentru companii și pentru inteligența artificială. Acest lucru le face o țintă majoră pentru infractorii cibernetici. Amenințările la adresa datelor pot fi în principal clasificate ca acces neautorizat, acest lucru reprezentând atacuri intenționate ale unui infractor cibernetic și scurgeri de date prin care se expun involuntar informații. Motivația principală a acestor atacuri sunt de cele mai multe ori sumele sub formă de bani, astfel că doar 10% din cazuri sunt datorate spionajului [35].

Alt tip de atac este cel prin amenințări la adresa disponibilității (Anexa 5). Acest atac blochează accesul la date și servicii (DoS). Atacurile de tip „DoS" (Denial of Service[19]) sunt strategii folosite de infractorii cibernetici pentru a împiedica accesul utilizatorilor la servicii sau resurse online. Scopul principal al acestor atacuri este de a bloca sau de a degrada semnificativ funcționarea unui site web, a unei aplicații sau a unui serviciu online. Într-un atac de tip „DoS", atacatorii își concentrează eforturile pentru a supraîncărca resursele unui server sau a unei rețele. Aceasta se poate realiza prin trimiterea unei cantități mari de cereri către server, depășindu-i capacitatea de procesare și determinându-l să devină inaccesibil pentru utilizatori legitimi. Obiectivul principal al unui atac „DoS" este de a bloca accesul utilizatorilor la serviciile online. De exemplu, un site web vizat poate deveni indisponibil pentru vizitatori, determinând pierderi de trafic pentru proprietarii site-ului. Atacurile „DoS" pot avea consecințe grave pentru organizații și utilizatori. Acestea pot duce la indisponibilitatea serviciilor critice, pierderi financiare, pierderea încrederii utilizatorilor și daune de imagine. Atacurile de tip „Denial of Service" (DoS) afectează din ce în ce mai mult rețelele mobile și dispozitivele conectate. Sunt foarte folosite în războiul cibernetic dintre Rusia și Ucraina [35]. Au fost vizate și site-urile web legate de „COVID-19", cum ar fi cele pentru vaccinare, raportul efectuat de „ENISA" arătând creșterea masivă a numărului de atacuri efectuat între iunie 2021 și iulie 2022, diferențele între lunile iulie a celor doi ani fiind de 7 ori mai mari în cel de al doilea an (Fig 9.).

[19] este un tip de atac cibernetic conceput pentru a dezactiva, închide sau întrerupe o rețea, un site web sau un serviciu

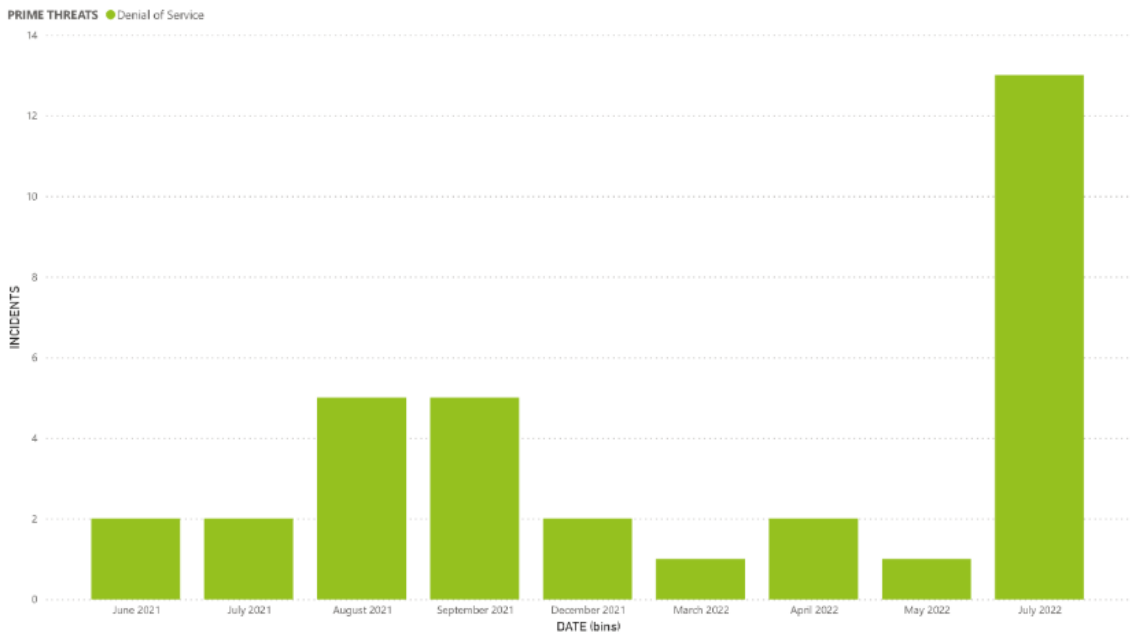


Fig. 9. Incidente majore cauzate de atacuri „DoS" între iunie 2021 și iulie 2022
Sursa: ENISA - Perspectiva atacaturilor 2022 (iulie 2021 – iulie 2022)

Tot din categoria amenințărilor la adresa disponibilității, întâlnim cel de al șaselea atac prin care se împiedică accesul la internet (Anexa 5). Acest tip de atac include și capturarea fizică, respectiv distrugerea infrastrucruii necesare internetului. Un bun exemplu, evidențiat de „ENISA" este cenzura activă, prin intermediul căreia Rusia a blocat în anul 2022, aproximativ 3000 de site-uri, datorită invaziei Ucrainei. Printre cele mai cunoscute pagini web care au fost blocate amintim de „Instagram", „Facebook", „Twitter", „BBC News" și altele [37]. Totodată, această decizie a Rusiei a condus la multe sancțiuni venite din partea guvernelor vestice deoarece certificatele „TSL/SSL" (certificate prin care se asigură o conexiune de încrede la date și la internet) erau expirate, rezultând conexiuni instabile și lipsite de încredere pentru utilizatori, expunând totodată întreaga rețea unui risc continuu prin care orice atacator putea pătrunde în rețea, accesând date lipsite de orice măsură de securitate.

Cea de a șaptea tehnică este cea de dezinformare (Anexa 6), prin care se distribuie informații înșelătoare, chiar și fără intenția de a produce daune. O tehnică modernă este cea numită „deepfake" care reprezintă o tehnolgie prin care se generează sunete, imagini, videoclipuri [35] sau informații false, create prin diverse programe de editate sau prin inteligență artificială și care datorită tehnologiilor moderne aproape că nu pot fi distinse de realitate. Astfel, odată create și distribuite către publicul larg, ajung să fie exploatate de mass-media și de rețelele sociale, împrăștiind informații false la nivelul întregii societăți. Astfel de metode precum „deepfake" își fac apariția și în rândul alegerilor politice, războaielor și alte asemenea, fiind de multe ori folosite chiar de către guvernul unei țări ca și avantaj împotriva guvernului altei țări cu care se confruntă. Exemple recente sunt cele reprezentate de numărul persoanelor infestate cu virusul „SARS-CoV-2", precum și numărul persoanelor rănite, atât în războiul dintre Rusia și Ucraina [37], cât și în războiul dintre Israel și Iran. Cu toate acestea, datorită dezinformării tot mai dese și a lipsei unor surse clare, nu se poate afirma sau infirma cu exactitate raportul de activitate al prezenței „deep-fake-ului", scopul principal fiind acela de a crea incertitudine în rândul oamenilor.

A opta cea mai cunoscută tehnică de atac este reprezentată de amenințările pe lanțul de aprovizionare (Anexa 6). Aceasta prevede relația dintre organizații și furnizorii de servicii, raportându-ne la un cumul de doua atacuri, pe de o parte la adresa furnizorului, iar pe de altă parte la adresa clientului. Mai specific, un prim atac asupra unui furnizor este folosit ulterior pentru a ataca o țintă prin care se obține acces la activele sale. Această țintă poate fi clientul final sau un alt furnizor. Astfel, pentru ca un atac să fie clasificat ca o agresiune asupra lanțului

de aprovizionare, atât furnizorul, cât și clientul trebuie să fie ținte [37]. Scopul unui atac asupra lanțului de aprovizionare poate fi variat, dar include de obicei obținerea accesului neautorizat la date și informații sensibile din rețelele furnizorilor, interferența cu procesele de producție sau livrare, cauzând întârzieri sau defecțiuni, alături de slăbirea încrederii în siguranța și securitatea lanțului de aprovizionare, precum și furtul de proprietate intelectuală sau secrete comerciale. Atacurile asupra lanțului de aprovizionare pot implica diverse tactici și tehnici, cum ar fi:
a) Compromiterea infrastructurii IT: „hackerii" pot compromite serverele sau rețelele furnizorilor pentru a obține acces la date.
b) Furtul de date și informații: obținerea datelor sensibile, cum ar fi planurile de produse sau informațiile financiare.
c) Atacuri de tip „phishing" și „malware": trimiteri de e-mailuri false sau infectarea cu „malware" a sistemelor furnizorilor pentru a obține acces.
d) Furtul de identitate: folosirea identității unui furnizor pentru a obține acces în rețelele și sistemele organizației țintă.
Desigur că principalele efecte ale unui astfel de atac implică pierderi financiare ale organizației, daune reputaționale, slăbind încrederea entității, precum și riscul de întrerupere a producției sau a livrării de produse sau servicii, lucru care denaturează afacerile și relația cu clienții.

Toate aceste tipuri de atac cibernetic, potrivit Agenției Europene pentru Securitate Cibernetică (ENISA), vizează pe primul loc administrația publică și guvernul (Anexa 7) [35], motiv pentru care instituțiile publice trebuie să se conformeze și să stabilească norme și reglementări prin care să își asigure securitatea cibernetică, protejând datele confidențiale și cu caracter sensibil. Așa cum am menționat, pe primul loc în topul amenințărilor la adresa securității cibernetice în Uniunea Europeana, între iunie 2021 și iunie 2022, conform „ENISA", 24% dintre incidentele raportate au ca țintă de guvernele și administrația publică, fiind pe primul loc în acest top. Pe locul doi se situează furnizorii de servicii digitale, înregistrându-se atacuri cibernetice la adresa acestora în proporție de 13%, fiind urmați de public larg (11,8%). Pe locul patru se situează sectorul serviciilor, având coeficientul de 11,8% în rândul atacurilor cibernetice, fiind urmat de sectorul financiar/bancar (8,6%), iar pe locul șase sectorul sănătății a reprezentat o altă țintă populară în rândul atacatorilor, reprezentând 7,2% din totalul atacurilor cibernetice înregistrate intre iunie 2021 și iunie 2022.

În urma formelor de atac adresate organizațiilor și nu numai, este important să evidențiem măsurile de apărare venite din partea entităților supuse atacurilor cibernetice, raportându-ne cu precădere la entitățile sectorului public. Sectorul public are responsabilitatea de a proteja informațiile sensibile și de a menține încrederea publică în fața amenințărilor avansate de securitate cibernetică. Tocmai de aceea este important să se implementeze practici solide de securitate cibernetică pentru a atinge acest obiectiv.

O bună practică de organizare a sectorului public în privința atacurilor cibernetice ar fi dispunerea unei proceduri legislative care să conțină norme și reglementări cu privire la acest aspect. În urma unei legislații bine puse la punct, este extrem de important ca sectorul public să pregătească funcționarii publici în vederea combaterii unor astfel de atacuri. Spre exemplu, un atac de tipul „phishing-ului", ar putea trece neobservat printr-un mail instituțional, indiferent de măsurile de securitate și de tehnologice puse la dispoziția respectivei entități. Un singur „click" al unuia dintre angajații instituției prin intermediul acelui mail, ar putea genera consecințe grave întregii instituții. Tocmai de aceea, este important ca personalul sa ia la cunostință astfel de tehnici, fiind instruiți să evite pe cât posibil accesarea unor astfel de mailuri. Aceștia ar trebui să transmită orice apariție a unor astfel de situații de tipul atacurilor „phishing", pentru a fi raportate mai departe. De asemenea, tehnici de tipul „autentificării în doi factori" și schimbul de parole regulate, stocarea datelor cu privire la accesarea documentelor, precum și modul de prelucrare al datelor cu caracter sensibil, nu trebuiesc a fi neglijate de către angajații organizațiilor. De menționat este că o singură pregătire a angajaților în vederea cunoașterii și aplicării unor astfel de principii nu ar fi suficientă datorită dezvoltării continue a tehnologiilor și apariției regulate a noi forme de atac, motiv pentru care instruirea personalului ar trebui să fie una regulată.

Un alt aspect important, îl constituie „backup-urile” regulate. Termenul de “backup” semnifică stocarea datelor sub formă de copie într-un alt loc al computerului sau pe un alt dispozitiv, astfel încât atunci când este nevoie să va putea reveni la forma originală în cazul unui eveniment care generează pierderea datelor. Așadar, „backup-urile” pot salva datele unei entități în cazul în care un atac cibernetic le va cripta sau le va șterge, păstrându-le integritatea în totalitate, fără riscul de a fi corupte fișiere importante. De asemenea, în cazul în care un angajat efectuează o acțiune neintenționată ce are ca efect denaturarea unui document, prin „backup” se va putea reveni la forma lui inițială. Din cauza unor astfel de erori umane, cel mai bine este ca accesul angajaților să fie limitat strict la sarcinile lor de lucru, evitând erori sau acțiuni care să încalce normele „GDPR”. De asemenea, pe lângă pregătirea personalului este desigur important ca instituțiile publice să beneficieze de aparatură de specialitate și de softuri menite să lupte împotriva atacurilor cibernetice. Pe lângă personalul obișnuit este important să existe experți în domeniul securității cibernetice care să asigure monitorizarea continuă a activităților digitale instituționale, cunoscând credențialele angajaților, domeniile, „IP-urile” și alte astfel de informații [38].

Astfel, prin adoptarea celor mai bune practici, cum ar fi implementarea unui cadru cuprinzător de securitate, evaluarea și gestionarea regulată a riscurilor, instruirea și conștientizarea angajaților, utilizarea unei strategii de apărare și implementarea unui plan de „backup” la incidente, organizațiile publice pot fi mai bine pregătite să facă față amenințărilor cibernetice din ce în ce mai avansate. De asemenea, este esențial să se acorde o atenție deosebită monitorizării continue și creării unui profil de securitate comun pentru simplificarea proceselor. Prin adoptarea acestor măsuri, organizațiile publice pot proteja informațiile sensibile, pot preveni încălcările de date și pot menține încrederea publică în mediul digital. Nu în ultimul rând, o colaborare prin schimb de informații eficiente între entități publice și private poate consolida, reziliența cibernetică globală, oferind o mai mare protecție împotriva amenințărilor cibernetice.

3.3. Legislație și reglementări privind digitalizarea în administrația publică

În urma subcapitolelor anterioare am discutat despre măsuri de securitate și amenințări cibernetice, alături de responsabilitatea instituțiilor în protejarea și securitatea datelor. Important de menționat este că toate aceste măsuri de securitate și responsabilități nu ar fi posibile fără un set de reguli si dispoziții în acest sens, în baza cărora instituțiile guvernamentale să își îndeplinească obligațiile. Tocmai de aceea, necesitatea unei legislații privind digitalizarea în administrația publică este esențială. În România, conceptele cu privire la digitalizarea din cadrul administrației publice sunt reglementate de mai multe legi și acte normative care impun anumite standarde și măsuri în ceea ce privește protejarea datelor și a infrastructurii informatice. Una dintre legile de bază în acest sens este Legea nr. 362/2018 privind securitatea cibernetică a rețelelor și a sistemelor informatice. Această lege a fost adoptată pentru a impune cerințele Directivei UE privind securitatea rețelelor și a sistemelor informatice (Directiva „NIS”), stabilind cadrul legal pentru protejarea infrastructurii critice, a serviciilor esențiale și a datelor sensibile în cadrul administrației publice și nu numai [39].

Directiva „NIS” (Network and Information Systems Directive) este o directivă a Uniunii Europene adoptată în anul 2016, ce are ca obiectiv îmbunătățirea securității rețelelor și a sistemelor informatice ale tuturor statelor membre. România, fiind stat membru al Uniunii Europene, este obligată să transpună și să aplice prevederile acestei directive în legislația sa națională. Astfel, transpunerea acestei directive în legislația națională a României a dus la adoptarea Legii nr. 362/2018 privind securitatea cibernetică a rețelelor și a sistemelor informatice.

Legea nr. 362/2018 stabilește standarde minime obligatorii de securitate cibernetică pe care instituțiile publice trebuie să le respecte. Aceste standarde acoperă aspecte precum protecția împotriva accesului neautorizat, gestionarea incidentelor de securitate, criptarea datelor și altele.

Totodată, impune cerințe pentru desemnarea operatorilor de servicii esențiale și a furnizorilor de servicii digitale și impune acestor entități să respecte anumite obligații și să pună în aplicare măsuri adecvate de securitate cibernetică. De asemenea, impune instituțiilor publice să raporteze incidentele de securitate cibernetică către Autoritatea pentru Digitalizarea României (ADR) sau alte autorități competente într-un interval de timp specificat. Acest lucru permite o gestionare mai eficientă a incidentelor și o înțelegere mai clară a peisajului amenințărilor cibernetice. Aceasta permite autorităților să efectueze audituri și inspecții periodice în instituțiile publice pentru a verifica respectarea standardelor de securitate cibernetică. Acest lucru asigură conformitatea și identificarea potențialelor vulnerabilități sau neconformități. Nu în ultimul rând, legea prevede sancțiuni pentru instituțiile publice care nu respectă cerințele de securitate cibernetică. Aceste sancțiuni pot include amenzi financiare substanțiale sau alte măsuri punitive [40]. Prin urmare, Legea nr. 362/2018 reprezintă un cadru legal esențial pentru asigurarea securității cibernetice în administrația publică din România. Instituțiile publice sunt obligate să respecte aceste cerințe pentru a proteja datele și informațiile sensibile, asigurând astfel un nivel adecvat de securitate în mediul digital în care operează.

Pe lângă apariția legii nr 362/2018, directiva „NIS" stabilește cerințe specifice pentru operatorii de servicii esențiale și a furnizorilor de servicii digitale, care sunt entități considerate vitale pentru funcționarea societății și a economiei. În România, aceste entități trebuie să respecte anumite obligații în ceea ce privește securitatea cibernetică, inclusiv raportarea incidentelor majore de securitate către autoritățile competente. Directiva „NIS" încurajează cooperarea și schimbul de informații între statele membre ale Uniunii Europene în ceea ce privește securitatea cibernetică. Acest lucru permite identificarea și răspunsul rapid la amenințările cibernetice care pot afecta mai multe țări. În conformitate cu această directivă, statele membre trebuie să desemneze autorități naționale pentru securitate cibernetică care să monitorizeze și să coordoneze măsurile de securitate cibernetică la nivel național. În România, această autoritate este Autoritatea pentru Digitalizarea României (ADR). Totodată, prin intermediul acestei directivei se includ cerințe specifice pentru protejarea infrastructurilor, cum ar fi energie, transporturi, sănătate și altele. În România, aceste sectoare sunt supuse unor reguli stricte privind securitatea cibernetică pentru a preveni și a gestiona eficient amenințările.

În era digitală, protejarea datelor sensibile devine o prioritate pentru administrația publică din România. Cu o cantitate enormă de date confidențiale gestionate de instituțiile publice, respectarea legislației și reglementărilor privind protecția datelor devine principala prioritate pentru menținerea integrității și securității acestor informații. Legea nr. 190/2018 care reprezintă implementarea Regulamentului General privind Protecția Datelor („GDPR") a adus cu sine cerințe stricte pentru protecția datelor personale. Această lege este aplicabilă tuturor instituțiilor publice care prelucrează date personale și impune standarde ridicate de securitate cibernetică. Instituțiile publice sunt obligate să adopte politici și proceduri interne clare pentru protejarea datelor sensibile. Acestea includ măsuri precum criptarea datelor, controlul accesului la informații confidențiale, gestionarea eficientă a parolelor și implementarea unor controale stricte pentru transferul și stocarea datelor. Pentru a asigura conformitatea cu standardele de protecție a datelor, instituțiile publice sunt supuse auditurilor și inspecțiilor periodice. Acest lucru este realizat atât de către autorități competente, cât și de către entități independente specializate în audituri de securitate cibernetică. Formarea personalului este un alt factor esențial în protejarea datelor sensibile. Instituțiile publice oferă programe de formare și sesiuni de conștientizare pentru angajați, pentru a-i instrui în cele mai bune practici privind securitatea cibernetică și protecția datelor. Obligația de a raporta incidentele de securitate cibernetică care implică date personale către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) este un alt aspect important al legislației „GDPR". Instituțiile publice trebuie să raporteze incidentele într-un termen de 72 de ore de la constatarea acestora. Prin implementarea acestor măsuri și respectarea reglementărilor stricte privind protecția datelor, administrația publică din România își asigură un nivel adecvat de securitate cibernetică și protecție a datelor sensibile împotriva amenințărilor din ce în ce mai sofisticate din mediul online. Aceste eforturi nu numai că protejează informațiile confidențiale ale cetățenilor, ci și

contribuie la menținerea încrederii în instituțiile publice și respectarea normelor legale și etice în ceea ce privește prelucrarea datelor personale.

O altă lege cu privire la digitalizarea organizațiilor guvernamentale este Legea 9/2023, care reprezintă un pas semnificativ către modernizarea și digitalizarea administrației publice din România. Această lege urmărește să reducă birocrația din instituțiile publice, eliminând, printre altele, necesitatea dosarului cu șină, un simbol al birocrației. Una dintre principalele prevederi ale Legii 9/2023 este obligația tuturor instituțiilor publice din România de a primi documente de la cetățeni în format electronic, inclusiv documentele de identitate [41]. Această schimbare înseamnă că cetățenii nu vor mai fi obligați să se deplaseze fizic la o instituție pentru a depune documente, ci le vor putea trimite online, economisind astfel timp și resurse. De asemenea, instituțiile publice sunt obligate să furnizeze pe propriile lor site-uri adrese de e-mail dedicate pentru expedierea documentelor în format online. Această măsură va facilita accesul la serviciile publice și va îmbunătăți eficiența în administrația publică. Un alt aspect important al Legii 9/2023 este impactul său potențial asupra procesului de obținere a certificatului constatator, un document esențial pentru companiile din România. În prezent, acest proces poate implica vizite la Oficiul Registrului Comerțului și depunerea de documente fizice. Odată cu intrarea în vigoare a acestei legi, procesul de obținere a certificatului constatator ar putea deveni mult mai eficient. Companiile vor putea trimite documentele necesare în format electronic, reducând timpul de așteptare și simplificând procedurile administrative [42]. Astfel, Legea 9/2023 marchează o schimbare semnificativă în administrația publică din România, cu un accent puternic pe digitalizare și eficiență. Aceasta va avea un impact profund asupra relației dintre cetățeni și instituțiile publice, simplificând procesele administrative și facilitând accesul la serviciile publice.

Amintim, totodată de legi care nu privesc în mod direct digitalizarea administrației publice, dar care influențează acest domeniu. Astfel, întâlnim Legea 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției. Această lege a fost una dintre primele inițiative legislative care au introdus conceptul de transparență și acces la informații în administrația publică. A stabilit obligația instituțiilor publice de a publica online informații despre activitățile lor, bugete, cheltuieli, decizii și alte aspecte relevante. Astfel, cetățenii au acces mai ușor la informații despre modul în care sunt administrate resursele publice și pot monitoriza mai eficient activitatea instituțiilor. De asemenea, amintim de Legea republicată nr. 52 din 21 ianuarie 2003, privind transparența decizională în administrația publică. Această lege a fost adoptată pentru a asigura transparența în procesul decizional al instituțiilor publice. Ea prevede obligația autorităților și instituțiilor publice de a publica proiectele de acte normative, hotărâri, regulamente și alte decizii într-un registru public online. Astfel, cetățenii și organizațiile pot să își exprime opiniile și să facă propuneri cu privire la aceste proiecte înainte de adoptarea lor. Nu în ultimul rând, amintim de Legea nr. 129 din 11 iulie 2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului, precum și pentru modificarea și completarea unor acte normative. Respectiva lege are un impact semnificativ asupra administrației publice prin introducerea obligației instituțiilor financiare și entităților publice de a implementa măsuri de verificare a identității clienților lor. Acest lucru implică adesea utilizarea unor sisteme digitale de verificare a identității, cum ar fi sistemele de identificare electronică și semnătură electronică. Acestea sunt doar câteva exemple de legi care vizează digitalizarea în administrația publică din România. Eforturile continue în acest sens au ca scop îmbunătățirea accesului cetățenilor la serviciile publice, simplificarea procedurilor administrative și creșterea transparenței în administrație.

Prin adoptarea unor legi și reglementări moderne precum Legea 9/2023 și alte acte normative menite să promoveze utilizarea tehnologiilor informatice, se urmărește reducerea birocrației, creșterea transparenței și îmbunătățirea accesului la serviciile publice. Implementarea unui cadru legislativ adecvat pentru digitalizare, precum și promovarea unor soluții tehnologice moderne, cum ar fi semnătura electronică, platformele online pentru depunerea documentelor și sistemele de verificare a identității, sunt pași importanți în această direcție. Aceste eforturi au ca

rezultat o administrare publică mai eficientă, simplificarea proceselor administrative pentru reducerea timpului și costurilor asociate interacțiunii cu instituțiile publice, precum și creșterea transparenței și responsabilității în administrația publică. Prin urmare, adoptarea unui cadru legislativ în administrația publică destinat ramurii digitale aduce beneficii semnificative atât pentru cetățeni, care au acces mai ușor la serviciile publice, cât și pentru instituțiile publice, care devin mai receptive la nevoile societății.

Capitolul 4. Transformarea digitală în administrarea fiscală: o analiză a eficienței și transparenței în cadrul ANAF

Datorită erei digitale în continuă expansiune, transformarea proceselor administrative devine o necesitate pentru instituțiile publice din întreaga lume. Administrarea fiscală nu este exlusă din acest proces, devenind un domeniu de interes major pentru implementarea soluțiilor tehnologice și digitale. În acest context, Administrația Națională de Administrare Fiscală (ANAF) din România încearcă să se adapteaze schimbărilor tehnologice pentru a îmbunătăți eficiența și transparența proceselor sale.

4.1. Descriere generală și obiective

Această cercetare are ca scop evaluarea transformării digitale în cadrul ANAF și impactul acesteia asupra eficienței și transparenței în administrarea fiscală. Transformarea digitală în acest context presupune adoptarea și implementarea tehnologiilor informației și comunicațiilor (TIC) pentru a îmbunătăți calitatea serviciilor din administrarea fiscală.

Astfel, obiectivul principal al acestui studiu este de a evalua eficiența și transparența în administrarea fiscală în cadrul ANAF, în contextul transformării digitale. Pentru a atinge acest obiectiv, cercetarea se va concentra pe două subcategorii: eficiența în procesele administrative și transparența în relația cu contribuabilii.

Principalele ipoteze generale ce stau la baza cercetării sunt:
- Utilizarea e-facturii poate simplifica și automatiza procesele de facturare și raportare, prin reducerea erorilor și a timpului necesar pentru gestionarea documentelor fiscale;
- Apariția „Spațiului Privat Virtual" a eficientizat modul de depunere al declarațiilor fiscale
- Utilizarea eficientă a tehnologiilor digitale poate genera o transparență sporită între ANAF și contribuabili, prin distribuirea informațiilor fiscale și a proceselor decizionale.

Prezenta analiză are la bază o cercetare empirică, în cadrul careia se va apela la o metodă de cercetare cantitativă. Prin intermediul unei astfel de metode de cercetare se oferă posibilitatea unei generalizări valide și fiabile cu privire la experiențele contribuabililor din cadrul ANAF. Totodată, această metodă a facilitat obținerea unor informații obiective care au condus la evaluarea eficienței și transparenței în administrarea fiscală.

Abordarea descriptivă estea cea mai potrivită formă pentru contextul studiului nostru, dorind să obținem o imagine detaliată a nivelului de adaptare și eficiență a digitalizării în administrația fiscală, în special în cadrul ANAF. Acest tip de abordare se concentrează pe descrierea fenomenelor, a caracteristicilor și a relațiilor dintre variabile, fără a se concentra pe cauzalitate. În cazul de față, dorim să obținem o înțelegere detaliată a modului în care transformarea digitală este adoptată și percepută în cadrul ANAF de către contribuabili, astfel că abordarea descriptivă permite explorarea acestor aspecte în profunzime. Totodată permite identificarea unor tendințe și modele în urma datelor colectate, cum ar fi preferințele sau comportamentele comune ale participanților. Aceste informații pot fi folosite pentru a evidenția aspectele relevante și pentru a oferi o perspectivă complexă asupra transformării digitale în administrarea fiscală. De asemenea, datele obținute prin abordarea descriptivă pot servi drept bază pentru procesul decizional în ceea ce privește implementarea și îmbunătățirea politicilor și strategiilor legate de digitalizare în cadrul ANAF-ului. Aceste informații pot ajuta la dezvoltarea și implementarea

unor strategii mai eficiente care vizează nevoile utilizatorilor. În urma acestei abordări urmărim formularea unor observații și concluzii despre fenomene care nu sunt direct observabile.

În ceea ce privește eșantionarea, a fost folosită metoda eșantionării neprobabile. Această metodă este cea mai potrivită în cadrul cercetării noastre deoarece, spre deosebire de celelalte tipuri care vizează un număr mare de membri ce necesită să fie proporționați în funcție de anumiți factori de probabilitate, prezenta metodată se bazează pe alți decât probabilitatea. Astfel, selecția eșantionului este realizată fără a acorda șanse egale de participare pentru toți cei interesați. Eșantionarea folosită în cadrul acestei cercetări a țintit o anumită tipologie de indivizi care să îndeplinească următoarele cerințe:

- Participantul dobândește cunoștințe minime de utilizare a tehnologiei și a internetului pentru a folosi serviciile digitale ale ANAF;
- Participanții trebuie să fi interacționat anterior cu serviciile digitale ale ANAF, cum ar fi depunerea declarațiilor fiscale online sau înregistrarea în „Spațiului Privat Virtual"
- Participantul a interacționat sau cunoaște concepte cu privire la e-factură și la semnătura digitală

Cercetarea nu necesită un număr maxim de participanți pentru atingerea eșantionului propus, iar aspectele de tipul vârstei, genului sau etniei sunt considerate drept irelevante pentru îndeplinirea obiectivelor propuse.

Cercetarea noastră a avut ca scop principal chestionarea angajaților din cadrul a 10 organizații, fie ele publice sau private, chestionând între 5 și 10 angajați (în funcție de mărimea numărului de angajați din respectiva organizație). În urma finalizării chestionarului, s-a înregistrat un număr de 83 de participanți care au finalizat chestionarul, participanți care interacționează în prezent sau au interacționat în trecut cu serviciile ANAF, fiind contribuabili ai acestei instituții.

Tehnica de cercetare utilizată pentru analiza noastră folosită drept metodă de colectare a datelor cercetării, a fost metoda anchetei, iar instrumentul folosit pentru colectarea datelor a fost chestionarul online, prin intermediul platformei „Google Forms".

Chestionarul presupune participarea voluntară și anonimă a tuturor participanților, răspunsurile acestora fiind utilizate strict în scopul cercetării. Aceste aspecte au la bază garantarea respectării dreptului la confidențialitate în baza Regulamentului (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor). În introducerea chestionarului au fost amintite toate aceste aspecte, furnizând si două adrese de contact pentru orice sesizare sau nelămurire. Totodată, am prezentat participanților scopul chestionarului și timpul aproximativ necesar completării acestuia.

Lista întrebărilor din cadrul chestionarului a fost divizată în trei părți. În prima parte, participanții chestionarului au primit o singură întrebare în cadrul careia trebuiau să confirme interacțiunea acestora anterioară cu serviciile digitale ANAF. Această întrebare avea ca și răspuns doar varianta „Da", pentru a ne asigura că orice persoană a întrunit condiția obligatorie de participare în cadrul chestionarului. Prin această întrebare ne-am asigurat că toate rezultatele obținute din analiza următoarelor întrebări vor conține doar răspunsuri ale unor participanți care au mai interacționat cu serviciile ANAF.

Cea de a doua parte a chestionarului a cuprins doua întrebări, cu privire la „Spațiului Privat Virtual" și semnătura electronică, urmărind măsura de interacțiune a participanților, în relația cu unele dintre cele mai importante servicii cu care interacționează ANAF.

După prima parte, cea de verificare a participanților și cea de a doua parte de acomodare, a urmat cea de a treia parte care a cuprins o varietatea de întrebări, cu o singură variantă de răspuns. Răspunsurile au fost de trei forme. Una dintre forme avea ca variantă de răspuns la întrebare una dintre variantele „Da"/„ Nu", acolo unde răspunsurile puteau îmbrăca doar o

formă clară si concisă de acest tip. Cea de a doua formă, avea cinci variante de răspuns, în scară liniară, varianta de mijloc fiind una care să arate neutralitatea, iar prima și ultima fiind polurile opuse de răspuns (exemplu: foarte neclar, neclar, neutru, clar, foarte clar). Cea de a treia formă de răspuns folosită la una dintre întrebările chestionarului, este destul de asemănătoare cu cea menționată anterior, reprezentând o „scară" de la 1 la 5, în care 1 semnifică o atitudine foarte negativă vizavi de întrebarea adresată participantului, iar 5 o atitudine foarte pozitivă. Această parte a chestionarului a urmărit furnizarea unor răspunsuri certe, cu privire la site-ul ANAF și la informațiile furnizatea de acesta, la drepturi și obligații fiscale furnizate de această instituție, la claritatea și coerența comunicării în relația cu cetățenii, la disponibilitatea comunicării schimbarilor legislative și a obligațiilor fiscale, la transparența proceselor de colectare a taxelor și impozitelor, la furnizarea de rapoarte fiscale, la accesibilitatea datelor fiscale și a clarității acestora, la receptivitatea sugestiilor și reclamațiilor contribuabililor, la influența proceselor decizionale, precum și a utilității „Spațiului Privat Virtual", a semnăturii electronice și a e-facturii.

4.2 Perspective ale analizei

În urma finalizării chestionarului am acumulat un număr semnificativ de răspunsuri din partea participanților, urmând să analizăm aceste răspunsuri pentru a putea proiecta o concluzie ulterioară. Prima întrebare, așa cum am menționat este una de verificare a participanților, astfel că vom începe cu cea de a doua întrebare:

- În ce măsură sunteți familiarizat(ă) cu depunerea declarațiilor online prin intermediul „Spațiului Privat Virtual"? (Fig. 10)

Răspunsurile acestei întrebări au prezentat o pondere majoritară cu privire la folosirea regulată a acestor servicii, fiind selectată de peste jumătate din participanți (54,2%). Tot din variantele de răspuns cu privire la persoanele care au mai interacționat cu astfel de servicii, am obținut un procentaj de 37,3% de răspunsuri ale participanților care au folosit de câteva ori astfel de servicii, restul de 8,4% neinteracționând vreodată cu aceste servicii ale ANAF-ului. Acest lucru poate indica faptul că majoritatea contribuabililor au deja cunostință despre astfel de servicii ale ANAF, precum „Spațiului Privat Virtual" și peste jumătate din aceștia folosesc în prezent sau au folosit măcar o dată aceste servicii.

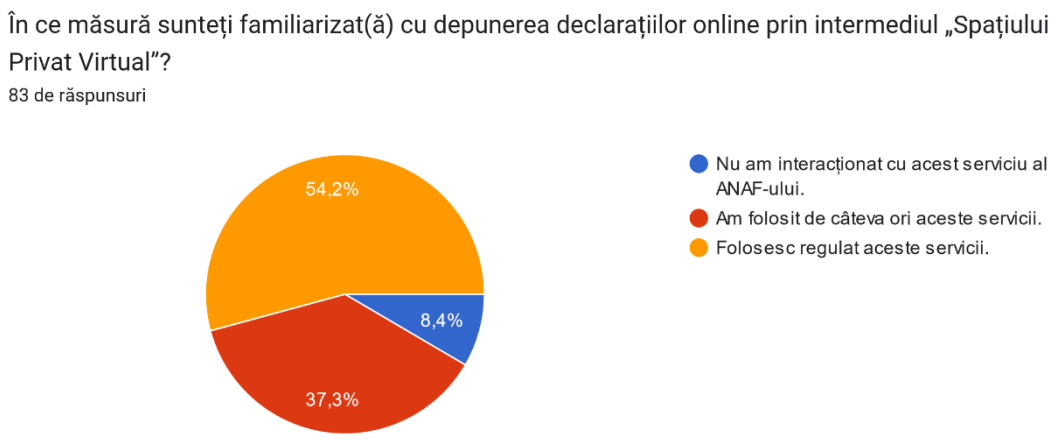


Fig. 10. A doua întrebare din chestionar
Sursa: Google Forms

- Dobândiți în prezent un certificat pentru semnătură electronică? (Fig. 11)

Aceasta a fost cea de a treia întrebare, cu privire la utilizarea semnăturii electronice, prin intermediul căreia documentele pot fi depuse direct online, evitând timpul pierdut pentru depunerea acestora în mod fizic la ghișeu. Certificatul pentru semnătura electronică poate fi de două feluri, fie prin intermediul unui „token", fie prin „cloud". Deținerea unui „token" presupune accesul semnăturii electronice printr-un stick, care odată introdus în device-ul de unde se dorește efectuarea semnăturii electronice, se va permite accesul. În general această metodă este folosită de persoanele care doresc ceva palpabil și nu au suficientă încredere în serviciile „cloud", din diverse motive precum securitatea contului acestora. Cea de a doua metodă, prin care certificatul se află în „cloud", este folosită în general de persoanele care nu vor să aibă grijă în permanență de un „token", folosind certificatul digital pentru semnătura electronică de oriunde, accesându-și contul, prin intermediul unui username și a unei parole. Astfel, aproape jumătate din participanți (44,6%) au ales metoda clasică, de a avea acces la certificat prin intermediul unui „token", iar 27,7% dintre aceștia, au ales metoda accesării certificatului prin intermediul „cloud". Cu toate acestea, există și alți participanți, în proporție de 10,8% care au utilizat una dintre aceste variante în trecut, însă fie le-a expirat certificatul, fie nu mai doresc utilizarea acestuia în prezent. Restul de 16,8% nu au acces la un astfel de instrument, însă 10,8% din totalul participanților doresc să utilizeze în viitorul apropriat un astfel de certificat prin care să aibă acces la semnătura electronică.

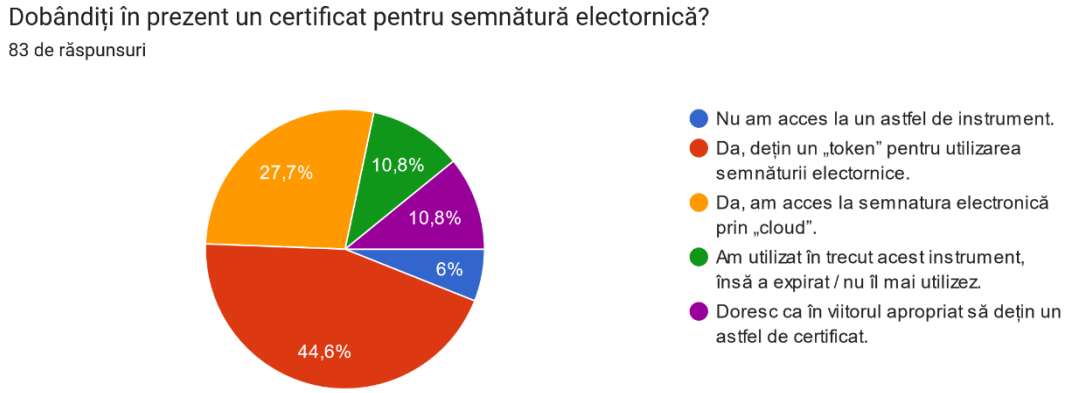


Fig. 11. A treia întrebare din chestionar
Sursa: Google Forms

- Cât de ușor vă este să găsiți informații, proceduri, proiecte sau reguli fiscale pe site-ul ANAF? (Fig. 12)

Această întrebare a urmărit nivelul de transparență al informațiilor furnizate de ANAF pe site-ul oficial al acestei instituții. În urma rezultatelor, participanții au avut păreri foarte diversificate, astfel că cea mai mare majoritate a ales varianta de răspuns prin care reiese că le este destul de ușor să găsească informații, fiind de părere că informațiile furnizate sunt relativ accesibile și pot fi găsite relativ rapid pe site-ul ANAF, răspunsul acestora având o pondere de 42,2% din totalul răspunsurilor. Următorul grup semnificativ este de 37,3%, aceștia considerând găsirea informațiilor extrem de ușoară, simplă și rapidă, site-ul având o organizare excelentă, prezentând un acces ușor la resursele necesare. Ca și răspuns neutru, aproximativ 10% din participanți sunt de părere că gasirea informațiilor este posibilă, însă necesită fie căutări repetate, fie navigarea în diverse părți ale site-ului. Din restul răspunsurilor concluzionăm că două persoane consideră accesarea informațiilor puțin dificilă, fiind necesar timp suplimentar pentru găsirea informațiilor, necesitând efort, iar alte două persoane sunt de părerea că găsirea informațiilor pe site-ul ANAF nu este o activitate deloc ușoară, informațiile fiind neorganizate corespunzător și greu de găsit. Alte patru persoane din numărul total de participanți, s-au abținut din a răspunde acestei întrebări sau nu au luat la cunoștință astfel de informații.

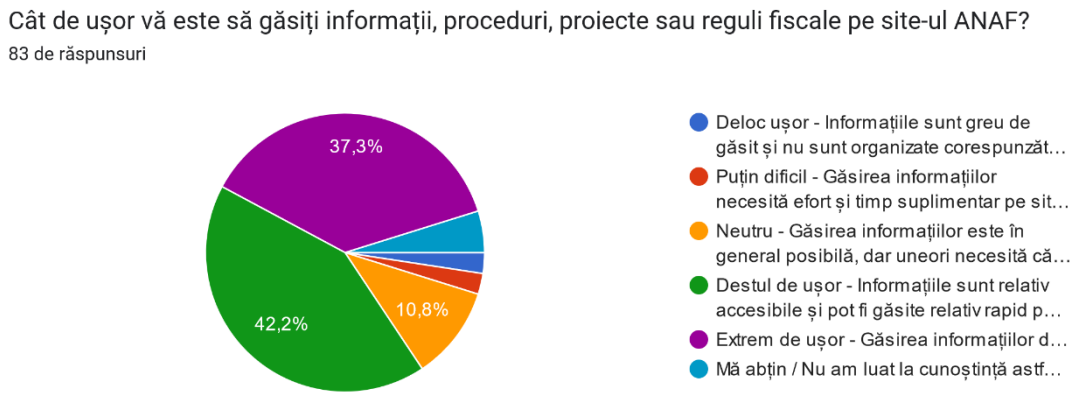


Fig. 12. A patra întrebare din chestionar
Sursa: Google Forms

- Considerați că ANAF furnizează suficiente informații despre drepturile și obligațiile fiscale ale contribuabililor?

Aceasta a fost cea de a cincea întrebare adresată partipanților, în cadrul căreia aproximativ 42% dintre aceștia consideră destul de suficiente informațiile furnizate de ANAF despre drepturile și obligațiile fiscale ale contribuabililor, însă aceștia sunt de părere că unele aspecte ar putea fi mai accesibile sau mai bine explicate. Aproape 35% din răspunsuri consideră aceste informații cu privire la drepturile și obligațiile fiscale ca fiind suficiente, participanții fiind de părere că ANAF oferă informații cuprinzătoare și clare, facilitând astfel înțelegerea și respectarea acestora. Trei persoane consideră că astfel de informații nu sunt îndeajuns de suficiente, astfel că, deși ANAF oferă anumite informații, acestea sunt limitate sau vagi, ceea ce poate crea confuzie sau incertitudine pentru contribuabili. Alte două persoane au votat că informațiile menționate anterior nu sunt deloc suficiente, fiind din perspectiva lor incomplete sau greu de găsit. Restul de trei participanți se abțin de la această întrebare sau nu au luat la cunostință astfel de informații.

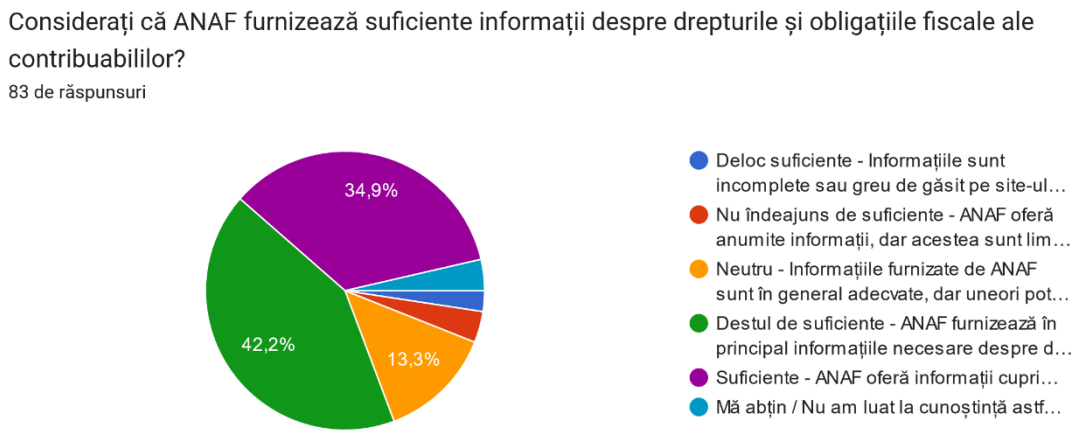


Fig. 13. A cincea întrebare din chestionar
Sursa: Google Forms

- Cum evaluați claritatea și coerența comunicării oficiale a Agenției Naționale de Administrare Fiscală în ceea ce privește schimbările legislative și fiscale? (Fig. 14)

Și de această dată, întrebarea propusă este una menită să evalueze transparența în relația cu contribuabilii ANAF. Peste o treime dintre răspunsuri sugerează o înțelegere clară a informațiilor oferite de ANAF în privința schimbărilor legislative. O altă treime (într-o proporție

mai numeroasă cu o persoană spre deosebire de cea menționată anterior), evaluează claritatea și coerența ANAF asupra schimbărilor legislativ-fiscale, una foarte clară și ușor de înțeles. Aproximativ 15% din participanți în schimb, abordează o atitudine neutră vizavi de acest subiect, considerând comunicările efectuate de ANAF drept unele inconsistente. Două dintre răspunsuri evaluează această comunicare efectuată de ANAF drept una neclară, în care informațiile furnizate sunt ambigue, iar alți doi consideră că aceste schimbări sunt confuze, alegând o varintă de răspuns care evaluează claritatea comunicării oficiale ANAF ca fiind foarte neclară. Nu în ultimul rând, trei dintre participanți s-au abținut din a furniza un răspuns.

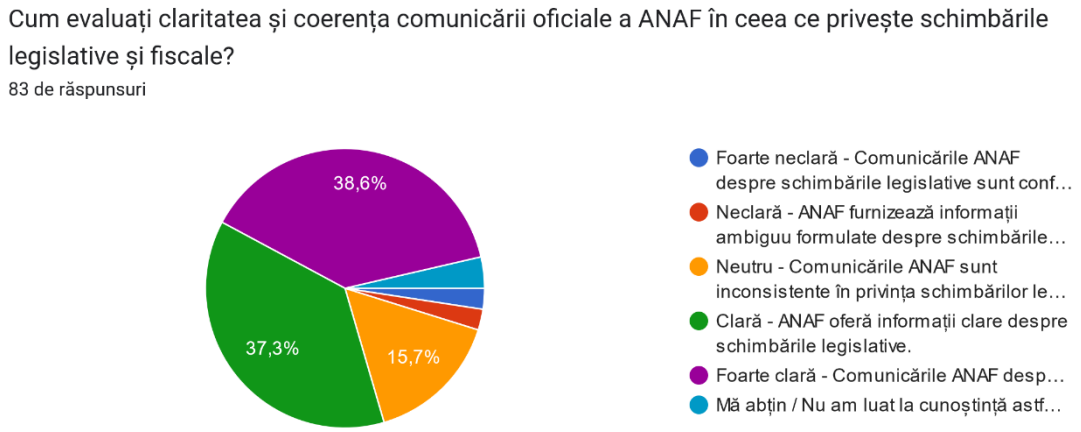


Fig. 14. A șasea întrebare din chestionar
Sursa: Google Forms

- Sunteți mulțumit de modul în care ANAF comunică cu contribuabilii cu privire la obligațiile fiscale și la posibilele modificări ale legislației? (Fig. 15)

La prima vedere, această întrebare seamăna destul de mult cu întrebarea anterioară. Acest lucru are loc pe de o parte pentru a verifica consistența răspunsurilor participanților atunci când iau o decizie cu privire la un răspuns, iar pe de altă parte, în întrebarea anterioară doream să aflăm dacă informațiile legislative și fiscale sunt clare și transparente. pe când această întrebare dorește să clarifice opinia participanților cu privire la modurile în care ANAF comunică cu contribuabilii, din punct de vedere al eficienței. Astfel, mai bine de 40% din răspunsuri sunt de părere că ANAF oferă informații adecvate, existând însă loc de îmbunătățire. Peste treizeci de participanți sunt foarte mulțumiți de modul în care ANAF comunică cu aceștia, afirmând despre comunicarea ANAF că este una eficientă și clară. Peste 8% dintre răspunsuri au fost neutre, participanții fiind indiferenți vizavi de modul în care ANAF comunică, iar 6% din totalul participanților consideră că deși ANAF comunică cu aceștia, nu o face în mod eficient. Alți trei participanți ai chestionarului consideră că ANAF nu prea comunică cu aceștia, eficiența în comunicare fiind insuficientă, iar alți trei participanți nu au luat la cunoștință astfel de informații.

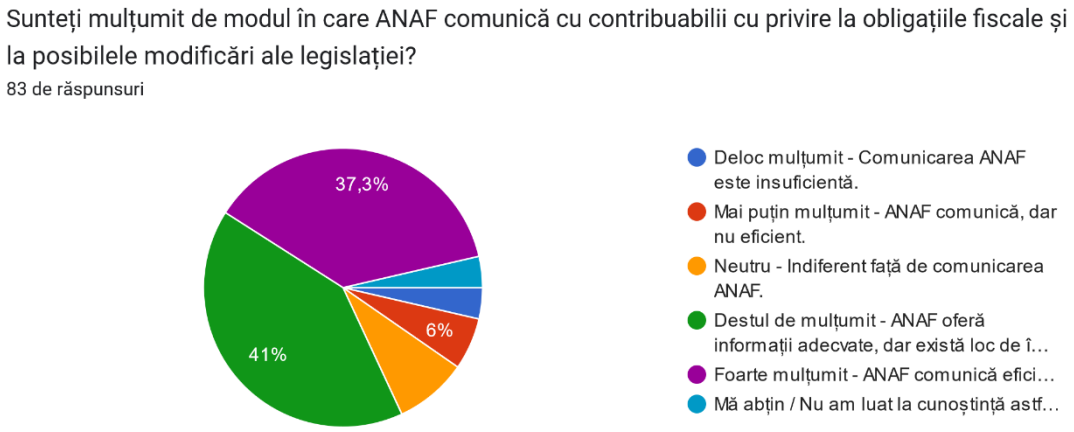


Fig. 15. A șaptea întrebare din chestionar
Sursa: Google Forms

- Considerați că ANAF furnizează suficiente informații despre modul în care sunt colectate și gestionate impozitele și taxele? (Anexa 8)

Această întrebare va avea ca rezultat un raport ce va evidenția transparența instituției ANAF deoarece informațiile de natura colectării și gestionării impozitelor și taxelor reprezintă una dintre principalele preocupări ale unui contribuabil. Contribuabilii ANAF poartă acest nume deoarece prin definiția lor reprezintă acele entități obligate la plata impozitelor către agențiile fiscale. Tocmai de aceea, aceste persoane sunt interesate să afle ce se întâmplă cu banii datorați statului. Aproximativ 90% dintre răspunsuri consideră că ANAF furnizează suficiente informații despre colectarea și gestionarea impozitelor și taxelor, restul de circa 10% având păreri opuse, considerând informațiile oferite de ANAF ca fiind insuficiente.

- Aveți încredere că procesele de colectare a impozitelor și taxelor sunt transparente și echitabile? (Anexa 9)

Și de această dată, prin intermediul celei de a noua întrebare din chestionarul nostru, dorim să aflăm opinia contribuabililor cu privire la procesul de colectare a impozitelor și taxelor menționate la întrebarea anterioară, urmărind nivelul de transparență a instituției ANAF. Spre deosebire de întrebarea anterioară, raportul între varianta de răspuns „Da” și “Nu” se schimbă, însă nu semnificativ, astfel că doar 85% dinte participanți consideră că au încredere în procesele de colectare a impozitelor și taxelor într-un mod transparent și echitabil, în timp ce aproximativ 15% din restul voturilor reprezintă participanți a căror încredere este scăzută, fără a fi de acord cu afirmația conform căreia procesele de colectare a taxelor și impozitelor sunt unele transparente. Cu toate acestea, datorită scepticismului și a lipsei de informații în anumite cazuri, nivelul transparenței ANAF, poate fi denaturat de astfel de factori. Cu toate acestea, peste jumătate din participanți, la o diferență considerabilă de opiniile celorlalți, au arătat încrederea contribuabililor cu privire la modul de colectare a impozitelor și taxelor acestora de către ANAF.

- Aveți acces la informațiile și rapoartele fiscale relevante pentru a vă gestiona corect situația fiscală? (Fig. 16)

În cadrul acestei întrebari am încercat să aflăm în ce măsură contribuabilii pot accesa informații relevante pentru aceștia, în procesul de gestionare a situației lor fiscale. Accesarea rapoartelor fiscale este esențială pentru a gestiona corect situația fiscală, creând un mediu transparent între ANAF și contribuabili. Observăm cum peste jumătate dintre aceștia (57,8%) au acces la informațiile și rapoarte fiscale în mod corect. Aproximativ 21% dintre entitățile care au votat însă, sunt de părere că deși au acces la rapoarte și alte informații fiscale, întâmpină uneori

dificultăți în gestionarea acestora în mod corect. Aproximativ 17% dintre contribuabili afirmă că au acces la unele informații, dar nu la toate, ceea ce poate afecta gestiunea corectă a situației lor fiscale. Doi dintre contribuabili susțin că nu au acces la informațiile și rapoartele fiscale necesare deși își doresc acest lucru în vederea gestionării corecte a situației loc fiscale. Totodată, una dintre entități susține că nu are acces la informațiile și rapoartele fiscale revelante.

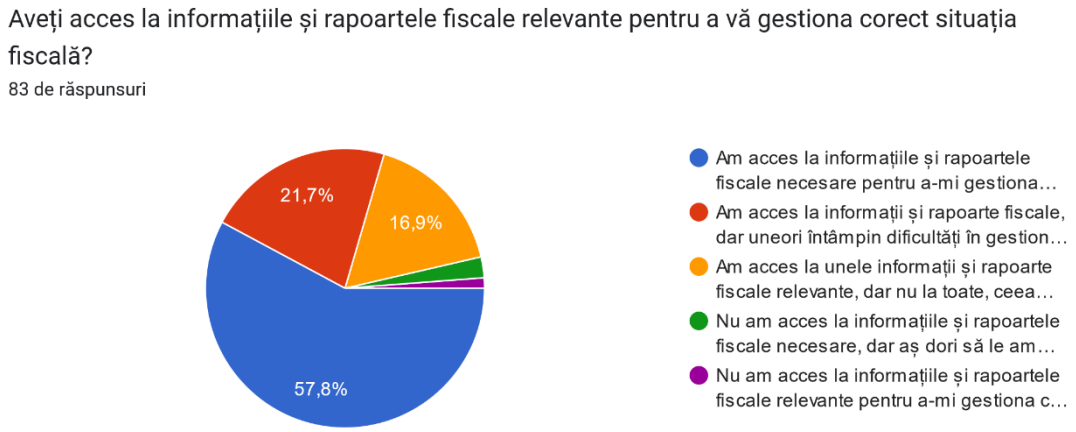


Fig. 16. A zecea întrebare din chestionar
Sursa: Google Forms

- Cum evaluați accesibilitatea și claritatea datelor fiscale disponibile în platformele online ale Agenției Naționale de Administrare Fiscală? (Fig. 17)

Această întrebare valorifică atât nivelul de transparență, cât și cel de eficiență în ceea ce privește platformele online ale ANAF. Răspunsul majoritar, constituit din aproape jumatate din totalul participanților (45.8%) evaluează accesibilitatea și claritatea datelor fiscale regăsite pe platformele online ale ANAF ca fiind destul de clare, astfel că datele sunt ușor de accesat, iar claritatea lor este una adecvată. În continuare, peste 33% dintre participanți sunt de părere că datele fiscale sunt foarte accesibile și clar formulate pe platformele online ale ANAF, facilitând înțelegerea și utilizarea lor de către contribuabili. Alți 12% au o opinie neutră vizavi de această evaluare astfel că, accesibilitatea și claritatea datelor fiscale sunt acceptabile conform opiniei acestora, însă există și aspecte care necesită îmbunătățiri. Cinci dintre persoanele care au răspuns la chestionar consideră accesibilitatea și claritatea datelor fiscale disponibile pe platformele online ale ANAF puțin neclare, fiind de părere că există eforturi pentru a primi date fiscale, dar accesibilitatea și claritatea acestora pot fi îmbunătățite. Restul de două entități catalogheză acest aspect drept unul neclar și dificil în care datele fiscale disponibile în platformele online ale ANAF sunt greu de accesat și de înteles.

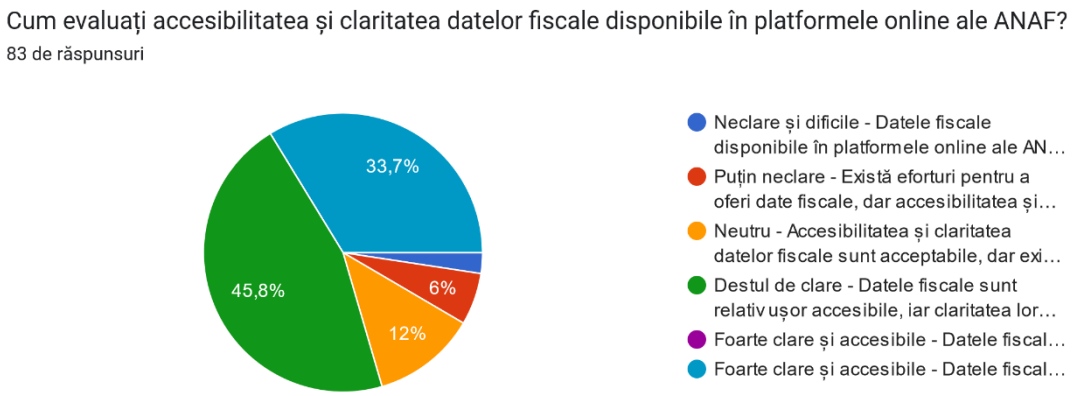


Fig. 17. A unsprezecea întrebare din chestionar
Sursa: Google Forms

- Considerați că ANAF este receptiv la feedback-ul și sugestiile contribuabililor în ceea ce privește îmbunătățirea proceselor fiscale? (Fig. 18)

La această întrebare părerile au fost destul de divizate, astfel că entitățile au întâmpinat în unele cazuri un nivel de comunicare deficitar al ANAF, comparativ cu situatiile celorlalți. Desigur, această raportare diferită, a instituției în relație cu contribuabilii, se poate datora sugestiei în sine. Astfel, dacă o sugestie este neeficientă și irealizabilă, desigur că feedback-ul venit din partea ANAF nu va fi unul foarte receptiv. Cu toate acestea, aproximativ 42% dintre răspunsuri vizează receptivitatea ANAF la feedback-ul contribuabililor ca fiind una parțială, în care ANAF-ul poate fi receptiv la anumite sugestii, existând însă loc pentru îmbunătățiri în această privință. Alte 20 de entități (24,1% din totalul participanților) cataloghează ANAF drept o instituție receptivă, în care feedback-ul și sugestiile contribuabililor sunt luate în considerare pentru îmbunătățirea proceselor fiscale. Doisprezece entități (14,5% din totalul răspunsurilor) au o abordare neutră cu privire la receptivitatea ANAF, nefiind sigure dacă sugestiile și feedback-ul acestora este sau nu luat în considerare pentru îmbunătățirea proceselor fiscale. Alți 8,4% dintre candidații chestionarului afirmă despre receptivitatea ANAF că este insuficientă, considerând că instituția nu este îndeajuns de receptivă la feedback-ul și sugestiile contribuabililor. Nu în ultimul rând 10,8% din totalul participanților clasifică receptivitatea ANAF pe cea mai joasă treaptă de răspuns, considerând că aceasta nu este deloc receptivă la feedback-ul și sugestiile contribuabililor în ceea ce privește îmbunătățirea proceselor fiscale.

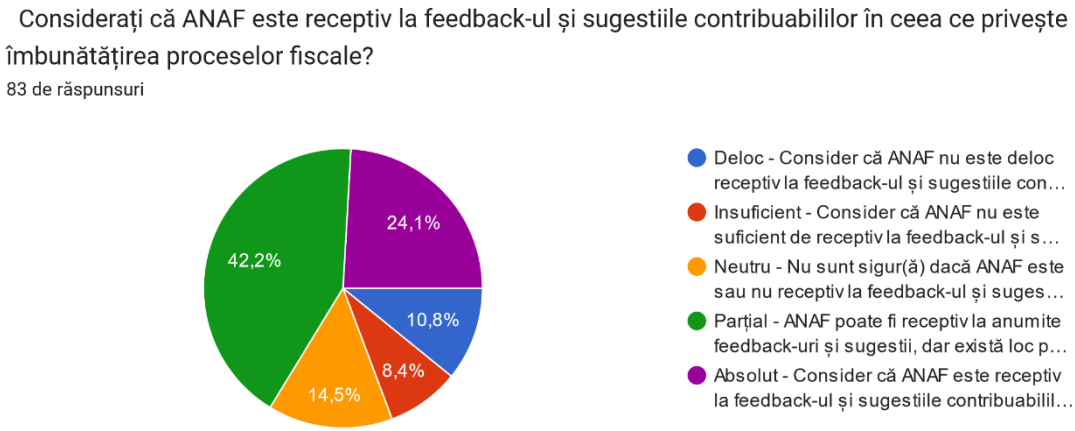


Fig. 18. A doisprezecea întrebare din chestionar
Sursa: Google Forms

- Aveți cunostință despre posibilitatea și modalitățile prin care contribuabilii pot influența procesele decizionale ale ANAF? (Fig. 19)

O relație stabilă între stat și cetățeni are la bază implicarea cetățenilor în procesele decizionale. Tocmai de aceea, este extrem de important ca și o instituție precum ANAF să ofere posibilitatea contribuabililor de a se implica în precesele decizionale. Haideți să vedem însă în ce măsură cunosc participanții noștri această posibilitate. Observăm cum partea majoritară, în proporție de aproximativ 35% cunoaște într-o oarecare măsură aceste aspecte, având o vagă cunoștință despre aceste modalități, fără să fie pe deplin familiarizați cu toate detaliile. Alte 13,3% din entități au o cunoștință parțială vizavi de aceste aspecte, cunoscând câteva modalități prin care contribuabilii pot influența procesele decizionale ale ANAF, însă sunt de părere că nu au luat la cunoștință toate posibilitățile. Aproximativ 17% dintre entitățile supuse chestionarului, nu prea au luat la cunoștință de aceste aspecte afirmând că au auzit vag de aceste lucruri, fără să cunoască informații detaliate despre modalitățile în care contribuabilii pot influența procesele ANAF. Alte 23 de răspunsuri (27,7% din totalul răspunsurilor) afirmă că dețin cunoștinnțele necesare despre aceste modalități de influențare a proceselor decizionale, pe când restul de 7,2% entități nu au nicio cunoștință despre modalitățile menționate anterior.

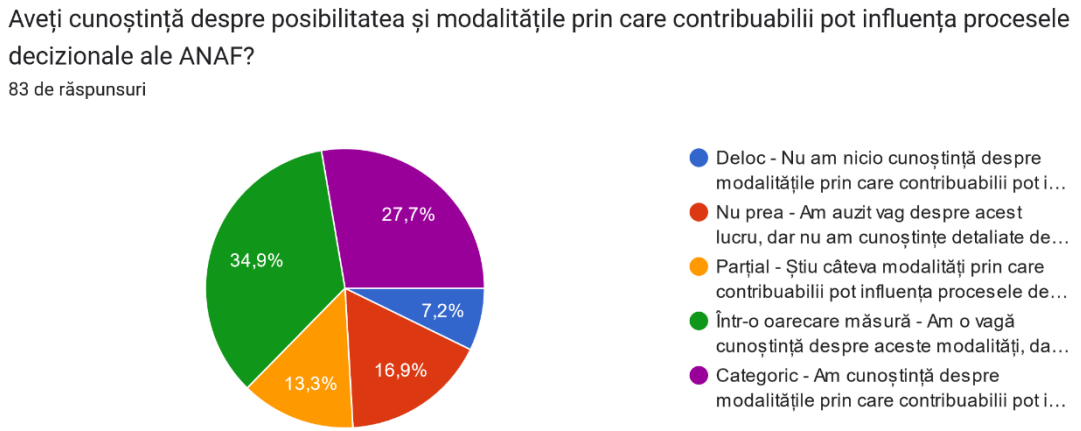


Fig. 19. A treisprezecea întrebare din chestionar
Sursa: Google Forms

- În ce măsură v-a ajutat / credeți că v-ar ajuta depunerea declarațiilor online prin intermediul „Spațiului Privat Virtual" spre deosebire de depunerea acestora în format fizic? (Fig. 20)

Aceasta a fost cea de a paisprezecea întrebare adresată contribuabililor care au răspuns acestui chestionar. Prin intermediul unei astfel de întrebări am creat o gamă largă de răspunsuri pentru a permite participanților să-și exprime opiniile cât mai clar, concluzionând nivelul de eficiență al ANAF. Astfel, patruzeci dintre participanți consideră că utilizarea SPV-ului i-a ajutat foarte mult, iar depunerea declarațiilor online prin acest serviciu este mult mai eficientă și convenabilă decât depunerea lor în format fizic. Alți treizeci de participanți consideră ca accesul în SPV i-a ajutat destul de mult, fiind o variantă mai ușoară decât depunerea declarațiilor fiscale în format fizic, existând totuși ușoare dificultăți. Alți zece contribuabili au avut o atitudine neutră vizavi de eficiența ANAF printr-un astfel de serviciu, fiind de părere că nu este observabilă nicio diferență între eficiența depunerii declarațiilor online și fizice. Alți doi contribuabili consideră că ambele metode sunt eficiente, însă metoda de depunere a declarațiilor online este puțin mai eficientă decât posibilitatea de a depune declarațiile fiscale prin intermediul SPV-ului. O singură entitate neagă în totalitate utilitatea și eficiența serviciului de depunere a declarațiilor online prin SPV, considerând că nu este deloc o metodă utilă și convenabilă, spre deosebire de depunerea documentelor în format fizic.

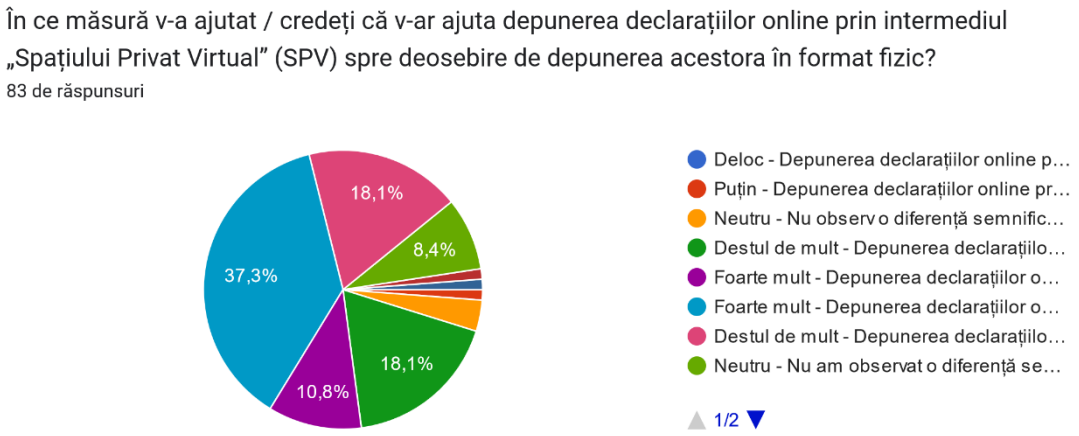


Fig. 20. A paispreprezecea întrebare din chestionar
Sursa: Google Forms

- Considerați că utilizarea semnăturii electronice a eliminat necesitatea stocării documentelor semnate și a copiilor de rezervă, precum și a imprimării fiecărui document pentru semnare? (Fig. 21)

Un alt serviciu esențial în domeniul administrativ, prin care se dorește sporirea eficienței este acela de utilizare a semnăturii electronice. Tocmai de aceea, o mare parte din contribuabili au ales abordarea unui astfel de instrument pentru a elimina necesitatea stocării documentelor în format fizic pentru semnarea acestora sau a imprimării copiilor. Deși șaizeci dintre participanți dețin în prezent acces la semnătura electronică, iar alți nouă au utilizat în trecut acest instrument, dorim să aflăm opinia tuturor participanților vizavi de utilitatea unui astfel de certificat. Observăm cum, aproximativ 60% dintre contribuabilii care au efectuat chestionarul afirmă despre semnătura electronică faptul că aceasta elimină complet necesitatea stocării documentelor semnate și a copiilor de rezervă, precum și a imprimării fiecărui document în vederea semnării. Alți contribuabili, în proporție de 31,3% sunt de părere că utilizarea semnăturii electronice reduce necesitatea stocării și imprimării documentelor semnate, dar nu o elimină complet. Patru entități nu sunt sigure dacă utilizarea semnăturii electronice elimină această necesitatea sau nu, în timp ce alte trei entități neagă eliminarea necesității stocării documentelor semnate și a copiilor de rezervă, precum și a imprimării documentelor pentru semnare în totalitate.

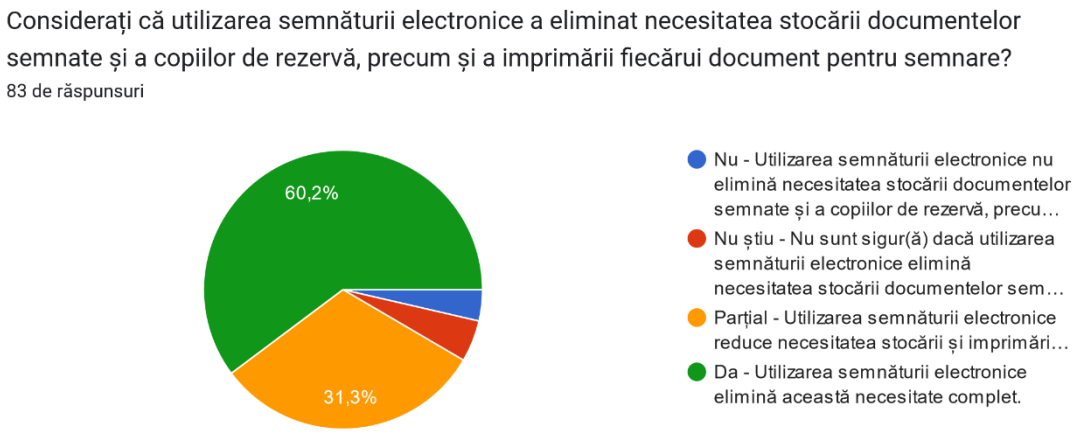


Fig. 21. A cincisprezecea întrebare din chestionar
Sursa: Google Forms

- Opinia dumneavoastră în privința utilității facturilor electronice (e-facturi) în relația cu ANAF este una…:

Aceasta a fost cea de a șaisprezecea întrebare din cadrul chestionarului, fiind și ultima întrebare prin care ne-am dorit să aflăm dacă încă unul din serviciile puse la dispoziție de ANAF ajută la creșterea eficienței instituției. Am folosit ca variante de răspuns metoda scării liniare, de la 1 la 5, unde 1 reprezintă o atitudine foarte negativă vizazi de utilitatea e-facturii, iar 5 reprezintă varianta de răspuns diametral opusă, sugerând o atitudine foarte pozitivă față de un astfel de serviciu, precum cel al facturii electronice. În urma colectării răspunsurilor, patru entități folosesc ca variantă de răspuns treapta unu, sugerând astfel o atitudine foarte negativă vizavi de utilitatea e-facturii în relația dintre aceștia și ANAF. Pe următoarea treaptă, treapta numărul doi, nu am identificat niciun răspuns. Urcând la cea de a treia treaptă, observăm un cumul de treisprezece voturi. Acestea sugerează o atitudine neutră vizavi de un astfel de serviciu, precum e-factura, fiind indiferenți de o astfel de tematică abordată. În continuare, aproximativ 30% din numărul participanților au ales ca variantă de răspuns treapta numărul patru, sugerând atitudinea lor pozitivă în privința utilității facturilor electronice în relația cu ANAF, lăsând impresia că există loc de îmbunătățiri. Cea mai mare majoritate, constă în aproximativ jumătate din totalul contribuabililor supuși chestionarului (49,4%) care s-au situat pe treapta numărul cinci, cea care sugerează atitudinea acestora foarte pozitivă față de serviciile de e-factură, considerând că un astfel de serviciu este extrem de util și eficient în relația dintre ANAF și contribuabili.

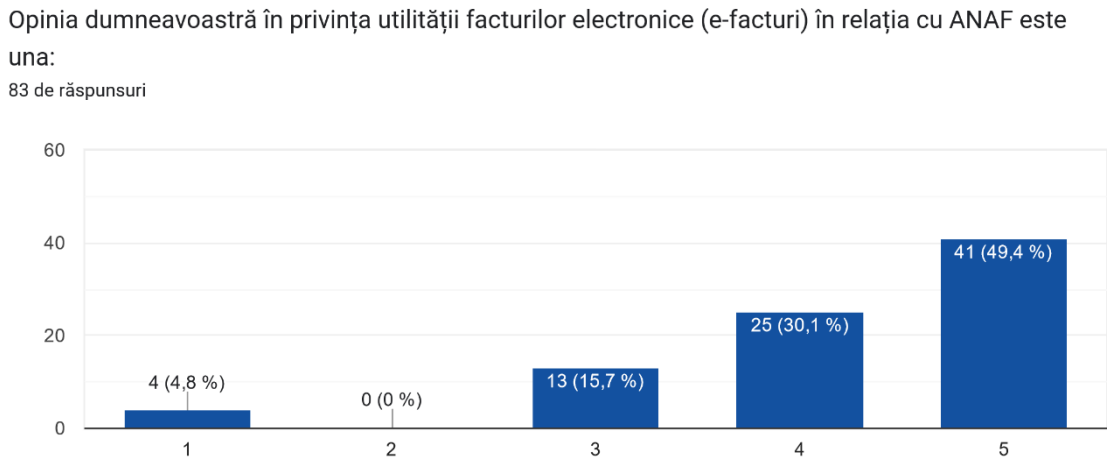


Fig. 20. A șaisprezecea întrebare din chestionar
Sursa: Google Forms

Discuții / Concluzii

În urma studiului de caz privind transformarea digitală în administrația fiscală și a analizei chestionarului asupra transparenței și eficienței ANAF, concluzionăm că ipotezele de cercetare pe care ni le-am propus au fost valide. Digitalizarea instituțiilor de nivel central, în speță ANAF, contribuie la îmbunătățirea calității guvernării statale, prin creșterea eficienței operaționale și a transparenței în relația cu cetățenii.

Astfel, contribuabilii ANAF afirmă în mare măsură că utilizarea e-facturii poate simplifica și automatiza procesele de facturare și raportare, reducând erorile și timpul necesar pentru gestionarea documentelor fiscale. Totodată, apariția „Spațiului Privat Virtual" a eficientizat modul de depunere al declarațiilor fiscale, simplificând demersurile birocratice. Studiul de caz a arătat că utilizarea eficientă a tehnologiilor digitale poate genera o transparență sporită între

ANAF și contribuabili, prin distribuirea informațiilor fiscale și a proceselor decizionale. Observăm cum peste jumătate din contribuabilii care au luat parte în cadrul chestionarului au sugerat un nivel de transparență ridicată între instituțiile de nivel central (în speță ANAF) și aceștia, fiind mulțumiți în mare măsură de serviciile puse la dispoziție de Agenția Națională de Administrare Fiscală. Aceste servicii au clădit un nivel ridicat de transparență prin furnizarea informațiilor de natură fiscală către cetățeni, prin diverse căi de comunicare.

Toate aceste aspecte nu ar fi fost realizabile fără implicarea directă a digitalizării în cadrul proceselor decizionale de natură să stabilizeze și să îmbunătățească serviciile ANAF, oferind o mai bună calitate a serviciilor guvernamentale pentru cetățeni. Digitalizarea instituțiilor de nivel central subliniază procesul și evoluția acestora pentru sporirea calității guvernării statale. În ultimii ani, digitalizarea a avut un impact puternic, atât pentru eficientizarea guvernării, cât și în transparența statului în relația cu cetățenii.

Procesul de digitalizare a instituțiilor centrale, inclusiv ANAF, vine cu numeroase avantaje, dar și cu anumite riscuri care trebuie gestionate eficient. Printre garanțiile oferite de digitalizare se numără creșterea eficienței operaționale, reducerea costurilor administrative și îmbunătățirea accesului la servicii pentru cetățeni. Cu toate acestea, tranziția către un mediu digital ridică provocări semnificative legate de securitatea cibernetică și protecția datelor.

Una dintre cele mai mari provocări ale digitalizării este asigurarea protecției și securității datelor personale ale contribuabililor. Instituțiile de nivel central, și nu numai, au responsabilitatea de a implementa măsuri de securitate cibernetică pentru a proteja informații sensibile sau cu o importanță deosebită împotriva amenințărilor cibernetice. Aceste măsuri includ criptarea datelor, implementarea de protocoale de autentificare multi-factor și monitorizarea continuă a sistemelor pentru a detecta și preveni atacurile cibernetice.

Astfel, amenințările cibernetice reprezintă un risc semnificativ pentru instituțiile digitalizate. Atacurile de tip phishing, ransomware și breșele de securitate pot compromite datele instituțiilor și ale cetățenilor, precum integritatea sistemelor și a bazelor de date. Tocmai de aceea, este important ca instituțiile guvernamentale să adopte o strategie complexă de securitate cibernetică, care să includă măsuri de prevenire, detectare și securitate sporită împotriva unor astfel de atacuri.

Amintim pe această cale de necesitatea reglementării digitalizării administrației publice printr-un cadru legislativ specific care să stabilească standardele și cerințele pentru protecția datelor și securitatea informațiilor. Respectarea acestor reglementări este fundamentală pentru asigurarea conformității și protejării drepturilor cetățenilor. Instituțiile trebuie să se asigure că implementarea tehnologiilor digitale este aliniată cu reglementările naționale și internaționale privind protecția datelor.

Transformarea digitală a instituțiilor de nivel central, precum ANAF, demonstrează impactul semnificativ asupra eficienței și transparenței proceselor fiscale. Utilizarea e-facturii, semnăturii digitale și a „Spațiului Privat Virtual" a simplificat interacțiunea contribuabililor cu instituțiile fiscale, reducând birocrația și crescând accesibilitatea serviciilor fiscale. Rezultatele studiului confirmă că digitalizarea contribuie la îmbunătățirea calității serviciilor guvernamentale, oferind cetățenilor o experiență mai eficientă și mai transparentă. De asemenea, eficiența transformării digitale depinde de gestionarea adecvată a riscurilor și de asigurarea securității datelor. ANAF și alte instituții de nivel central trebuie să rămână vigilente în fața amenințărilor cibernetice și să adopte practici riguroase de protecție a datelor pentru a menține încrederea cetățenilor și a îmbunătăți continuu calitatea serviciilor oferite.

Cu toate acestea, procesul de digitalizare nu este lipsit de provocări. Este important ca instituțiile publice să adopte măsuri adecvate pentru a proteja datele personale ale cetățenilor și pentru a preveni amenințările cibernetice. Investițiile în securitatea cibernetică și formarea

personalului în domeniul protecției datelor sunt necesare pentru a asigura un mediu digital sigur și de încredere.

Astfel, concluzionăm că transformarea digitală a instituțiilor de nivel central reprezintă un pilon principal pentru modernizarea administrației publice, aducând beneficii substanțiale atât pentru instituții, cât și pentru cetățeni. Este esențial să continuăm să investim în tehnologii digitale și în securitate cibernetică pentru a asigura un mediu guvernamental eficient, transparent și sigur pentru toți cetățenii.

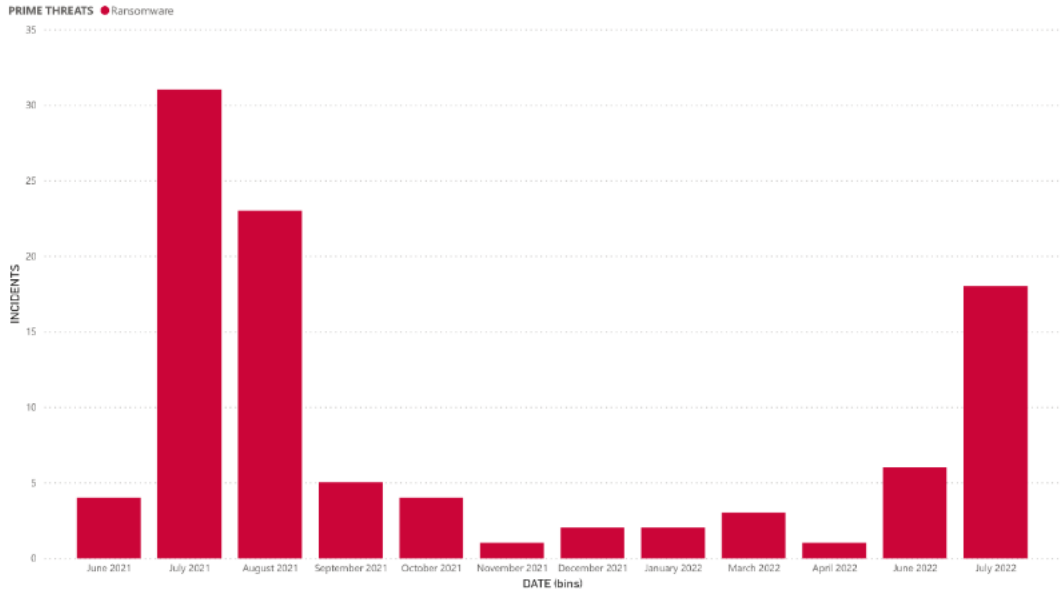
Anexa A. Figuri utilizate în cadrul lucrării

Indicator / changes, %	2019/2018	2020/2019	2021/2020
paper sheets, number	-8,2%	-14,1%	-58,9%
price of 1 box [1], EUR	0,7%	-2,1%	2,0%
total paper, EUR	-7,2%	-16,1%	-57,6%
printing equipment, EUR	-51,5%	-3,4%	-17,3%
digital equipment, EUR	-16,1%	-21,3%	71,1%
digital platforms, EUR	3,4%	188,4%	101,6%
number of pupils	8,0%	2,3%	-1,0%
paper, EUR per pupil	-14,0%	-18,0%	-57,2%
paper, sheets per pupil	-14,9%	-16,0%	-58,5%
digital platforms, EUR per pupil	-4,2%	182,0%	103,6%
number of employees	2,0%	4,0%	1,2%
paper, EUR per employee	-9,0%	-19,4%	-58,2%
paper, sheets per employee	-9,9%	-17,4%	-59,4%

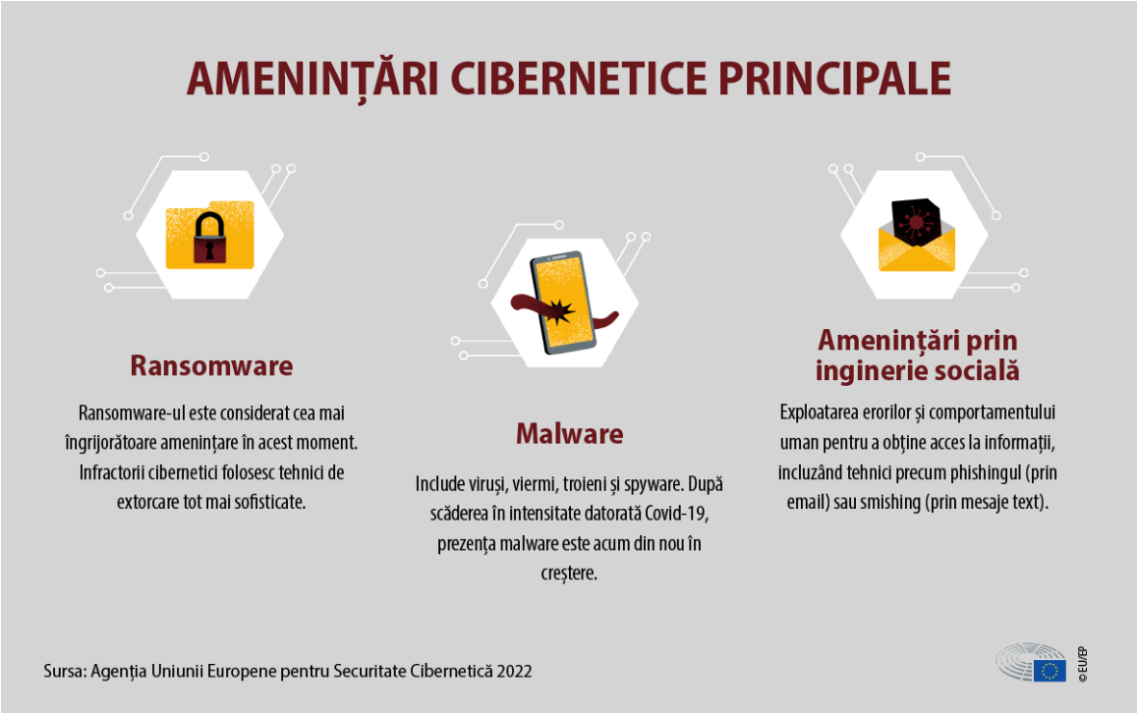
A.1. Comparația consumului de hârtie, a numărului de angajați și a numărului de accesări de platforme digitale în cadrul instituțiilor publice raporte între anii 2018-2019, 2019-2020 și 2020-2021.
Sursa: Proceedings of the 11th International Scientific Conference Rural Development 2023 - The Use Of Paper In The Era Of Digitalization

A.2. Principalele amenințări ale atacurilor cibernetice
Sursa: ENISA - Perspectiva atacaturilor 2022 (iulie 2021 – iulie 2022)

nex

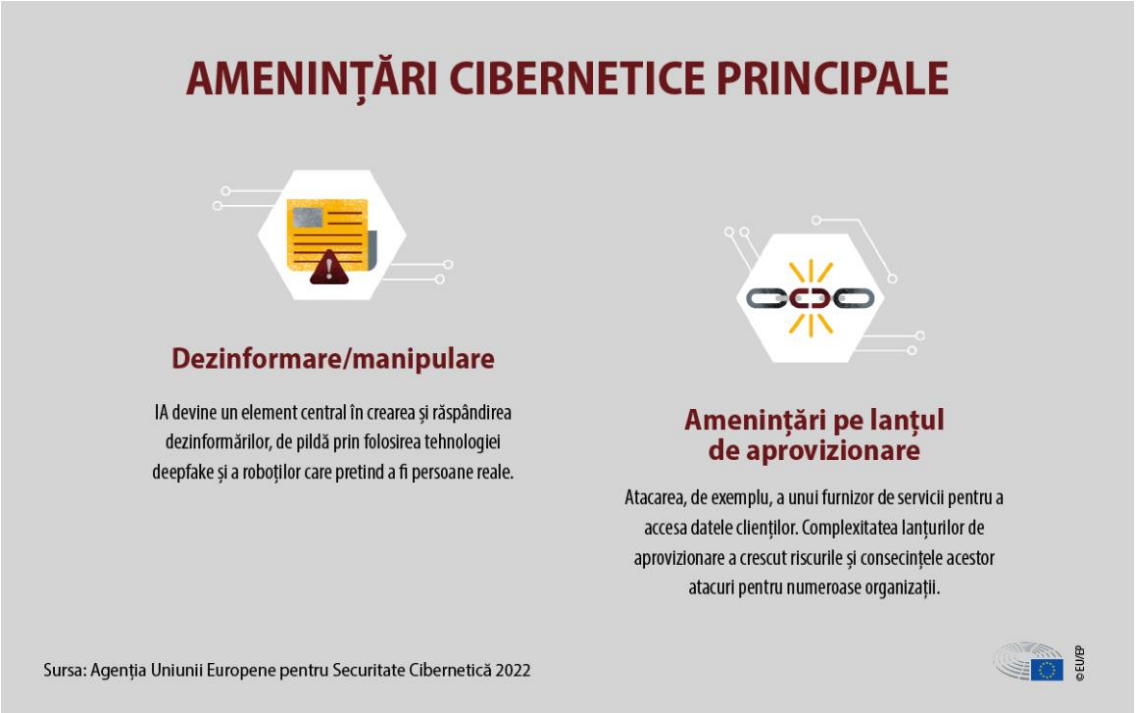


A.3. Incidente majore observate de ENISA în ordine cronologică (iunie 2021 – iulie 2022)
Sursa: ENISA - Perspectiva atacaturilor 2022 (iulie 2021 – iulie 2022)

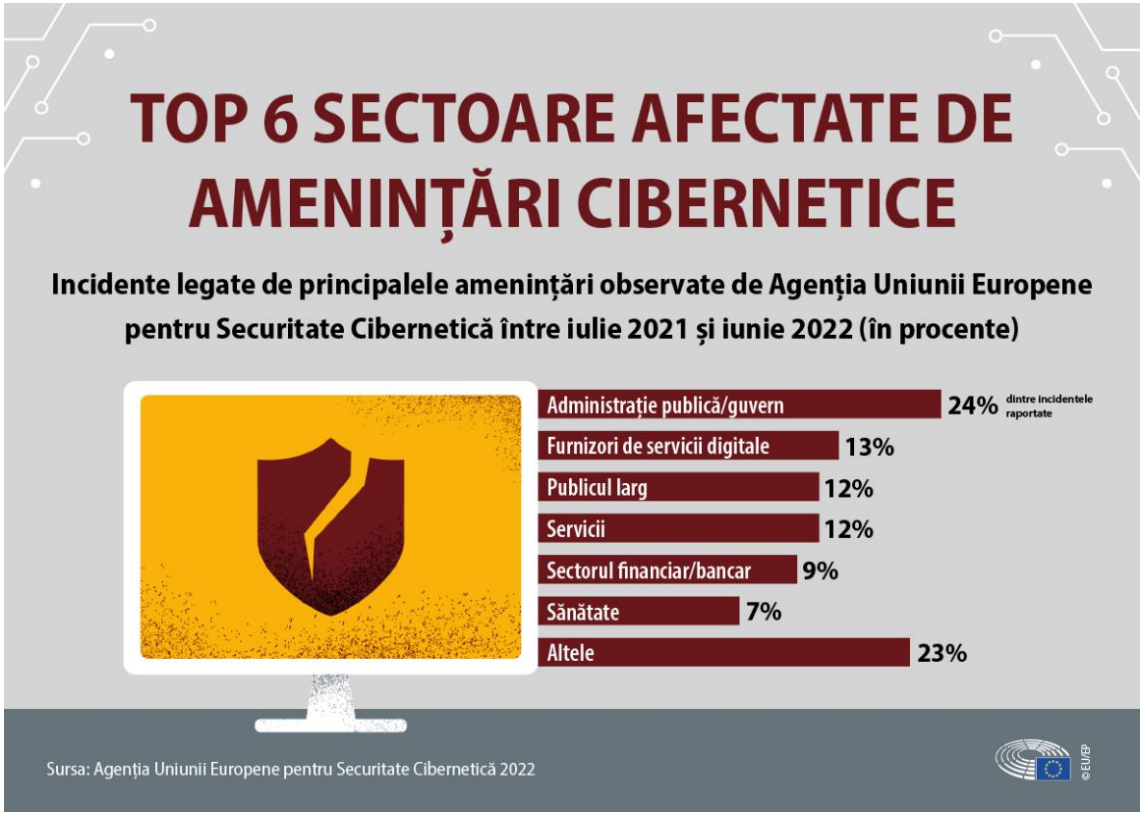


A.4. Primele trei amenințări cibernetice principale
Sursa: Parlamentul European - Securitate cibernetică: principalele amenințări

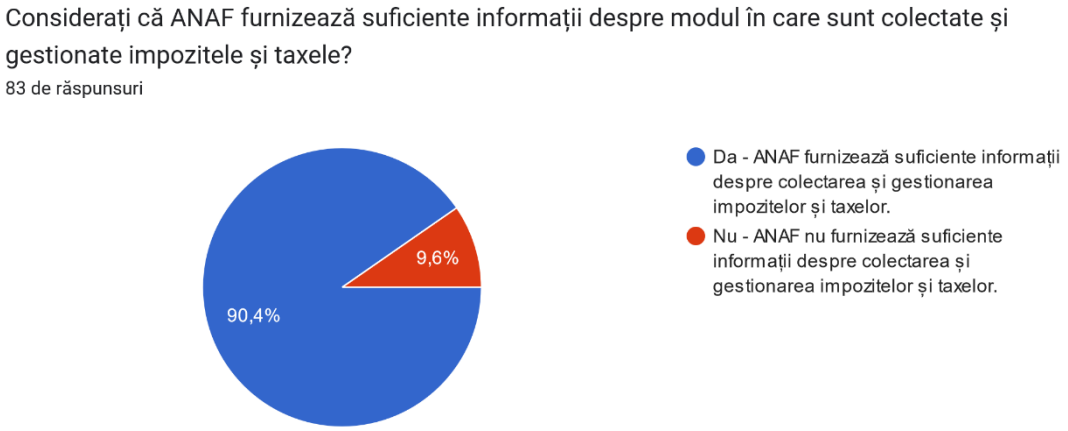
A.5. Următoarele trei amenințări cibernetice principale
Sursa: Parlamentul European - Securitate cibernetică: principalele amenințări



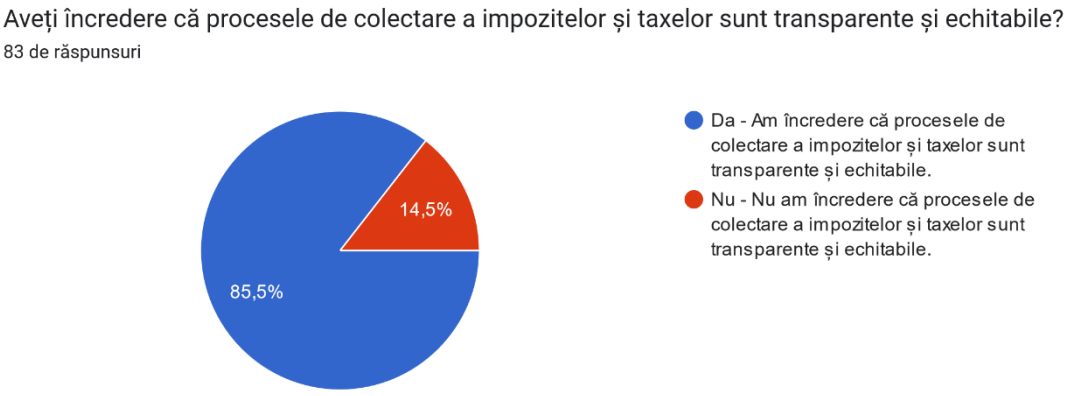
A.6. Celelalte două amenințări cibernetice principale
Sursa: Parlamentul European - Securitate cibernetică: principalele amenințări



A.7. Topul sectoarelor afectate de amenințări cibernetice
Sursa: Parlamentul European - Securitate cibernetică: principalele amenințări



A.8. A opta întrebare din chestionat
Sursa: Google Forms



A.9. A noua întrebare din chestionar
Sursa: Google Forms

References

[1] D. R. E. Online. [Interactiv]. Available: https://www.dictionarroman.ro/?c=calculator. [Accesat 20 01 2024].

[2] V. Baltac, Lumea Digitală. Concepte esențiale, EXCEL XXI BOOKS, 2015, p. 4.

[3] V. Baltac, Mituri si realitate in lumea digitala. Blog, comentarii eseuri, EXCEL XXI BOOKS, 2016, p. 13.

[4] B. Mondiala, The e-government handbook for developing countries., 2002, pp. 5-10.

[5] O. Hughes, Public Management & Administration. Conclusion. A New Paradigm for Public Management. Macmillan, 2003, p. 182.

[6] E. D. Cătălin Vrabie, Smart Cities. De la idee la implementare sau despre cum tehnologia poate da strălucire mediului urban, Universul Academic & Universitara, 2019, p. 17.

[7] ANAF, „Raport de activitate ANAF semestrul 1 2023," 2023. [Interactiv]. Available: https://static.anaf.ro/static/10/Anaf/Informatii_R/Raport_activitate_ANAF_semI2023.pdf. [Accesat 15 01 2024].

[8] „SISTEMUL NAȚIONAL RO e-Factura," [Interactiv]. Available: https://mfinante.gov.ro/ro/web/efactura. [Accesat 15 01 2024].

[9] K. C. Viktor Mayer Schonberger, Big Data: A Revolution That Will Transform How We Live, Work, and Think, 2014, p. 145.

[10] M. Pelse, L. Strazdina și S. Ancans, „Digitalization in public administration institutions," în *International Conference „ECONOMIC SCIENCE FOR RURAL DEVELOPMENT"*, 2021.

[11] J. Gleick, The Information: A History, A Theory, A Flood, Knopf Doubleday Publishing Group, pp. 144-145.

[12] C. Vrabie, Elemente de E-Guvernare, Pro Universitaria, 2016, p. 81.

[13] The Email Revolution: Unleashing the Power to Connect, Shiva Ayyadurai, 2013, p. 35.

[14] ANAF, „Spațiul Privat Virtual," 2015. [Interactiv]. Available: https://static.anaf.ro/static/10/Anaf/Informatii_R/Tutorial_SPV_10feb2015v2.pdf.

[15] „adr.gov.ro," [Interactiv]. Available: https://www.adr.gov.ro/ghiseul-ro/. [Accesat 29 02 2024].

[16] „Licitații SEAP," [Interactiv]. Available: https://licitatiiseap.ro/seap/. [Accesat 01 03 2024].

[17] G. Diana, Ce este Guvernarea Electronică?, 2006, p. 3.

[18] C. Baesu, Digitalization of Public Administration in Romania, vol. XXI, 2021, p. 215.

[19] PWC, „Studiu privind implementarea Guvernării Digitale în România," p. 30, 2018.

[20] A. Guțu, Importanța Debirocratizarii și digitalizării administrației publice, 2022, pp. 62-64.

[21] V. Anghel, E-guvernare - Transparență și Eficiență, 2015, p. 413.

[22] M. Finanțelor, „Comunicate de presă,” 2023. [Interactiv]. Available: https://mfinante.gov.ro/despre-minister/-/asset_publisher/uwgr/content/facturarea-electronic-c4-83-obligatorie-de-la-1-ianuarie-2024-pentru-toate-tranzac-c8-9biile-c3-aentre-firme. [Accesat 17 03 2024].

[23] C. Europeană, „eGovernment Benchmark 2020,” 2020.

[24] C. Europeana, „Digital public services,” în *Digital Economy and Society Index (DESI)* , 2020.

[25] B. Tomlinson, Greening through IT: Information Technology for Environmental Sustainability, 2012, pp. 103-112.

[26] R. Kupcs, „The Use Of Paper In The Era Of Digitalization,” în *Proceedings of the 11th International Scientific Conference Rural Development*, 2023.

[27] A. M. Townsend, Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia, 2013, pp. 180-190.

[28] T. Erkkila, „Transparency in Public Administration,” 2020.

[29] B. C. L. C. S. J. S. J. T. Martin Alessandro, „Transparency and Trust in Government. Evidence from a Survey Experiment,” în *World Development*, 2021.

[30] O. K. Foundation, „Open Data Handbook,” [Interactiv]. Available: https://opendatahandbook.org/guide/ro/what-is-open-data/. [Accesat 20 03 2024].

[31] A. p. D. R. (A.D.R.), „Sistemul Electronic de Achiziții Publice (SEAP),” [Interactiv]. Available: https://www.e-licitatie.ro/pub/staticpages/Legal. [Accesat 22 03 2024].

[32] „Dicționarul explicativ al limbii române (DEX),” [Interactiv]. Available: https://dexonline.ro/definitie/hacker.

[33] C. Europeană, „Protecția datelor în UE,” [Interactiv]. Available: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_ro. [Accesat 01 04 2024].

[34] G. României, „HOTĂRÂRE nr. 585 din 13 iunie 2002,” [Interactiv]. Available: https://legislatie.just.ro/Public/DetaliiDocument/37319. [Accesat 02 04 2024].

[35] P. European, „Securitate cibernetică: principalele amenințări,” [Interactiv]. Available: https://www.europarl.europa.eu/topics/ro/article/20220120STO21428/securitate-cibernetica-principalele-amenintari. [Accesat 07 04 2024].

[36] ENISA, „THREAT LANDSCAPE FOR RANSOMWARE ATTACKS,” 2022.

[37] ENISA, „THREAT LANDSCAPE 2022 (July 2021 to July 2022),” 2022.

[38] L. Sadoian, „Guarding Governance: Cybersecurity in the Public Sector”.

[39] „Informații generale despre NIS (Legea 362/2018),” Directoratul Național de Securitate Cibernetică.

[40] „LEGE nr. 362 din 28 decembrie 2018 (privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice),” Parlamentul României.

[41] „LEGE nr. 9 din 4 ianuarie 2023,” Parlamentul României.

[42] „Legea 9/2023: Reducerea Birocrației și Încurajarea Digitalizării în Instituțiile Publice,” [Interactiv]. Available: https://www.certificatconstatatoronline.ro/articole/reducerea-birocratiei-legea-9-2023-certificat-constatator/. [Accesat 15 04 2024].