Școala Națională de Studii Politice și Administrative
Facultatea de Administrație Publică

PROTECȚIA DATELOR CU CARACTER PERSONAL ÎN ADMINISTRAȚIA PUBLICĂ ÎN CONTEXTUL SIGURANȚEI NAȚIONALE

- lucrare de licență, specializarea Administrație Publică -

Coordonator

Conf. Univ. Dr. Cătălin VRABIE

Absolventă

Stanciu Cristiana

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: Stanciu Cristiana

Data și semnătura: 05.12.2023

Cuprins

Template redactare lucrare licență / disertație (A se citi cu atenție!!)

Abstract

Protecția datelor cu caracter personal în administrația publică reprezintă un pas important în evoluția digitalizării din România, astfel că această lucrare se concentrează asupra investigării și înțelegerii profunde a modalităților de colectare și protecție a informațiilor personale într-un context administrativ. De asemenea, este mai mult decât necesară o atenție sporită asupra modului în care acestea sunt păstrate, în paralel cu evaluarea nivelului de informare al cetățenilor cu privire la acest proces complex. În conformitate cu cercetările consacrate în SCRD JOURNAL, avansările recente din punct de vedere tehnologic conturează un cadru în care accesul la datele personale devine din ce în ce mai imperativ pentru a facilita recunoașterea cetățenilor în diverse contexte impuse de serviciile publice. Abordarea metodologică adoptată se caracterizează prin utilizarea unui sondaj de opinie extins, strategic construit pentru a evalua gradul de conștientizare al cetățenilor în ceea ce privește datele personale colectate de către entitățile administrației publice. Rezultatele obținute prin această cercetare furnizează o perspectivă esențială asupra impactului tehnologiei asupra cetățenilor și ilustrează nivelul de documentare al acestora în ceea ce privește gestionarea propriilor date confidențiale. Această analiză comprehensivă aduce o contribuție semnificativă la înțelegerea situației actuale din administrația publică din România, oferind, în același timp, o reflexie detaliată asupra optimizării strategiilor de protecție a informațiilor cu caracter personal, fără a ignora potențialele riscuri de scurgeri de date. Implicarea cetățenilor în acest proces devine astfel esențială pentru consolidarea unui cadru eficient și etic de protecție a datelor cu caracter personal.

Cuvinte cheie: confidențialitate informațională, scurgeri de date, strategii de securitate informațională

Introducere

Într-o societate modernă în care tehnologia și schimbul de informații sunt utilizate din ce în ce mai des, devenind indispensabile și considerate fiind coloana vertebrală a comunicării *on-line*, nevoia de a securiza informațiile personale stocate pe un anumit dispozitiv devine, cu precădere, un subiect de neignorat. Cum dispozitivele sunt protejate de anumite programe sau aplicații dezvoltate în acest sens și care oferă protecție în funcție de nevoia exprimată, la fel și instituțiile publice își exprimă mai mult și mai mult necesitatea de a dezvolta programe performante de prevenire a scurgerilor de date sau a atacurilor cibernetice în acest sens. Pentru a echilibra balanța – protecția datelor cu caracter personal din punct de vedere legal, lucrarea își propune să concretizeze importanța prevenirii amenințărilor la adresa securității naționale, cât și să crească gradul de informare al cetățenilor cu privire la procesul de colectare și stocare al datelor introduse ulterior într-un anumit tip de document cerut de o entitate publică a statului român.

Administrația publică din România dispune de o aparatură informatică în majoritatea instituțiilor, utilizată pentru diferitele nevoi ale cetățenilor. Din aceasta rezultă și faptul că informațiile cu caracter personal colectate sunt într-un număr mare și, totodată în continuă creștere și deși administrației publice îi revine rolul de a gestiona aceste informații într-un mod responsabil bazat pe un cadru legal reglementat prin *Regulamentul General privind Protecția Datelor*, nu poate prevedea posibile atacuri sau scurgeri de date. Astfel, legislația privind protecția datelor cu caracter personal – cu precădere într-un cadru atât de complex, fiind vorba de instituții publice ale statului, devine o componentă esențială a unui context legal coerent și adaptat la provocările unei societăți avansate din punct de vedere tehnologic și informațional.

Nu este de ignorat relația strânsă dintre protecția datelor cu caracter personal și securitatea națională într-o eră aflată în continuă dezvoltare a tehnologiei informației la nivel global. Amenințările la adresa securității se dovedesc a fi din ce în ce mai sofisticate și mai atent lucrate de atacatori, astfel că s-a dovedit că autoritățile se văd nevoite să utilizeze date cu caracter personal pentru a anticipa și pentru a contracara potențiale riscuri. Este de la sine înțeles faptul că această abordare trebuie pusă în practică având o deosebită atenție asupra personalului care gestionează aceste informații – în primul rând pentru a menține un echilibru între necesitățile de securitate națională și respectarea drepturilor și libertăților fundamentale ale cetățenilor cărora li s-au colectat ulterior anumite date sensibile cu potențial risc de scurgere către terțe părți. Și cum societatea se cunoaște ca fiind guvernată de democrație și transparență, este imperios necesară consolidarea unui cadru tehnic pentru acest domeniu ce utilizează datele personale zilnic.

Lucrarea își propune să analizeze în același timp și lacunele pe care le dețin atât entitățile publice care colectează aceste date cu caracter personal, cât și lacunele cetățenilor cu privire la gradul de cunoaștere al procesului de stocare al datelor. Nu sunt de ignorat nici bunele practici de păstrare a acestor date, întrucât autoritățile pot utiliza datele personale în mod legal și legitim în scopul consolidării securității naționale, respectând în același timp principiile de confidențialitate și protecție a drepturilor individuale, la fel cum am menționat anterior. Analiza se concentrează pe aducerea unei contribuții semnificative la modelarea unei viziuni asupra sistemului informațional prezent astăzi în administrația publică, dar și asupra relației dintre securitatea datelor cu caracter personal și protecția acestora, având în vedere nevoile imperioase ale unei societăți moderne în tandem cu complexitatea amenințărilor posibile din partea atacatorilor experimentați din domeniu.

Pe de altă parte, educația cetățenilor în acest sens ridică un mare semn de întrebare autorităților cibernetice – necunoștința de cauză, semnarea documentelor pentru acordul folosirii datelor personale, ori pur și simplu navigatul pe internetul larg fără un program de protecție a acestora poate contribui la un mediu propice pentru atacatori în ceea ce privesc scurgerile de date. Nu este exclus ca dintr-un singur click eronat pe un banner neconform, site neconform sau link-uri infectate cu malware-uri parolele, adresele, datele unui card de credit utilizat anterior pentru cumpărături online, sau chiar adresa personală a locuinței să fie compromise și să conducă spre o instituție – fie publică sau privată cu scopul infectării și scurgerii datelor respective și din acele spații.

Este imperativ să se întreprindă eforturi susținute pentru a facilita informarea cetățenilor cu privire la modul în care datele lor sunt colectate, stocate și utilizate de către administrația publică în acest context al securității naționale. Îmbunătățirea nivelului de conștientizare al cetățenilor asupra acestor aspecte conduce la alcătuirea unei relații mai transparente și a unei încrederi reciproce între instituțiile statului și cetățenii țării.

Analizând atent modalitățile prin care autoritățile pot comunica eficient cu cetățenii și, bineînțeles, pot asigura transparența în procesul de colectare al datelor cu caracter personal, putem afirma că la finalul zilei cetățenii pot confirma că vor alege și următoarea dată serviciile entităților publice cunoscând și cadrul legal reglementat. Importanța implicării active a acestora în procesul de colectare al datelor constă în o mai bună dezvoltare a manierelor de gestionare informațională și – implicit la încrederea acestora că datele nu le vor fi compromise sau furate.

Așadar, în paralel cu dezvoltarea unui cadru legal tehnic și robust, ținând cont de reglementările în vigoare se va accentua necesitatea investirii în programe educaționale și campanii de informare pentru asigurarea faptului că cetățenii se pot implica activ în procesul de păstrare al datelor lor, fapt ce nu doar că va spori gradul de conștientizare, însă va consolida și legătura dintre aceștia și entitățile publice desemnate să lucreze cu datele sensibile ale acestora. Este important faptul că în zilele noastre, chiar și un simplu formular, ori o simplă cerere adresată unui director de unitate sau șef de departament poate fi compromisă, întrucât cineva o semnează, altcineva o primește și o înregistrează, creându-se un lanț prin care securitatea dacă nu este foarte bine pusă la punct – va suferi atacuri și scurgeri de date nedorite.

Context

Analiza acestei lucrări se concentrează pe înțelegerea și aprofundarea colectării datelor cu caracter personal de către entitățile administrative cetățenilor într-un context guvernat de circulația masivă a datelor și informațiilor personale. Este de subliniat faptul că majoritatea informațiilor personale sunt preluate din cererile tip adresate publicului, într-un procent deosebit de mic constând datele preluate din mediul on-line – implicit cu ajutorul software-urilor instituțiilor de stat. Reglementările în vigoare, legile din domeniul apărării cibernetice sau hotărârile luate în acest sector vor scoate în evidență necesitatea sporirii protecției împotriva unor scurgeri de date neprevăzute. De asemenea, nu este de neglijat faptul că cetățenii ce

completează cererile care conțin date personale precum adresă, număr de telefon, extras de cont, ș.a.m.d. nu cunosc în totalitate procesul de stocare a acestora de către entitatea colectoare. Lucrarea analizează modul de stocare, colectare și completare, cât și observarea gradului de protecție al acestora. Se va pune accentul pe gradul de informare al cetățenilor cu privire la acest proces de colectare, inclusiv protecția datelor și va accentua nivelul de pregătire al instituțiilor din diverse județe ale României în acest domeniu pentru a pune în evidență o mai bună abordare a acestor cunoștințe. Totodată, în contextul siguranței naționale – strâns legat de cadrul legal aflat în vigoare, se poate pune problema unor noi tehnologii de adaptare la o mai amplă strategie de protecție a datelor personale colectate, precum și modalitățile protejate prin care cetățenii aleg să completeze voluntar aceste date sensibile din punct de vedere tehnic. În lumina acestui context, este vital să se acorde o atenție sporită și specială și educației cetățenilor în acest sens, întrucât este dovedit că aceștia nu sunt suficient de informați.

Capitolul 1. Progresul digitalizării administrației publice.

În contextul evoluției României în gestionarea informațiilor de-a lungul timpului, este important să evidențiem că țara a parcurs un drum semnificativ, adaptându-se la schimbările politice și sociale dramatice. În perioadele marcate de războaie și regimuri totalitare din secolul trecut, protecția datelor sensibile și confidențiale a reprezentat o prioritate majoră, fiind gestionată cu profesionalism și rigurozitate pentru a asigura securitatea informațiilor de interes public. O transformare semnificativă s-a produs odată cu tranziția către democrație, deschizând calea către o mai mare transparență în guvernare și acces public sporit la informații. Această schimbare a contribuit la crearea unui mediu mai deschis și democratic, unde cetățenii beneficiază de o mai mare accesibilitate și înțelegere a informațiilor oficiale. [1]

De asemenea, digitalizarea Administrației Publice a reprezentat un alt punct de cotitură în evoluția României la nivel informațional. Prin implementarea tehnologiilor informatice în cadrul instituțiilor guvernamentale, s-a construit un fundament solid pentru un sistem digital modern. Acest lucru a condus la optimizarea proceselor administrative și la îmbunătățirea accesului public la serviciile și informațiile oferite de stat. [1]

Evoluția digitalizării a constat în gestionarea informațiilor care reflectă un parcurs complex și adaptabil la cerințele timpului, trecând de la o strictă protecție a datelor sensibile în perioadele istorice dificile la o deschidere către transparență și accesibilitate în această eră digitală [2]. Aceste transformări au contribuit la modernizarea structurilor guvernamentale și la îmbunătățirea relației dintre stat și cetățeni, promovând o guvernare mai eficientă și responsabilă [2].

România a parcurs o evoluție remarcabilă în gestionarea informațiilor și în adoptarea tehnologiilor digitale în administrația publică. Aceste progrese au contribuit la consolidarea transparenței și a responsabilității în guvernare, oferind cetățenilor un mediu mai deschis și mai participativ. Evoluția s-a caracterizat prin nevoile infinite în paralel cu resursele finite ale țării, aspect reglementat prin adoptarea și implementarea Regulamentului General privind Protecția Datelor sub egida Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal înființată în anul 2005, conform Legii 102. [3]

1.1. Parcursul colectării datelor personale: Evoluția de-a lungul timpului

Să presupunem că începem analiza odată cu primii ani ai secolului XX. Firește că în lipsa oricărui device performant, funcționarii publici utilizau metode manuale tradiționale de colectare a datelor personale prin prisma simplelor coli albe și a cernelii. Înțelegem, de aici, că atât procesul de stocare și cel de arhivare era unul anevoios, neavând soft-uri care să sorteze datele, de exemplu, în ordine alfabetică. De aici apar și anumite situații neplăcute, din punct de vedere legal și tipuri de infracțiuni care scot în evidență lipsa digitalizării într-un secol care era dominat de putere, autoritate și propagandă. Bineînțeles că rezolvările nu au întârziat să apară,

însă amprenta acestor fapte care contraveneau legilor de atunci și de acum se resimte la nivel național.

Dacă astăzi utilizatorii internetului cunosc faptul că fiecare acțiune on-line este de natură să producă efecte (atât vizibile, cât și invizibile) [4], în trecut cetățenii mizau pe încrederea pe care organele de stat o confereau prin mijloace de autoritate. Desigur că se cunoaște – prin viu grai (transferul de informații de la o persoană la cealaltă de-a lungul timpului) faptul că în trecut, atunci când o persoană influentă de rang înalt din societate dorea să obțină informații cruciale referitor la o anumită familie sau o anumită persoană care cauza probleme, ori prezenta interes de natură politică, mergea la administrația publică locală a orașului din care făcea parte. Cadrul favorabil din trecut datorat de lipsurile tehnologice oferea un context prielnic înalților funcționari publici pentru oferirea informațiilor cu caracter personal ale unei anumite terțe părți în schimbul unor sume de bani considerabile sau obiecte valoroase.

Totodată, nu este de ignorat nici faptul că furtul de identitate tocmai prin aceleași metode utilizate în secolul XX, a generat o controversă în rândul societății la nivel internațional. Atât în România, cât și în alte țări, indivizii obișnuiau să intre în posesia unor informații sensibile ale altora: nume, prenume, adresa de domiciliu, numele copiilor, numele părinților, soțului/ soției ș.a.m.d. pe care mai apoi și le atribuiau, din cauza faptului că aveau antecedente penale și teama de condamnare era tot mai des întâlnită [5]. Odată cu această problemă s-a evidențiat nevoia existenței unui sistem de recunoaștere biometrică a individului în cauză care se înfățișa la instituțiile de stat abilitate ale apărării naționale pentru o faptă/ fapte contra legii comisă/e anterior. Într-adevăr, la începutul secolului XX s-au înregistrat primele încercări de a captura un infractor prin intermediul amprentelor digitale la locul crimei [6], însă neconcordanța cu standardele impuse ale fiecărui stat și xenofobia au condus la nenumărate polemici în domeniul cercetării legale – paradoxal, atât din lipsa informațiilor personale ale cetățenilor implicați în cazuri penale, cât și din cauza abundenței acestora. Astfel, a luat naștere în anul 1985 sistemul amprentelor genetice sub umbrela academică a descoperirii lui Alec Jeffreys care făcea legătura dintre schema complexă a acidului dezoxiribonucleic (ADN) cu cea a amprentelor digitale [7].

În România, amprentele genetice au apărut ca urmare unui caz de crimă cu premeditare a unui copil în anul 2003, eveniment ce a dus la finalizarea și soluționarea altor dosare. Fiind un punct de cotitură ca urmare unui eveniment destul de tragic, această evoluție ne reamintește cât de important este să ținem cont de orice detaliu mărunt în lucrul cu datele, cu atât mai mult – cu datele din administrația publică. Într-un articol din Revista Nature, Andrew Watson afirmă că datele biometrice sunt de departe cea mai utilă metodă în identificarea unui individ, chiar dacă acesta pretinde a fi o cu totul altă persoană [8] cu absolut toate faptele care corespund unui furt de identitate.

Furtul de identitate este o infracțiune bine-cunoscută, probabil încă de la începuturi. De ce este crucial să amintim de aceasta? Pentru că dacă am fi puși în situația în care în zilele noastre, unde mediul online este din ce în ce mai complex și de dezvoltă consistent de la o zi la alta, am descoperi faptul că nu putem întreprinde absolut nici o acțiune care să ne protejeze 100% de furtul de identitate. Comparând această infracțiune cu evenimentele de aceeași natură din secolul trecut, descoperim că fenomenul ia amploare astăzi, prin simpla reproducere a conturilor valabile pe toate platformele de social media. Fenomenul este dezbătut intens în rândul persoanelor de specialitate și înțelegem de aici că indivizii tind să își atribuie cu totul alte personalități, înfățișări sau interese. Un exemplu concret îl constituie jocurile video, unde majoritatea utilizatorilor consideră că realitatea este un subiect tabu, astfel construind alte realități virtuale ce diferă de la joc la joc [9]. Legătura cu datele personale aici însă, este evidențiată de acțiunile utilizatorilor în ceea ce privește criptarea accesului și securizarea navigării, de unde realizăm cu stupoare că nu sunt mulți cei care pun în practică aceste aspecte.

De aici ne confruntăm și cu furtul de identitate ori infectarea cu malware-uri[1] a device-urilor utilizate.

Parcursul colectării datelor personale a constat într-un proces simplu, dar în același timp anevoios, presărat cu suișuri și coborâșuri, întrucât evenimentele prezentate anterior au contribuit la un progres semnificativ. Atât colectarea, cât și stocarea (arhivarea) sunt pași pe care instituția administrației publice trebuie să îi respecte pentru a facilita lucrul cu un volum foarte mare de date.

Documentul poate fi definit și înțeles diferit. Așadar, în viziunea Mariei Enătescu, documentul este *o […] unitate de informații identificată în mod unic pentru utilizarea de către om, de exemplu un raport, o specificație, un manual sau o carte* [10] ori putem să îl catalogăm ca fiind un cumul de informații personale (sau nu – în cazul în care gestionăm o situație a unei entități).

În lucrarea sa *Aspecte Teoretice ale Sistemului de Management al Documentelor*, Marcela Crețu, lector universitar în cadrul Academiei de Studii Economice din Moldova ne prezintă faptul că managementul documentelor se realizează urmărind o serie de funcționalități precum: versiunile soft-urilor pentru a determina schimbările survenite pe suprafața documentelor, monitorizarea distribuirii documentului în cauză, pentru a verifica modul în care acesta este utilizat și reutilizat, securitatea și, ceea ce am considerat că este mult mai important: *integrarea fluxului de activitate pentru a asocia ciclul de viață al unui document cu oameni, proiecte și programe* [11].

1.2. Accesul cetățenilor la informații publice

Instaurarea regimului democratic a jucat un rol crucial în dezvoltarea administrației publice din România, iar dacă analizăm acest aspect din perspectiva accesului cetățenilor la informațiile publice, parcursul a fost unul fluidizat prin prisma eficientizării procesului decizional. Cetățenii pot solicita în orice moment o informație de interes public de la oricare din instituțiile statului, cu atât mai mult de la instituțiile administrației publice, iar principiile comune care guvernează aceste decizii alcătuiesc cadrul legislativ pe care orice cetățean se poate baza la momentul solicitării informațiilor de interes public.

Această deschidere și transparență în relația dintre administrație și cetățeni reprezintă un pilon fundamental al unei societăți democratice și contribuie la consolidarea încrederii în autorități [4]. Accesul la informațiile publice permite cetățenilor să fie mai bine informați, să participe activ la procesul decizional și să poată monitoriza activitatea instituțiilor publice. Prin urmare, este crucial ca administrația publică să fie receptivă și să ofere informațiile solicitate în mod transparent și eficient. Promovarea transparenței și a accesului la informațiile publice reprezintă un semn al maturizării democrației și reflectă angajamentul autorităților față de cetățeni. Este important ca acest proces să fie constant îmbunătățit și consolidat, pentru a asigura o relație sănătoasă și constructivă între administrație și societate. Dispunem, așadar de:

- Legea 544/2001 privind liberul acces la informațiile de interes public, unde prin informație de interes public înțelegem *orice informație care privește activitățile sau rezultă din activitățile unei autorități publice sau instituții publice, indiferent de suportul ori de forma sau de modul de exprimare a informației* [12]
- *Principiul simplificării structurii și activității administrației publice* [13]
- Principiul *Government to Citizen – G2C* [14] de unde putem înțelege faptul că *furnizarea serviciilor guvernamentale se poate face pe mai multe canale, atât în mod tradițional, cât și prin mijloace electronice, pentru a permite cetățenilor să opteze între acestea.* [14]

[1] Malware – o aplicație rău intenționată; un cod care deteriorează sau perturbă utilizarea normală a dispozitivelor; cunoscut sub denumirea populară de *virus*

Însă procesul ne ajută înțelegem pașii:

- Solicitarea liberă a informațiilor – cetățenii sau organizațiile pot face solicitări formale pentru accesul la anumite informații deținute de instituțiile publice; solicitările trebuie să conțină o adresare clară și concisă care să includă detalii precise despre informațiile solicitate [15].
- Procesarea solicitării – autoritățile publice sunt responsabile de procesarea solicitării accesului la informații de interes public; ele pot verifica solicitările pentru a se asigura că sunt conforme cu legislația în vigoare și pot solicita taxe de procesare, în funcție de circumstanțe, ori însemnătatea documentelor ulterior prezentate solicitantului [15].
- Răspunsul – Organele publice sunt obligate să răspundă în mod corespunzător solicitărilor de informații publice într-un interval de timp specificat în lege. Răspunsurile pot include furnizarea informațiilor solicitate, respingerea solicitării sau furnizarea unor motive justificate pentru refuz [15].
- Apeluri, respectiv contestații – atunci când o solicitare de informații de interes public este respinsă, ori solicitantul este nemulțumit de răspunsul primit ulterior, acesta din urmă se poate adresa instanțelor de judecată prin apel sau contestație, conform procedurilor stabilite prin lege [15].
- Transparență în publicarea informațiilor de interes public – în plus față de solicitările survenite din partea cetățenilor ori organizațiilor, instituțiile administrației publice alături de autoritățile publice adoptă politici de publicare activă a informațiilor de interes public general pe site-urile web oficiale ale acestora, pentru a spori și pentru a evidenția transparența și accesibilitatea informațiilor pentru publicul larg. Transparența joacă un rol public politic important, pentru că evaluează performanța administrației publice și, cel mai important, previne *acțiunile care amenință integritatea instituției* în cauză. [15]

Accesul la informațiile de interes public reprezintă o piatră de temelie în construcția și menținerea unei societăți democratice și transparente. Această accesibilitate este esențială pentru o guvernare responsabilă și pentru asigurarea echilibrului între puterea guvernului și participarea activă a cetățenilor. Datele și informațiile publice pot fi utilizate pentru a identifica problemele sociale și economice și pentru a formula politici și soluții eficiente. Accesul liber la aceste informații poate stimula inovația, creșterea economică și îmbunătățirea calității vieții pentru întreaga comunitate. Este necesar ca cetățenii să aibă posibilitatea de a accesa informațiile relevante pentru a-și forma o înțelegere clară a acțiunilor guvernului și a impactului acestora asupra societății. Prin intermediul transparenței și accesibilității informațiilor publice, se poate promova responsabilizarea autorităților și se pot preveni abuzurile de putere. Astfel, accesul la informațiile de interes public reprezintă un pilon fundamental al unei societăți democratice și progresive.

Procesul de colectare a datelor personale reprezintă un aspect esențial în era digitală actuală din care facem parte. Acest proces poate fi descris ca fiind unul complex, care implică o serie de etape reprezentative pentru a asigura securitatea și confidențialitatea informațiilor colectate [16]. În plus, este important ca aceste date să fie gestionate în conformitate cu legislația în vigoare pentru a proteja drepturile și intimitatea persoanelor vizate, la fel ca și procedurile sus-menționate. Colectarea datelor personale poate începe în momentul în care o persoană interacționează cu un site web, completează un formular online sau care pur și simplu navighează pe internet. Informațiile colectate pot include nume, adresă, număr de telefon, adresă de e-mail, dar și date sensibile precum informații medicale sau detalii financiare (de exemplu, numărul cardului de debit/ credit). Odată ce datele sunt colectate, acestea trebuie stocate într-un mod sigur și accesibil. Stocarea datelor poate fi realizată prin intermediul diferitelor facilități online, cum ar fi servere cloud sau baze de date securizate [16]. Este important ca aceste informații să fie protejate împotriva accesului neautorizat și să fie păstrate doar pentru perioadele necesare conform scopului colectării lor, fapt ce se aplică inclusiv în administrația publică de stat.

Instituțiile administrației publice, precum și orice altă entitate care colectează date personale, trebuie să respecte regulile impuse de legislația privind protecția datelor cu caracter personal. Astfel, acestea sunt obligate să informeze persoanele vizate cu privire la scopul colectării datelor, să obțină consimțământul acestora în mod clar și să asigure securitatea și confidențialitatea informațiilor acumulate. Colectarea și stocarea datelor personale reprezintă procese esențiale în lumea digitală de astăzi, iar respectarea regulilor și normelor impuse de legislație este crucială pentru protejarea drepturilor și intimității individuale. Este important ca entitățile implicate să fie transparente în privința modului în care gestionează datele personale și să asigure că acestea sunt utilizate în mod responsabil și în conformitate cu prevederile legale. Totodată, în momentul în care o persoană dorește să își retragă datele personale din baza de date a instituției cu care a colaborat, ori să verifice ce date sunt în posesia acesteia, aceasta din urmă este obligată prin lege să îndeplinească cerința solicitantului.

1.3. Gestionarea informațiilor

Gestionarea informațiilor la nivelul aparaturii organelor abilitate de stat se datorează programelor performante de care administrația beneficiază în prezent. Această gestionare eficientă a informațiilor este ideală pentru o mai bună funcționare a instituțiilor publice, deoarece permite o monitorizare mai precisă a datelor, o gestionare mai eficientă a resurselor și luarea deciziilor bazate pe informarea în prealabil. Prin intermediul programelor performante, administrația poate să își îmbunătățească fluxurile de lucru, să reducă erorile umane și să ofere servicii de o calitate superioară cetățenilor. De asemenea, aceste programe facilitează colaborarea între diferitele departamente și agenții guvernamentale, contribuind la o comunicare mai eficientă și la o coordonare mai bună a acțiunilor. Astfel, investiția în sisteme informatice performante reprezintă un pas esențial către modernizarea administrației publice și îmbunătățirea serviciilor oferite cetățenilor.

Prin „programe” înțelegem acele aparaturi care dispun de soft-uri performante ce simplifică operațiunea de introducere de date, asta în cazul în care datele cu caracter personal ale cetățenilor, să spunem dintr-un formular sau o cerere, sunt preluate manual.

Reducerea erorilor umane în gestionarea documentelor ce cuprind informații cu caracter personal reprezintă un punct cheie în lucrul cu datele cetățenilor, lucru datorat minimizării posibilelor confuzii apărute în procesul administrativ (de exemplu, două persoane cu același nume, persoane care locuiesc la aceeași adresă de domiciliu, omiterea sau surplusul unor litere în anumite cuvinte/ fraze importante care fac obiectul documentului în cauză ș.a.m.d.). Acest lucru este esențial pentru protejarea confidențialității și securității datelor sensibile ale persoanelor, deoarece prin implementarea unor proceduri clare de verificare a datelor și utilizarea tehnologiilor moderne, organizațiile pot reduce semnificativ riscul de erori umane care ar putea avea consecințe grave. O gestionare eficientă a informațiilor cu caracter personal implică nu doar precizia în introducerea acestora, ci și o monitorizare atentă a accesului la aceste date sensibile. Este important ca doar persoanele autorizate să aibă acces la informațiile respective pentru că există mecanisme de securitate robuste pentru protejarea acestor date împotriva accesului neautorizat. Prin urmare, implementarea unor politici clare de securitate a datelor și formarea profesională regulată a angajaților în privința acestor politici reprezintă pași esențiali pentru prevenirea erorilor umane în gestionarea datelor personale, întrucât cunoaștem faptul că tehnologia avansează într-un ritm totalmente alert. În plus, utilizarea sistemelor informatice specializate poate contribui la automatizarea proceselor administrative, reducând astfel dependența de introducerea manuală a datelor și, implicit, riscul de a produce erori. Aceste sisteme pot include funcții de validare a datelor, verificare a consistenței informațiilor și generare automată a rapoartelor, ceea ce crește eficiența și reduce volumul de muncă. Astfel, gestionarea documentelor cu informații cu caracter personal rămâne deosebit de importantă pentru menținerea securității și confidențialității datelor.

Prin implementarea unor politici și proceduri clare, utilizarea tehnologiilor moderne și formarea continuă a personalului, organizațiile pot minimiza riscurile asociate erorilor umane și pot asigura protejarea corespunzătoare a datelor sensibile ale cetățenilor.

De menționat este și faptul că în procesul de gestionare a informațiilor trebuie să includem, totodată și procesul de dezvoltare al instituției care le colectează. Indiferent de natura instituției – entitate publică sau entitate privată, aceasta are dreptul să utilizeze informații în scopuri informative sau de marketing, fie să le prelucreze doar în scopul declarat și înscris clar pe documentul în cauză. Informația constituie „putere" [4], astfel că informațiile personale contribuie la dezvoltarea abilităților de manipulare în campaniile de vânzări sau în alcătuirea unor statistici. Datele personale sunt vitale pentru actorii privați și publici, deoarece, pe de o parte, companiile private își pot mări cota de piață prin prelucrarea datelor personale [4], iar pe de altă parte își sporesc clientela, sau în cazul administrației publice – utilizatorii.

În același timp, este recomandată structurarea informațiilor pe măsură ce recensămintele periodice de populație expun datele extrase [17]. *Într-o economie de piață, orice informație despre cum, unde, ce să produci și să vinzi, este valorificată la maxim. Pentru un astfel de scop, microstatistica, prin definirea microzonelor şi furnizarea de informații referitoare la acestea, vine și dă o nouă dimensiune informației în limitele deontologice dictate de societatea democratică* [17]. Aceasta rezultă în punerea la dispoziție a informațiilor și în baza altor criterii de departajare. Să presupunem că dorim să structurăm informațiile pe baza recensămintelor dintr-un județ cu o populație între 200.000 și 400.000 de locuitori. În exemplul de mai jos este județul Buzău.

Exemplu de structurare a informațiilor bazată pe recensământul populației la nivel local:

- În anul 2022, potrivit Institutului Național de Statistică, județul Buzău înregistra o populație de 393.043 de persoane, iar dintre acestea, majoritatea a fost determinată de persoane de peste 60 de ani, cunoscută în continuare ca fiind categoria de *seniori*.
- Date fiind informațiile sus-menționate, informațiile se pot reorganiza în interesul populației județului Buzău pentru a informa seniorii cu privire la ceea ce este de interes pentru aceștia.
- Dacă populația majoritară ar fi fost reprezentată de tinerii cu vârstele cuprinse între 20-35 de ani, administrația publică ar fi putut integra informații, de exemplu, din zona de divertisment, evenimente găzduite de primăria locală, etc.

De asemenea, instituțiile se obligă să respecte o procedură în ceea ce constă oferirea informațiilor, însă pe lângă ceea ce am menționat anterior, ne referim la persoana desemnată să răspundă în cazul în care aceste informații nu corespund cu standardele legale. Încă o dată formarea profesională este un punct cheie în fluidizarea proceselor informaționale, nu doar în cadrul proceselor decizionale. Această persoană care poate avea rolul unui purtător de cuvânt este necesar să aibă cunoștințe solide în domeniul respectiv și să fie capabilă să gestioneze situațiile în care informațiile furnizate nu respectă standardele legale. O formare profesională adecvată îi poate oferi acesteia instrumentele necesare pentru a face față eficient acestor situații, contribuind astfel la buna desfășurare a proceselor informaționale și decizionale în cadrul instituțiilor. Este important să existe o comunicare clară și eficientă între toate părțile implicate, iar respectarea procedurilor stabilite poate asigura un flux corespunzător al informațiilor și o gestionare responsabilă a acestora. Astfel, profesionalismul și competența personalului desemnat devin elemente esențiale în asigurarea conformității cu cerințele legale și în menținerea integrității proceselor organizaționale.

Din punct de vedere legislativ, cadrul legal instituie obligativitatea acestei comunicări din oficiu [18], pentru că în absența acesteia structura ierarhică și organizatorică poate avea de suferit la nivel instituțional administrativ. Înțelegem nevoia de transparență, deci, implicit, nevoia de a pune la dispoziție absolut orice detaliu care poate face diferența. În lucrarea sa, Ana Elena Ranta ne evidențiază și ne detaliază aspectul informațiilor de interes public ca fiind lucruri esențiale în

dezvoltarea unei comunități guvernate de administrația publică: *Cu privire la mijloacele de comunicare (în general, cât și pentru accesul la informații de interes public) precizăm că sunt unul dintre elementele constitutive ale procesului de comunicare și presupun intermedierea dintre cel care informează (emițătorul) și cel care recepteză informația (receptorul) sau parcurgerea unui drum de către mesaj de la emițător la receptor. Mijloacele de comunicare pot fi atât formale, cât și informale.* [18] de unde înțelegem că această comunicare se poate întreprinde prin intermediul a nenumărate căi.

Transparența în publicarea informațiilor cu caracter public este un element eminamente necesar într-o societate democratică, deoarece contribuie la creșterea încrederii cetățenilor în instituțiile publice și la asigurarea unui control adecvat asupra deciziilor luate de acestea. Prin furnizarea de informații corecte, complete și ușor accesibile, instituțiile administrației publice demonstrează responsabilitate și deschidere față de cetățeni. Legea 544/2001 reglementează acest aspect și stabilește standarde clare privind transparența și accesul la informațiile de interes public. Astfel, cetățenii au dreptul să solicite și să primească informații de la autorități, iar acestea sunt obligate să ofere răspunsuri în termenul legal stabilit, după cum am menționat anterior. Prin respectarea prevederilor legale în materie de transparență, instituțiile publice contribuie la consolidarea statului de drept și la promovarea unei guvernări deschise și responsabile. Transparența în instituțiile publice este un pilon fundamental al unei democrații sănătoase, deoarece oferă cetățenilor posibilitatea de a înțelege și evalua acțiunile autorităților în numele lor.

Atunci când informațiile sunt disponibile publicului larg, se creează o relație de încredere între guvernanți și guvernați, iar corupția și abuzul de putere pot fi reduse semnificativ. Prin urmare, transparența în afișarea și procurarea informațiilor de interes public nu este doar un concept teoretic, ci o practică esențială pentru buna funcționare a unei societăți democratice. Este important ca cetățenii să aibă acces la informații precise și actualizate despre deciziile și acțiunile autorităților, deoarece acestea au un impact direct asupra vieților lor și a comunității în ansamblu. În plus, transparența în administrația publică și în egală măsură în procesul de gestionare al datelor sensibile poate îmbunătăți eficiența instituțiilor, deoarece procesele decizionale devin mai fluidizate și mai ușor de monitorizat la nivel național. Când deciziile sunt luate în lumină publică, există o presiune naturală pentru ca acestea să fie bine fundamentate și să servească în mod corect și concret interesele generale.

În același timp, transparența poate stimula implicarea cetățenilor în procesul decizional, deoarece aceștia se simt mai încrezători în faptul că opiniile și preocupările lor sunt luate în considerare de către autorități. Din acestea, constatăm că accesul cetățenilor la informațiile publice survenite în urma unei bune gestionări a acestora joacă un rol important pentru publicarea informațiilor de interes public, întrucât este vitală pentru o guvernare responsabilă și pentru menținerea unei societăți democratice sănătoase. Prin promovarea accesului la informație și respectarea normelor de transparență, instituțiile publice pot consolida încrederea cetățenilor în guvernare și pot asigura o mai bună reprezentare a intereselor acestora.

Prin facilitarea accesului la informații și respectarea normelor de transparență, instituțiile publice pot întări încrederea cetățenilor în guvernare și pot asigura o reprezentare mai bună a intereselor acestora. Este responsabilitatea fiecăruia dintre noi să sprijinim și să promovăm transparența în administrația publică, deoarece acest aspect reprezintă o componentă fundamentală a unei societăți democratice funcționale și echitabile.

Capitolul 2. Protecția datelor cu caracter personal

Prin *date cu caracter personal* la nivel comunitar putem număra acele date care fac obiectul existenței unui individ într-un anumit grup social sau platformă de social media. Din punct de vedere legislativ și academic, datele cu caracter personal reprezintă o multitudine, un cumul de informații deosebit de importante care alcătuiesc identitatea și identificarea unei persoane fizice [19]. Aceste date sunt protejate de legea privind protecția datelor cu caracter personal, care reglementează modul în care informațiile personale pot fi colectate, stocate, prelucrate și utilizate. În cadrul legislației europene, Regulamentul General privind Protecția Datelor (GDPR) este unul dintre principalele acte normative care stabilește standardele pentru protecția datelor cu caracter personal ale cetățenilor din Uniunea Europeană. Acest regulament impune organizațiilor să protejeze confidențialitatea și securitatea datelor cu caracter personal și să ofere transparență cu privire la modul în care aceste date sunt folosite. Astfel, respectarea prevederilor GDPR este esențială pentru orice entitate care colectează sau prelucrează date cu caracter personal, indiferent de dimensiunea sau domeniul de activitate al acesteia [20]. Prin urmare, este de evidențiat faptul că atât companiile, cât și indivizii să fie conștienți de drepturile și obligațiile prevăzute de legislația privind protecția datelor cu caracter personal pentru a asigura o gestionare corectă și responsabilă a informațiilor personale.

Sub umbrela Uniunii Europene, din care face parte și România, s-a subliniat importanța dezvoltării și aprofundării Regulamentului, întrucât drepturile și libertățile cetățeanului european trebuie să fie respectate cu orice preț în relația companie-cetățean [20].

2.1. Generalități

Referitor la drepturile omului, Curtea Europeană a Drepturilor Omului (CEDO) joacă un rol important în protejarea drepturilor și libertăților individuale în spațiul european. În ceea ce privește protecția datelor personale, CEDO a abordat diverse cazuri care vizează intimitatea datelor și intersectarea acesteia cu drepturile omului. Una dintre considerațiile principale în aceste cazuri este echilibrul dintre dreptul la intimitate, consacrat în Articolul 8 al Convenției Europene a Drepturilor Omului [21], și alte interese concurente cum ar fi libertatea de exprimare, securitatea și interesul public. CEDO a stabilit că protecția datelor personale este într-adevăr un aspect fundamental al dreptului la intimitate. În era digitală, în care cantități vaste de informații personale sunt colectate, stocate și procesate, Curtea a subliniat nevoia de cadre legale solide pentru a asigura cetățenii că datele individuale sunt tratate într-un mod care respectă drepturile acestora. Acest lucru include principii precum transparența, limitarea scopului, minimizarea datelor, exactitatea, limitarea stocării, integritatea și confidențialitatea. Mai mult, CEDO a evidențiat importanța remedierilor eficiente pentru persoanele ale căror drepturi privind protecția datelor au fost încălcate. Acest lucru include dreptul de acces la propriile date personale, dreptul la rectificare, ștergere sau restricționare a prelucrării, și dreptul de a cere repararea prin mecanisme independente și imparțiale. În ansamblu, jurisprudența CEDO privind protecția datelor subliniază interconectarea drepturilor la intimitate și importanța tot mai mare a asigurării unor măsuri de protecție solide în era digitală. Prin interpretarea prevederilor Convenției Europene a Drepturilor Omului în lumina provocărilor moderne generate de progresele tehnologice, Curtea continuă să contureze peisajul legal referitor la protecția datelor personale în Europa [22].

Raportându-ne la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), acestea din urmă se prelucrează exclusiv cu acordul persoanei în cauză [23]. Această prelucrare a datelor cu caracter personal trebuie să se facă în conformitate cu prevederile Regulamentului General privind Protecția Datelor[2]. GDPR impune operatorilor de date să obțină consimțământul clar și explicit al persoanelor vizate înainte de a prelucra datele acestora. Consimțământul trebuie să fie liber acordat, informat și specific în ceea ce privește

[2] *GDPR – General Data Protection Regulation*

scopurile prelucrării datelor. Articolele 13 și 14 din GDPR ne oferă indicații clare cum că operatorul de date personale trebuie și este obligat să furnizeze un set de informații persoanei vizate, atât în situația în care operatorul a obținut datele de la aceasta, cât și prin prisma altor terțe părți [5]. Pe lângă aceste informații, operatorul mai trebuie să specifice și perioada în care aceste date vor fi prelucrate [5].

De asemenea, persoanele vizate trebuie să aibă posibilitatea de a-și retrage consimțământul în orice moment [5]. Este important ca operatorii de date să respecte drepturile persoanelor vizate în ceea ce privește confidențialitatea și securitatea datelor lor personale. Într-un studiu înaintat de trei experți în securitate cibernetică ce activează sub egida *Google* intitulat *If I press delete, it's gone* s-a evidențiat faptul că majoritatea utilizatorilor internetului larg consideră că atunci când își exprimă clar, în scris[3] dorința de a-și retrage datele de pe o anumită platformă – acestea dispar definitiv. Experții au intervievat trei categorii de utilizatori: a) utilizatori ce posedă cunoștințele de la suprafață, b) utilizatorii care sunt pasionați de domeniul cibernetic și care posedă informații relevante și c) utilizaorii experimentați, care cunosc parcursul ștergerii datelor cu caracter personal. Acestora li s-au oferit două scenarii: 1. Ștergerea e-mailurilor și 2. Ștergerea informațiilor (ex.: fotografii) de pe platformele de social-media [24]. În tabelul de mai jos este ilustrată înțelegerea utilizatorilor referitor la ștergerea datelor lor personale.

Tabel 1, unde a); b); c) reprezintă categoriile de utilizatori intervievați

Scenarii	a)	b)	c)
E-mail	Mail-urile dispar definitiv	Este marcat ca fiind „șters", deci utilizatorul nu le mai poate accesa niciodată, însă serverele și bazele de date încă le stochează	Userul nu mai poate accesa nimic din ceea ce a fost șters, însă doar după ce serverul și baza de date primesc comanda automată de a le șterge, informațiile dispar
Social Media	Fotografiile dispar definitiv		

Sursa: "If I press delete, it's gone" - User Understanding of Online Data Deletion and Expiration, p.331 [24]

Din acest studiu putem să subînțelegem că este deosebit de important să cunoaștem o bază legală pe care să o putem aborda atunci când ne exprimăm dorința de a ne retrage datele de pe orice platformă din mediul online, cât și în realitate, de la orice entitate privată sau publică.

La o analiză mai detaliată, putem observa că, deși există unele situații în care drepturile omului promulgate în Convenția Europeană a Drepturilor Omului pot intra în conflict cu normele GDPR referitoare la protecția datelor cu caracter personal, legislația în vigoare încearcă să găsească un echilibru între aceste două aspecte importante. Este crucial să se asigure că operatorii de date respectă atât drepturile fundamentale ale individului, cât și cerințele stricte ale GDPR pentru a proteja confidențialitatea și securitatea informațiilor personale. Astfel, în ciuda aparențelor inițiale de posibil conflict, este esențial să se urmărească respectarea ambelor seturi de reguli pentru a menține un echilibru corect și legal în tratamentul datelor cu caracter personal [20] [22].

Dincolo de aspectele legale ale normelor, entitățile care gestionează un volum impresionant de date cu caracter personal au obligația de a face publică procedura colectării, prelucrării și stocării acestora. Procedurile sunt posibile doar în momentul în care persoana vizată și-a exprimat acordul în mod expres și neechivoc [20] [23]. Există, însă și spețe care permit entității aflate în poziția de operator de date cu caracter personal să prelucreze datele persoanei/

[3] De exemplu: utilizând comenzi rapide, precum „Unsubscribe" sau "I no longer wish to receive e-mails from this company", etc.

persoanelor vizate fără consimțământul acesteia/ acestora în prealabil. Câteva exemple relevante, conform ANSPDCP sunt următoarele:

- atunci când prelucrarea datelor este necesară în vederea executării unui contract semnat în prealabil de părți; [23]
- atunci când prelucrarea este realizată în scop academic, datele persoanei/ persoanelor vizate rămânând anonime pe toată durata cercetării; [23]
- atunci când prelucrarea face obiectul (oferirii informațiilor de interes public ex. statistici); [23]
- când prelucrarea este necesară în vederea protecției persoanei vizate, protejarea identității sale, sau chiar a vieții sale, ori când o altă persoană, respectiv terță parte este amenințată; [23]
- fie când prelucrarea conține în mod implicit date accesibile publicului larg, cunoștințe pe care un grup social îl posedă deja [23].

În altă ordine de idei, la nivel de instituție se impune ocuparea unei poziții de *responsabil cu protecția datelor* sau *Data Protection Officer (DPO)* [25], iar GDPR reglementează cadrele legale și situațiile speciale în care acesta trebuie să fie numit. În mod sugestiv, persoana care va ocupa această funcție, este supranumită „gardian" al datelor personale [26]. Deși funcția acestuia poate trimite cu gândul la aspectul că persoana în cauză este unica responsabilă de gestionarea datelor cu caracter personal, ori a informațiilor sensibile din entitatea în care activează, în realitate activitățile principale se raportează la activitățile de bază și *nu la prelucrarea datelor cu caracter personal drept activități auxiliare* [25]. Un exemplu concret în acest sens este reprezentat, din punct de vedere ipotetic, de un angajat al unei unități medicale: responsabilul cu protecția datelor preia dosarele cu datele pacienților de la doctori și asistente și le stochează într-o bază de date pentru a ușura atât volumul de muncă al instituției în materie de conformitate cu legislația în vigoare, cât și a colegilor săi când/ dacă pacienții revin în cabinetele sau pe paturile instituției spitalicești [25].

Păstrând cadrul medical, verificarea procesului de stocare și de utilizare a datelor personale în timpul pandemiei de COVID-19 s-a realizat și grație unui certificat care a fost supus în prealabil unor teste și verificări riguroase. Certificatul digital al UE privind COVID a fost special conceput pentru acele persoane care aveau o deosebită nevoie de a parcurge călătorii transfrontaliere. Acest document a favorizat temeiul juridic pentru prelucrarea datelor cu caracter personal în conformitate cu GDPR [27].

Certificatul conținea, bineînțeles, numeroase date sensibile personale ale posesorului referitoare la parcursul său prin pandemia de COVID-19 sau infectarea cu SARS-CoV-2: istoricul vaccinărilor, istoricul infectărilor și istoricul spitalizărilor ș.a.m.d. Scopul prelucrării a condus la asigurarea unui cadru legal conform în verificarea informațiilor într-un timp alert, cu respectarea absolută a GDPR-ului. În România, aplicația dezvoltată de Serviciul de Telecomunicații Speciale în temeiul OUG 68/2021 intitulată *Check DCC*, în lipsa unor măsuri de securitate insuficiente – datele personale colectate de la cetățeni creau, pe lângă obiectul reglementărilor certificatului UE privind COVID-19, un cadru deosebit de favorabil stocării și utilizării acestora în scopuri malițioase. *În Uniunea Europeană, aplicația Check DCC a Serviciului de Telecomunicații Speciale este singura aplicație dezvoltată de către o instituție guvernamentală identificată din eșantionul de cercetare care permite utilizatorului să stocheze date cu caracter personal prin operațiunea de screenshot, abătându-se de la scopurile prelucrării stabilite în Regulamentul (UE) 2021/953, […]* [27].

Astfel, putem să evidențiem natura sensibilă a datelor personale ale fiecărui individ și să punem într-o deosebită valoare soft-urile pe care atât entitățile publice, cât și cele private le utilizează pentru a livra o excelentă experiență utilizatorilor.

2.2. Modalități de păstrare a datelor cu caracter personal

Legislația europeană cuprinde afirmația că fiecărui cetățean îi sunt respectate drepturile și libertățile și, deci, implicit îi vor fi protejate și datele cu caracter personal în relația cu instituțiile cu care interacționează. Fie că vorbim despre aplicarea la un loc de muncă pe site-uri special concepute în acest scop, fie că achiziționăm un coș de cumpărături online, sau că alegem să încheiem un credit cu banca dorită – aceste acțiuni implică consimțământul cu privire la prelucrarea datelor personale, pentru că altfel va fi aproape imposibil ca un utilizator aflat în poziția de client să beneficieze de serviciile alese fără informațiile sale personale corecte și precise. Totodată, entitatea care colectează aceste informații urmează o serie de pași care asigură consumatorului o experiență unică, prin simplul fapt că a respectat intimitatea și integritatea acestuia, păstrându-i datele în siguranță [28].

Articolul 5, alineatul (1), litera (a) din GDPR [29] prevede că toate datele trebuie să fie colectate, păstrate și utilizate într-o manieră care este compatibilă cu cerințele și dorințele consumatorului, într-un mod echitabil, transparent și, bineînțeles, legal. Legalitatea, echitatea și transparența alcătuiesc un proces de colectare și de stocare al datelor sigur și conform, dacă entitatea ține cont în totalitate de acești pași [30].

Tabel 2

Legalitate	Echitate	Transparență
Se identică temeiul juridic pentru prelucrarea datelor	Evaluarea modului în care datele afectează persoana vizată	Deschiderea și sinceritatea față de persoana vizată și respectarea dreptului consumatorului de a fi informat în legătură cu orice prelucrare pentru care acesta nu și-a exprimat acordul
Dacă datele conțin informații deosebit de sensibile[4] se identifică o condiție pentru prelucrarea acestora	Informarea în prealabil a persoanei vizate dacă datele pot afecta persoana vizată	
	Scopul prelucrării trebuie să fie trecut în clar în termenii și condițiile serviciului pus la dispoziție	

Sursa: LegalUp − Regulamentul GDPR: Legalitatea, Echitatea și Transparența – principiu esențial

În mediul online prelucrarea și stocarea datelor se poate realiza și în situația în care consumatorul nu intenționează să beneficieze de un anumit serviciu, mai exact nu intenționează să achiziționeze un produs, să deschidă un credit, sau să aplice la un loc de muncă. Această acțiune este posibilă prin intermediul ***cookies*** [31].

Cookie-urile reprezintă fișiere mici de text descărcate pe echipamentul terminal[5] atunci când utilizatorul accesează un site web [31]. Acestea salvează informații relevante și îmbunătățesc experiența online utilizatorului [32]. Pentru referință, cu ajutorul cookie-urilor utilizatorul poate rămâne conectat la site-ul respectiv, platforma reținându-i datele de conectare și, de asemenea, salvează preferințele acestuia, oferindu-i conținut similar [32].

Există două categorii de cookie-uri:

- cookie-uri primare – alcătuite de site-ul accesat la momentul respectiv (site-ul poate fi observat în bara de adrese) [32];

[4] Exemplu: condamnări penale, respectiv datele aparțin unei categorii speciale [30]
[5] Exemplu: un computer sau un smartphone [31]

- cookie-uri terță parte – acele cookie-uri alcătuite de alte site-uri (un site accesat anterior poate afișa pe un altul imagini, texte, reclame, anunțuri) pentru a îmbunătăți experiența utilizatorului [32].

În imaginea alăturată este ilustrată interpretarea celor două tipuri de cookie-uri:

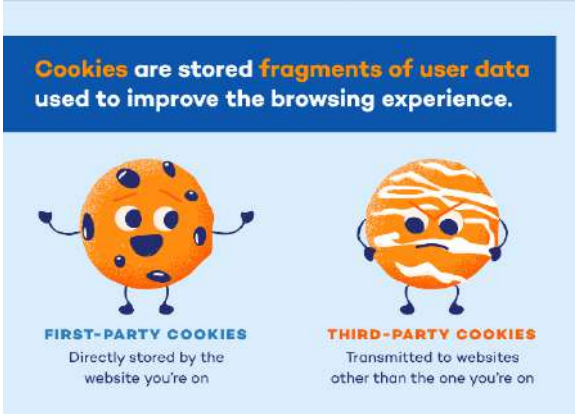

Fig. 1. Tipurile de cookie-uri
Sursa: https://malware.news/t/are-cookies-bad-how-to-clear-them/42393

Pentru că aceste cookie-uri stochează date relevante ale utilizatorului, adresa de IP este prima accesată pentru a obține informații importante referitoare la experiența navigării pe internet [31]. Adresa de IP (Internet Protocol) reprezintă baza comunicării online și, în mod sugestiv, este echivalentul adresei fizice [33]. Aceasta este formată dintr-un număr unic, atribuit fiecărui dispozitiv care are acces la internet și se comportă întocmai ca o adresă poștală, pentru ca informația solicitată prin servere să ajungă exact unde are nevoie [33]. Astfel, cele două comunică activ pentru a livra o experiență conformă GUI[6].

Știm că odată cu avansarea tehnologiei, la fel și traficul de date personale a crescut exponențial [34]. Deși reglementările legale interzic transferul de date între entități, acesta poate fi realizat în anumite condiții. Dacă anterior am menționat că adresa de IP și cookie-urile comunică pentru a oferi o experiență veritabilă utilizatorului, acest lucru se poate realiza și în scopuri malițioase. Cum spuneam, datele personale conțin nume, adrese, vârste, adrese de mail, numere de telefon sau, mai sensibil – informații legate de starea de sănătate a individului: diferite afecțiuni, spitalizări, rezultate de la analize ș.a.m.d, ori informații privind starea de libertate a unei persoane, sau dacă a fost condamnat penal în trecut, dacă a avut o amendă, etc. Entitățile care colectează și stochează astfel de date nu numai că influențează navigarea pe internet a utilizatorului, ci ajută alte terțe părți (voit sau nevoit din cauza unei securități slabe a site-ului) să selecteze posibili consumatori în funcție de nevoile proprii [34]. Cum se realizează această acțiune? Să presupunem că o companie dorește să angajeze o persoană pe un post de instructor de fitness. Compania poate selecta ca anunțul locului de muncă vacant să apară în căutările persoanelor care nu prezintă/ nu au prezentat afecțiuni grave de sănătate, precum tensiune arterială, astm, sau alte afecțiuni care ar afecta o bună desfășurare a unei activități al cărui obiect principal este sportul și sănătatea. Alt exemplu l-ar putea constitui o instituție bancară care și-ar putea selecta posibilii clienți prin simplul fapt că vinde reclame pentru accesarea unui credit persoanelor care nu au fost condamnate penal anterior, persoanelor care au un cazier curat, doar pentru a se asigura că acel consumator își poate achita datoriile la timp, fără complicații [34].

Din experiența personală, în calitate de angajat în domeniul vânzărilor telefonice, am întâlnit persoane care au semnat acordurile de marketing în necunoștință de cauză, astfel ca atunci când primeau un apel în care li se prezentau ofertele de actualitate, aceștia întrebau care este sursa din care compania apelantă deține numărul lor personal de telefon.

[6] GUI – Graphical User Interface [69]

Datele cu caracter personal trebuie să beneficieze de o securitate pe măsură, întrucât orice atac sau scurgere de date poate compromite activitatea companiei care le deține [35]. În lucrarea *Protecția și securitatea datelor personale în educația digitală* a autorilor Adriana-Maria Șandru și Daniel-Mihail Șandru se abordează securitatea unui volum impresionant de date cu care ar putea lucra instituțiile de învățământ. Autorii sugerează ideea de a renunța la anumite documente semnate în format fizic anual, de exemplu de către ambii părinți ai unui elev, deoarece în acest mod se va ușura procesul de arhivare și, implicit cel de stocare al datelor personale în momentul în care un document de acest gen este introdus într-o bază de date online. Bineînțeles, dacă o instituție școlară ar avea un sistem digital deosebit de dezvoltat ar putea utiliza o tehnologie proprie care să eficientizeze și să ușureze colectarea și stocarea datelor cu caracter personal [35].

Navigarea pe internet aduce cu sine consecințe cu fiecare click [4], atât pentru utilizator cât și pentru entitatea care pune la dispoziție anumit servicii și informații, sporind o activitate transparentă în materie de interes public și public [14]. Cu această avansare în tehnologie și dezvoltarea anumitor soft-uri performante, oamenii au ajuns să perceapă în mod diferit spațiile publice din mediul online, astfel că anumite rețele de socializare, s-au transformat în *comunități virtuale* [36].

Comunitatea virtuală se alcătuiește odată ce o categorie de persoane este deosebit de activă în jurul unui subiect anume, domeniu sau activitate comună [36]. Neexistând limite, decât cele conform legii, utilizatorii au libertatea de a de exprima liber și fără restricții, având posibilități nenumărate de a aborda situațiile cu care simpatizează și alții. Conform unei statistici realizate de site-ul https://statista.com/, în anul curent România utilizează cel mai des platformele Facebook, WhatsApp și Facebook Messenger [37].

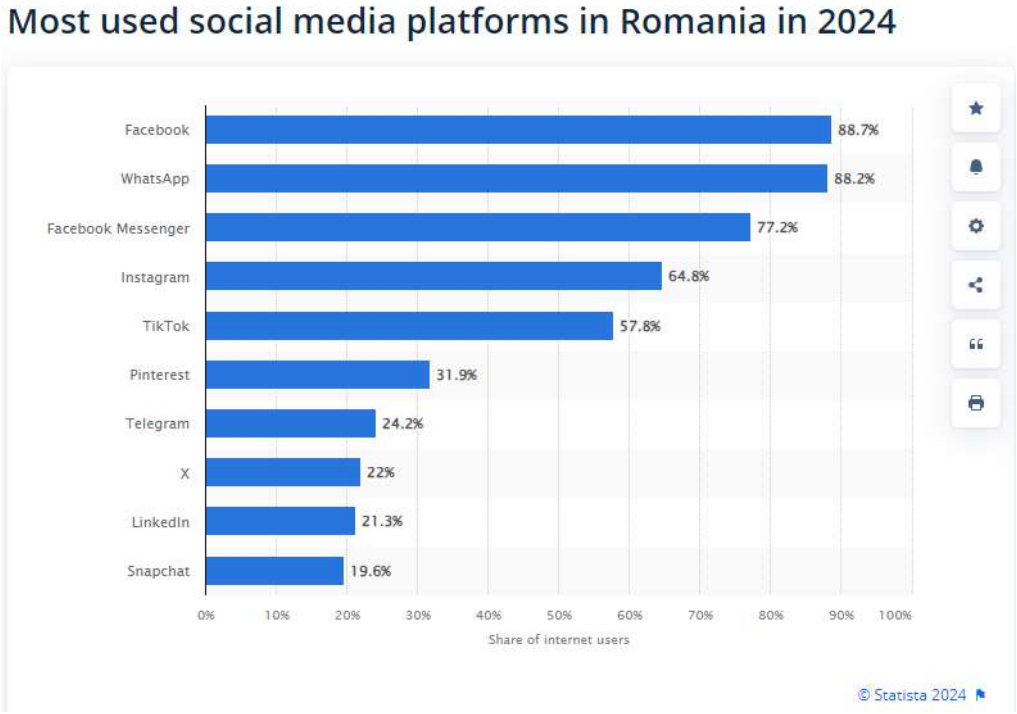

Fig. 2. Cele mai utilizate platforme de social media în România în anul 2024
Sursa: https://www.statista.com/statistics/1172720/romania-most-used-social-media-platforms/

Pentru că de-a lungul timpului acest clasament s-a păstrat cu aplicația Facebook în primul loc al clasamentului, în anul 2013 *rețelele sociale au fost considerate loc public de către instanțele române* [36]. Curtea de Apel Târgu-Mureș, secția a II-a civilă a anunțat atunci în urma unui caz că *„rețeaua de socializare Facebook, nu poate echivala, sub aspectul controlului mesajelor difuzate cu o căsuță poștală electronică. Profilul său personal pe Facebook chiar dacă este*

accesibil doar prietenilor adică unui grup restrâns de persoane, tot public este, oricare dintre „prieteni" putând distribui informațiile postate de titularul paginii, aspecte pe care reclamantul îl cunoștea" [36].

Securitatea datelor în mediul online, în special pe platformele de social media celebre și larg utilizate, este un subiect de mare importanță și dezbateri frecvente. Acest aspect devine crucial în momentul în care utilizatorii sunt solicitați să ofere informații personale, cum ar fi o fotografie de profil sau o descriere succintă a lor. Protejarea datelor personale în mediul online este esențială pentru a preveni posibilele abuzuri sau utilizări neautorizate ale acestor informații [36]. Este important ca utilizatorii să fie conștienți de riscurile implicate în dezvăluirea datelor lor personale și să fie precauți în a oferi informații sensibile pe internet. Folosirea parolelor puternice, actualizarea regulată a setărilor de confidențialitate și verificarea surselor sunt doar câteva măsuri pe care utilizatorii le pot lua pentru a-și proteja securitatea online. Este recomandabil ca indivizii să fie vigilenți și să se informeze cu privire la politicile de confidențialitate ale platformelor pe care le folosesc, pentru a se asigura că datele lor sunt în siguranță [38].

Profilarea utilizatorului reprezintă, conform articolului 4, pct. 4 din GDPR, *orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia* [39].

Pentru că securizarea reprezintă un pas crucial în protejarea unui cont pe un site sau o platformă de socializare [16], înainte de toate, accesul în contul respectiv trebuie să se facă după ce o serie de termeni și condiții a fost îndeplinită: alegerea unei parole și a unui nume de utilizator [40]. Majoritatea site-urilor companiilor sau platformelor renumite anunță utilizatorul dacă la momentul creării unui cont nou parola aleasă este una slabă sau foarte puternică prin intermediul unor măsurători alese de fiecare site în parte. Cele mai des întâlnite sunt barometrele [40], iar un exemplu concret îl reprezintă figura 3 alăturată:

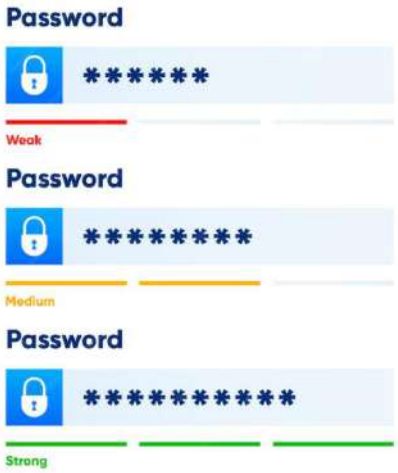

Fig. 3. Exemplu de metodă de măsurare a securității parolei
Sursa: https://www.freepik.com/

Prezența acestui barometru indică faptul că utilizatorii devin mai motivați să securizeze o parolă puternică, făcându-i astfel mai responsabili [40].

Nu doar parolele reprezintă „arma” împotriva pierderii conturilor online sau împotriva atacurilor cibernetice, deoarece există diferite modalități prin care o persoană se poate „apăra” de acțiuni malițioase, utilizând o serie de pași recomandați de experți [41]:

- autentificarea în doi pași (2FA) – reprezintă un token[7] suplimentar care facilitează accesul în cont utilizatorului atunci când introducerea parolei obișnuite nu este de ajuns, sau nu a trecut de brețele de securitate ale site-ului respectiv, oferindu-i opțiunea de a alege două din trei modalități de conectare: *un factor de cunoaștere, un factor de posesie și un factor de inerență* [42] [43];
- Verificarea identității prin intermediul introducerii codului primit pe telefon printr-un mesaj text [44];
- Utilizarea unor aplicații adiacente pentru a ușura procesul de logare, de exemplu: *Google Authenticator, Duo Mobile, FreeOTP, Microsoft Authenticator* ș.a.m.d. [41].

2.3. Contextul siguranței naționale

Siguranța națională în domeniul IT reprezintă o preocupare majoră pentru guvernele din întreaga lume, deoarece societatea modernă devine din ce în ce mai dependentă de tehnologia informației și comunicațiilor [45]. Cu evoluția rapidă a tehnologiei, infrastructura IT a devenit o componentă vitală pentru funcționarea eficientă a diferitelor sectoare și instituții. Protejarea acestor sisteme informatice și a datelor sensibile asociate lor este crucială pentru asigurarea securității naționale și prevenirea amenințărilor cibernetice [46]. Prin implementarea unor strategii și măsuri de securitate cibernetică eficiente, guvernele încearcă să prevină atacurile informatice, să protejeze informațiile sensibile și să asigure buna desfășurare a activităților critice pentru funcționarea statului și a societății în ansamblu [45].

Pentru că este necesar ca fiecare infracțiune să fie sancționată conform legislației în vigoare, s-a evidențiat nevoia apariției unui cadru legal favorabil la nivel european, cât și la nivelul conducerii din România [47].

Astfel, Directiva (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniunea Europeană reglementează cadrul legal pentru entitățile mijlocii și mari care utilizează diferite tehnologii pentru a-și dezvolta și spori activitatea. Printre sectoarele critice vizate în Directivă se numără sectorul bancar, sectorul sănătății, sectorul transporturilor și, printre multe altele încă, administrația publică care odată cu avansarea tehnologică a adoptat strategii de dezvoltare în mediul online pentru facilitarea accesului la informația publică cetățenilor [47].

La nivelul Comisiei Europene s-a stabilit, odată cu această Directivă, înființarea unor echipe de suport IT denumite *computer security incident response teams (CSIRT)* [48] care oferă asistență tehnică entităților prin monitorizarea și analizarea amenințărilor cibernetice, asigurarea unor funcționalități ce îi permit entității respective să prevadă posibilele atacuri, răspunsuri rapide la probleme întâmpinate, înaintarea procedurii de verificare în caz de incident/ atac cibernetic, sau, după caz, scanarea intensivă și proactivă a sistemelor utilizate pentru a detecta vulnerabilitățile cu un impact potențial semnificativ [48].

Strategia de Securitate Cibernetică a României pentru perioada 2022-2027 emisă de Guvernul României la 30 decembrie 2021 reglementează implementarea și aplicarea unor viziuni actualizate din punct de vedere tehnologic și se înscrie în demersurile întreprinse la nivel național cu scopul securității unui cadru informatic sigur [47].

[7] Token – unitate ce are o anumită valoare pentru a facilita accesul în conturi, denumit popular și „one time password”

Chiar dacă legislația asigură entitățile că siguranța cibernetică la nivelul Administrației Publice din România atinge cotele așteptate [47], există, totuși, o serie de tipuri de atacuri cibernetice pe care ***hackerii*** le pun în aplicare pentru a trece de brețele de securitate.

În primul rând, prin noțiunea de „hackeri" înțelegem acele persoane care posedă capacități profesionale de a crea sau chiar modifica codurile din limbajele de programare, intrând nedetectați de aplicațiile anti-virus[8] în sistemele informatice [16]. Conform Elenei Bădărău, în lucrarea sa *Securitatea Națională și Diminuarea Riscurilor Ciberamenințărilor*, hackerii sunt împărțiți în trei categorii:

- Hackeri „pălărie-albă" – cunoscuți sub denumirea de *hackeri non-malware* sunt reprezentați de persoanele aflate în poziția de angajați ai unei firme care testează securitatea propriului sistem cibernetic prin încercarea de a pătrunde în acesta [16];
- Hackeri „pălărie-neagră"/ „Crackers" – fiind categoria cea mai comună de hackeri, probabil aceea la care se gândesc toți oamenii la auzul acestui termen, este reprezentată de acele persoane care pătrund în mod ilegal în sistemele informatice cu intenția de a fura, ori de a vandaliza [16];
- Hackeri „pălărie-gri" – aceștia se încadrează între hackerii „pălărie-albă" și hackerii „pălărie-neagră" și sunt acele persoane care pătrund ilegal în sisteme și trec de brețele de securitate fără autorizație cu scopul de a depista vulnerabilitățile acestora, ca mai apoi să ceară proprietarului plata unei taxe pentru a înlătura problema identificată [16].

În al doilea rând, atacurile cibernetice pe care hackerii le pun în aplicare reprezintă un cumul de acțiuni pe care aceștia le pun în practică, targetând anumite categorii de persoane, entități sau instituții, printre care se numără și administrația publică. Parlamentul European a luat în considerare o serie de principale atacuri cibernetice preferate de hackeri, iar pe baza acestei prezumții, Agenția Uniunii Europene pentru securitate cibernetică (Enisa) a întocmit un raport care descrie principalele 8 atacuri, însă cele mai frecvente sunt atacurile de tip [49]:

- **Ransomware** – atacatorii criptează accesul proprietarului și cer plata unei taxe pentru a reda accesul acestuia [49];
- **Malware** – programe construite de atacatori care pot lua, din punct de vedere informatic, forma virușilor, cailor troieni, viermilor sau a programelor spion. Studiile arată că rata infectărilor cu malware-uri a scăzut pe perioada pandemiei de COVID-19, când populația globului a încetat să frecventeze mersul la birou, dar a crescut odată ce oamenii și-au reluat activitatea obișnuită la începutul anului 2021 [49];
- **Inginerie socială** („**Social engineering**") – acțiune ce se influențează utilizatorul prin simpla inducere în eroare cu scopul de a accesa informații ascunse, sau de interes larg, public. Practic, atacatorii ademenesc utilizatorii cu fișiere pe care aceștia să fie tentați să le deschidă pentru a pătrunde în sistem și a fura produsul sau produsele țintite. Cele mai cunoscute metode sunt „phishing-ul" (prin intermediul e-mail-ului) sau „smishing-ul" (prin intermediul mesajelor text) [49];
- **Distributed Denial of Service** (**DDoS**) – reprezintă amenințări la adresa disponibilității, mai exact blocarea accesului la baza de date și la servicii pentru publicul larg. Se caracterizează prin indisponibilizarea unui sistem și supraîncărcarea structurii de rețea. Cercetările și raportările arată că aceasta este cea mai comună metodă în contextul militar actual prezent pe glob: războiul cibernetic Rusia-Ucraina. În trecut, cercetătorii și experții afirmă că site-urile destinate vaccinării împotriva COVID-19 au fost și ele deosebit de afectate de acest tip de atac cibernetic [49];
- **Defacement** – atacatorii modifică arhitectura site-ului, schimbându-i complet înfățișarea, ori blocând accesul definitiv [49].

[8]Anti-virusul este un program de securitate informatică proiectat pentru a detecta, preveni și elimina programele malware, cum ar fi virușii, troienii, viermii, spyware-ul și alte amenințări cibernetice, de pe un computer sau dispozitiv electronic

Îngrijorător este faptul că administrațiile publice și guvernele din Europa se situează pe primul loc în topul celor mai afectate sectoare în materie de atacuri cibernetice, urmate de furnizorii de servicii digitale și, pe locul III − publicul larg [49].
Administrația publică a României s-a adaptat la schimbările informatice și tehnologice, iar odată cu evoluția digitalizării și a sistemelor performante, putem să corelăm activitatea acesteia cu o serie de politici de dezvoltare informațională la nivel național, tocmai pentru a combate și pentru a eradica posibilele atacuri cibernetice care pot conduce la scurgeri de date deosebit de sensibile și importante societății [2].

România s-a confruntat de-a lungul timpului cu o serie de atacuri cibernetice în rândul site-urilor oficiale ale instituțiilor importante din administrația publică, asta pentru că, spun experții, politica de securitate nu a fost una îndeajuns de puternică pentru a interzice atacatorilor să pătrundă în sistem și să treacă de brețele de securitate [16].

Astfel, putem menționa câteva exemple de atacuri cibernetice recente:

- **Atacurile cibernetice ale hackerilor ruși asupra site-urilor din România de tip DDoS:** În luna aprilie a anului 2022 mai multe site-uri oficiale guvernamentale au fost afectate de acest tip de atac cibernetic, printre care se numără și site-ul Guvernului României, al Ministerului Apărării, al Poliției de Frontieră și al Poliției Române. Oficialii instituțiilor au transmis atunci că accesul a fost blocat doar pentru utilizatorii site-urilor respective, interfața paginii web rămânând nealterată. Totodată, un grup de hackeri din Rusia a revendicat atacurile cibernetice, motivând dezbaterile în materie legislativă din acea perioadă. Pentru referință, la acea perioadă a fost pus în discuție ajutorul militar pe care România l-ar putea oferi Ucrainei pe fondul războiului dintre aceasta din urmă și Rusia. *Gruparea susține că liderul PSD ar fi promis „asistență maximă" în furnizarea de arme letale Ucrainei* [50], însă acesta din urmă, Marcel Ciolacu, susținea că gruparea a înțeles mesajul în mod eronat. Site-urile și-au reluat activitatea obișnuită următoarea zi după ce atacurile au fost raportate [50].
- **Atacurile cibernetice de tip ransomware asupra sistemelor medicale ale instituțiilor spitalicești din România:** La data de 15.05.2020 procurorii DIICOT[9] au efectuat percheziții domiciliare, având suspiciunea că un grup de infracțional organizat au atacat voluntar mai multe instituții din sectorul medical din România, prin pătrunderea în sistemele digitale ale acestora. Gruparea denumită ***Pentaguard*** a alterat integritatea datelor informatice și a întreprins infracțiunea fals informatic. Atacurile au fost de tip ransomware, iar hackerii au criptat datele stocate de pe echipamentele digitale, cerând răscumpărarea în schimbul recuperării acestora [51]. De menționat este și faptul că atacurile de acest gen continuă în rândul sistemelor spitalelor din România, astfel că în luna februarie a anului curent s-au înregistrat alterări în rândul a 18 instituții medicale, incident în urma căruia Ministerul Sănătății a transmis că *sistemul este nefuncțional, fișierele și bazele de date sunt criptate* [52].
- **Atacurile de tip defacement asupra mai multor site-uri ale unor instituții publice din România:** În ultima perioadă s-a conturat conceptul de ***hacktivism*** care constă în acțiuni de activism digital, influențând procesele decizionale ale scenelor politice, sociale și culturale [53]. În România un grup intitulat *Operation Romania* a dobândit notorietate și iar infracțiunile comise de aceștia (perturbarea funcționării sistemelor informatice, transfer neautorizat de date informatice, operațiuni legale cu dispozitive sau programe informatice) au luat amploare în anul 2023. Procurorii DIICOT au descoperit atunci că gruparea Operation Romania a înaintat o serie de atacuri de tip defacement asupra mai multor sisteme digitale ale unor instituții publice din țară, prin care alterau interfața site-urilor web și afișau mesaje politice, sociale sau culturale în scopul cauzei pe care o susțineau [54].

[9] DIICOT− Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism

Pentru ca aceste atacuri să fie evitate, este necesar să existe o strategie de securitate avansată, care să poată acționa împotriva atacatorilor și să prevină sensibilitatea datelor. Având o strategie puternică de securitate, erorile umane sunt semnificativ reduse, iar reputația site-urilor oficiale ar putea crește exponențial în materie de protecție digitală [55].

Capitolul 3. Studiu de caz – Percepția publicului asupra confidențialității informațiilor personale în relația cu instituțiile publice

Studiul de caz privind percepția publicului asupra confidențialității informațiilor personale în relația cu instituțiile publice reprezintă o investigație profundă a modului în care indivizii percep și gestionează confidențialitatea datelor lor personale atunci când interacționează cu instituțiile publice. Acest subiect este deosebit de relevant în era digitală actuală, în care datele personale sunt colectate și utilizate într-o varietate tot mai mare de contexte, iar preocupările legate de confidențialitate și securitate sunt tot mai accentuate [56].

Astfel, pe un eșantion de 100 de persoane care au interacționat cel puțin o dată cu o instituție publică, am reușit să iau pulsul la nivel de populație și să înțeleg nevoile cetățenilor în materie de digitalizare și modernizare în ceea ce privește tehnologia administrației publice.

Prin intermediul acestui studiu de caz, se explorează atitudinile, cunoștințele și comportamentele publicului în ceea ce privește furnizarea informațiilor personale către instituțiile publice, precum administrațiile locale, guvernul central sau alte entități publice. De asemenea, se analizează modul în care factori precum transparența proceselor, nivelul de încredere în instituțiile publice și gradul de informare influențează percepția individului asupra confidențialității datelor sale personale.

Totodată, se urmărește identificarea unor posibile discrepanțe între percepția publicului și practicile reale de colectare și gestionare a datelor personale de către instituțiile publice. De asemenea, se propun recomandări și soluții pentru îmbunătățirea transparenței, securității și respectării confidențialității datelor personale în relația cu instituțiile publice, în vederea consolidării încrederii și protejării drepturilor individuale. Așadar, se evidențiază importanța dialogului și colaborării continue între instituțiile publice și cetățeni pentru asigurarea unei protecții eficiente a datelor personale și pentru promovarea unei relații de încredere reciprocă. Astfel, acest studiu reprezintă un instrument valoros pentru înțelegerea și îmbunătățirea relației dintre public și instituțiile publice în contextul protejării confidențialității informațiilor personale. Prin intermediul unui chestionar derulat pe platforma *Google Forms* am realizat studiul de caz intitulat: ***Percepția publicului asupra confidențialității informațiilor personale în relația cu instituțiile publice***, din care am extras următoarele:

- Date demografice

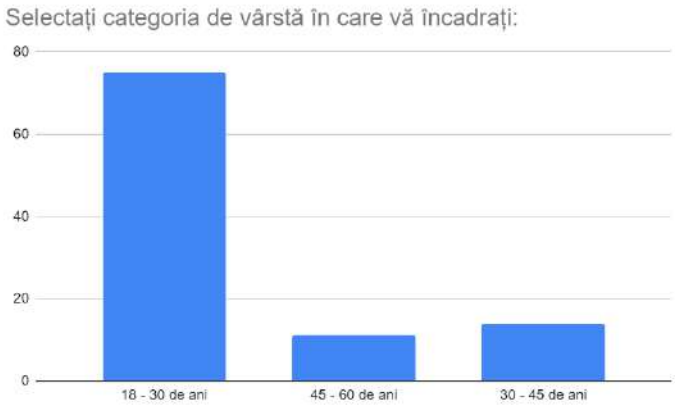

Fig. 4. Categoria de vârstă a respondenților

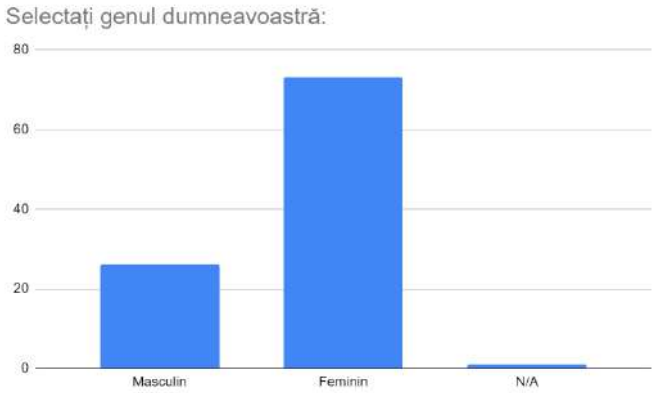

Fig. 5. Genul respondenților

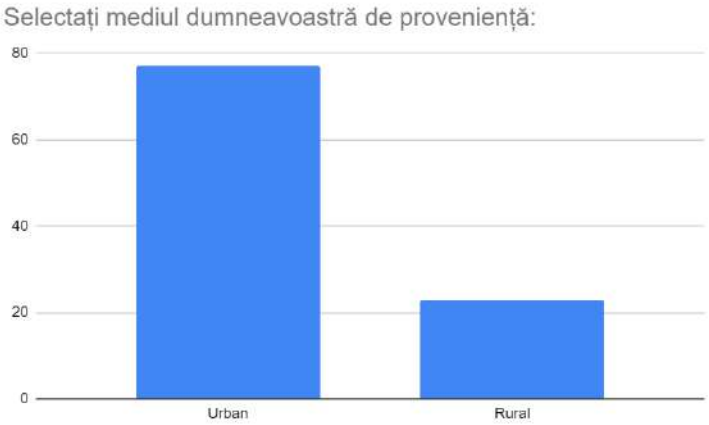

Fig. 6. Mediul de proveniență al respondenților

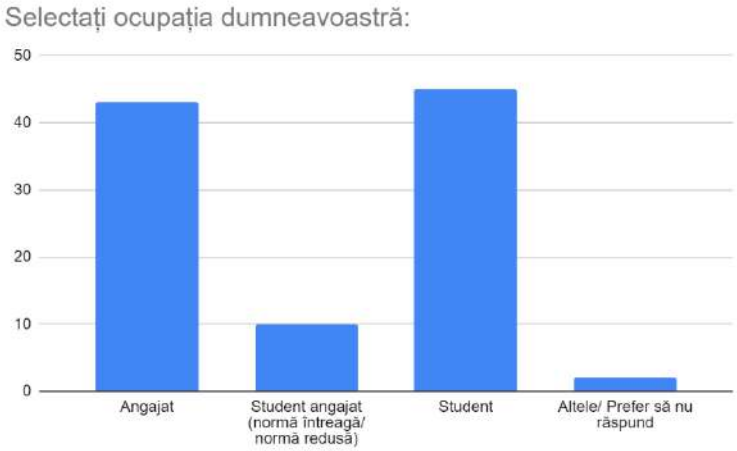

Fig. 7. Ocupația respondenților

Observăm din aceste date demografice că respondenții sunt împărțiți în diverse categorii – așadar, diversitatea este prezentă. Ne dăm seama după aceasta că 73% dintre aceștia au sexul masculin, 26% sex feminin, în timp ce 1% preferă să nu dezvăluie. În continuare, categoria de vârstă predominantă este între 18 și 30 de ani, lucru care dă de înțeles că populația tânără a

interacționat, cel puțin o dată, în scris sau nu, cu o instituție publică din România. De asemenea, studenții și angajații cu norma întreagă și-au arătat interesul pentru completarea acestui chestionar, în timp ce 77% dintre aceștia provin din mediul urban, iar restul de 23% provin din mediul rural.

- Întrebările destinate cercetării și studiului de caz

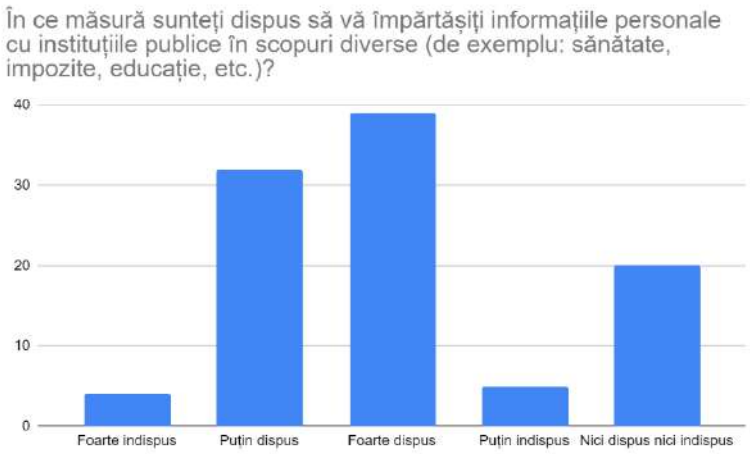

Fig. 8. Împărtășirea informațiilor personale de către respondenți în relația cu instituțiile de stat

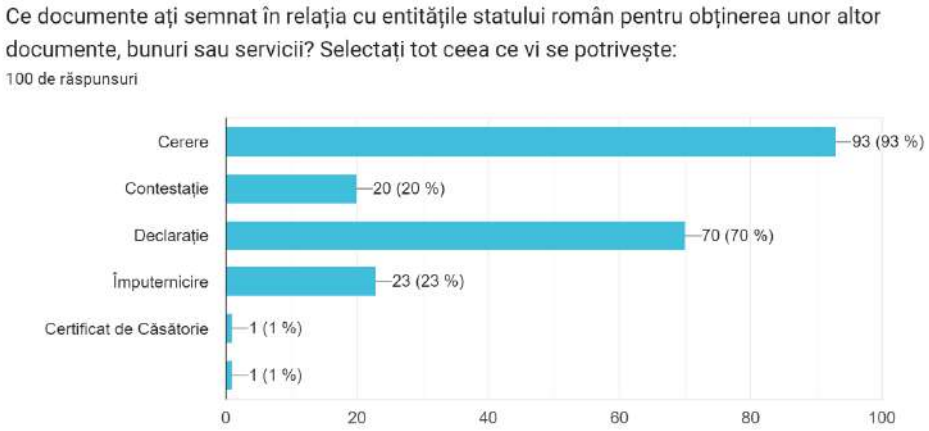

Fig.9. Documentele semnate de către respondenți în relația cu instituțiile statului

Observăm că documentele frecvent accesate de respondenți, prezente în figura 9 sunt cele pe care le putem întâlni atunci când accesăm un serviciu oferit de instituțiile administrației publice din România.

Cererea – prin definiție, conform Dicționarului Explicativ, reprezintă documentul care exprimă acțiunea de a solicita un anume serviciu [57], iar în termeni economici, putem face referință către oferte, prețuri și achiziții: cantitatea de produs pe care un client dorește să o acceseze în baza unei cheltuieli și o perioadă determinată de timp [58]

Contestația – este acel document prin care se atacă o anumită decizie sau un alt act, pe cale legală [59]

Declarația – Reprezintă o relatare făcută în scris prin care o persoană fizică se adresează unei entități de stat [60]

Împuternicirea și certificatul de căsătorie vorbesc de la sine, astfel că un cetățean poate realiza li poate atinge mai multe reușite în baza acestor documente.

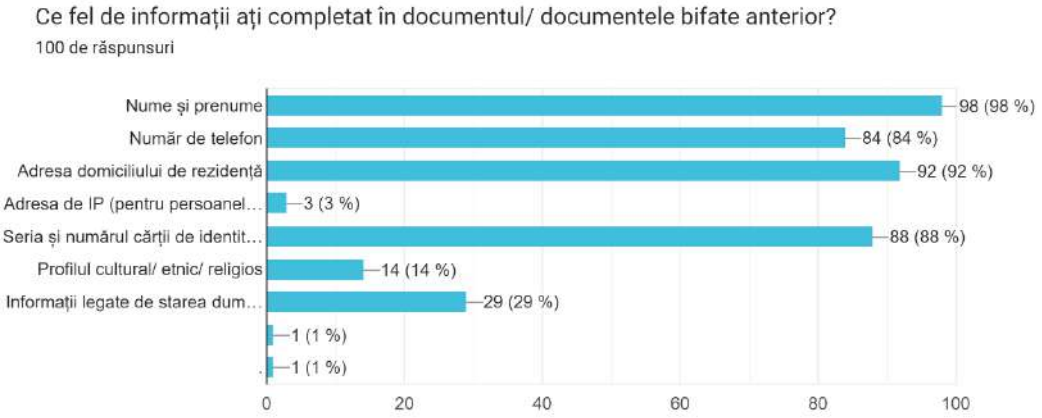

Fig. 10. Informațiile completate de către respondenți în documentele semnate la întrebarea anterioară a chestionarului

Următoarea întrebare s-a focusat pe informațiile completate de către respondenți în urma accesării documentelor prezentate în figura 9. O majoritate de 98% au declarat că informațiile generale și uzuale precum nume, prenume și adresa domiciliului au fost printre cele mai solicitate. Deși tipurile de documente diferă, fie că vorbim despre o declarație sau o cerere, informațiile mai sus prezente în figura 10 au fost completate cu precădere.

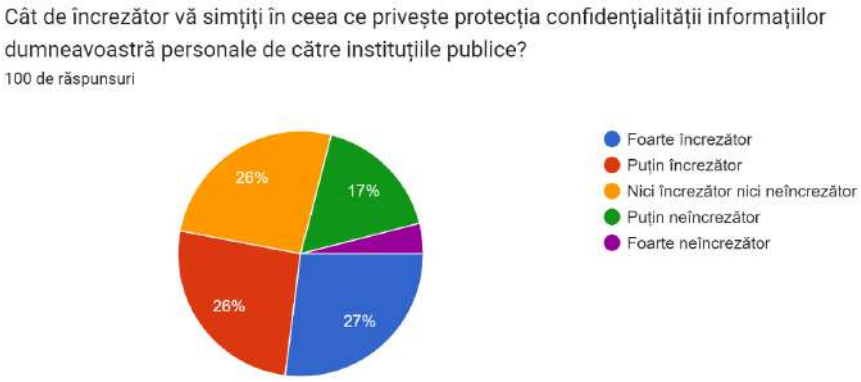

Fig. 11. Încrederea respondenților asupra protecției confidențialității informațiilor personale în relația cu instituțiile publice

Încă din primele întrebări destinate cercetării și studiului de caz regăsim *Cererea* ca fiind cea mai completată în rândul respondenților, datorită procentului de 93%. Fiind documentul care necesită completarea celor mai multe date [*a se vedea Anexa B*], este probabil, cea mai cunoscută formă de adresare către o instituție sau o entitate publică. *Declarația*, pe de altă parte, ocupă locul al II-lea în topul documentelor semnate de respondenții chestionarului, însumând un procent de aproape 70% dintre persoane. Acest document transpune nevoile instituției de a oferi beneficiarului (să presupunem, de data aceasta, că beneficiarul este însuși cetățeanul) un anumit privilegiu, sau serviciu, de exemplu, declarația pe proprie răspundere aferentă perioadei pandemiei de COVID-19, perioadă în care completarea acesteia era imperios necesară în momentul în care un individ părăsea locuința de domiciliu, conform OM nr.3/2020 [*a se vedea Anexa C*]. *Contestația, Împuternicirea* și *Certificatul de căsătorie* reprezintă alte documente pe care respondenții le-au completat în relația cu entitățile statului român din administrația publică, toate cele 3 având necesarul de informații personale pentru validare [*a se vedea Anexele D, E, F*].

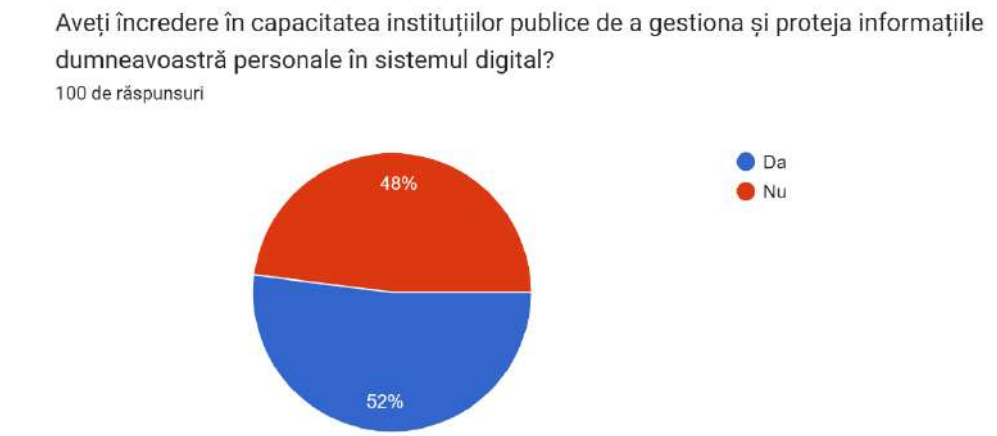

Fig. 12. Încrederea respondenților asupra capacității instituțiilor publice de a gestiona și proteja informațiile personale în sistemul digital

După această întrebare portretizată în figura 12, respondenților li s-a solicitat să motiveze răspunsul, pentru a oferi o imagine mai clară și în ansamblu a încrederii, respectiv neîncrederii asupra capacității instituțiilor publice de a gestiona informații personale ca un întreg. Răspunsurile au variat, astfel că motivațiile au avut drept răspunsuri predominante afirmațiile *„Instituțiile nu sunt îndeajuns de digitalizate pentru a gestiona un volum semnificativ de date, cu atât mai mult date personale”* și *„Instituțiile acționează conform legilor propuse de Uniunea Europeana, ceea ce îmi conferă o siguranță că datele mele personale nu pot fi compromise”.*

De asemenea, cei 52% care au confirmat că au încredere în capacitatea instituțiilor publice de a gestiona și proteja informațiile personale în sistemul digital au afirmat și că nu consideră că există un potențial risc, iar ceilalți 48% care sunt împotrivă au afirmat și faptul că în rândul funcționarilor publici există o *oarecare* ignoranță, respectiv nepăsare atunci când gestionează datele lor personale.
În continuare, respondenții au fost întrebați de măsurile de securitate pe care aceștia le consideră potrivite atunci când datele personale sensibile se regăsesc la nivelul entităților publice de stat din România.
Aceștia și-au arătat interesul pentru softuri performante, despre care am amintit în capitolul anterior, alături de antiviruși și cheile puternice de encripție, iar monitorizarea și prevenția traficului de date ar putea face referire la modul în care instituțiile gestionează timpul de lucru petrecut sub umbrela conexiunii la internet.

Respondenții au fost întrebați, totodată și de măsurile de securitate din realitate, care ar putea fi aplicate în rândul instituțiilor publice, atunci când ne referim la stocarea documentelor în format fizic.

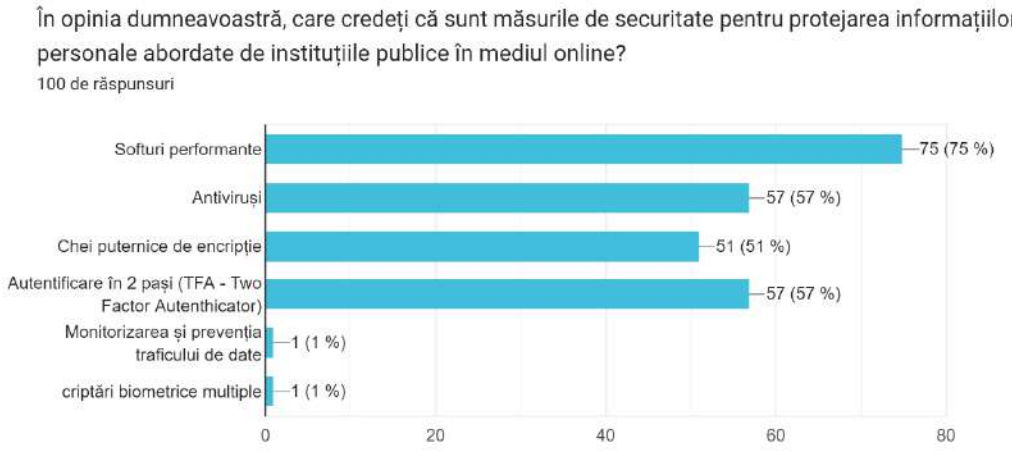

Fig. 13. Măsurile de securitate alese de respondenți în format digital

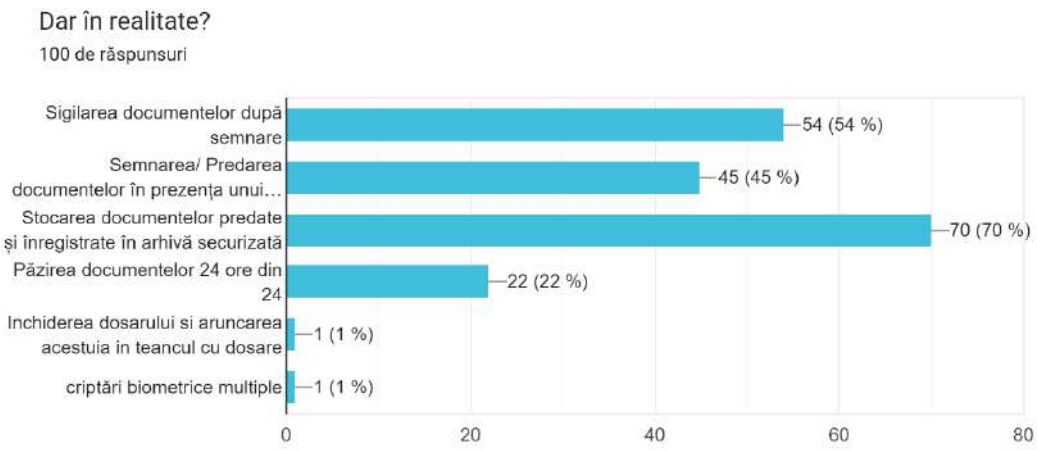

Fig. 14. Măsurile de securitate preferate de respondenți în realitate

Observăm o preferință crescută pentru o arhivă securizată, sau, mai exact o cameră, o sală specială unde arhivarea documentelor să se poată realiza fără riscuri și fără întreruperi, sau teama că anumite documente pot fi rătăcite sau distruse. Sigilarea documentelor, reprezintă și ea o măsură de securitate preferată de respondenți, probabil pentru că oferă o siguranță crescută cetățeanului după completarea și predarea documentului cu pricina.

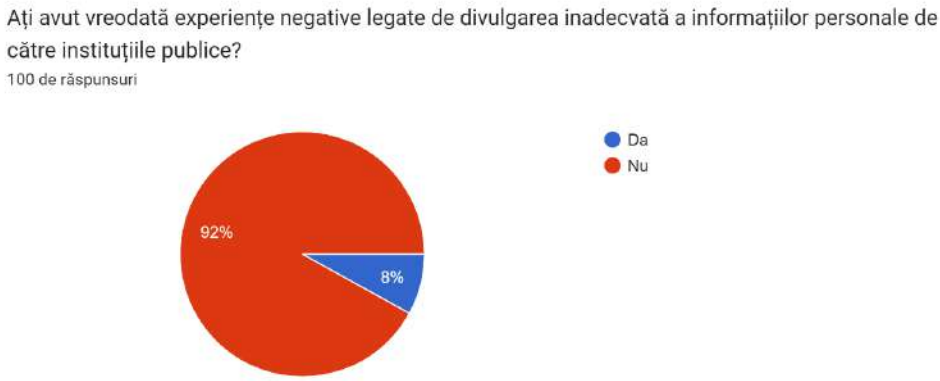

Fig. 15. Eventuale experiențe negative în ceea ce privește divulgarea inadecvată a datelor personale ale respondenților

Întrebați dacă au avut parte de experiențe negative legate de divulgarea inadecvată a informațiilor personale de către instituțiile publice, respondenții au declarat, în procent de 8% că da – iar motivând experiența, în mare parte aceștia susțin că au fost contactați fără acordul lor de către companii terță parte, precum o companie de telefonie care propunea achiziționarea de abonamente de telefonie, fie instituțiile de jurnalism au luat legătura cu ei pentru susținerea unor materiale din media, respondenții necunoscând sursa care a oferit acces la numerele de telefon personale.

Participanții la chestionar au declarat la întrebarea *Considerați că oamenii în general sunt destul de conștienți cu privire la drepturile lor legate de confidențialitate în interacțiunile cu instituțiile publice?* că majoritatea oamenilor nu sunt informați (65%), dar că 19% da. Acest lucru se datorează faptului că o mare parte dintre cetățeni limitează interacțiunile cu entitățile statului Român, din dorința de a evita aglomerația și procesul îngreunat de procesare a cererilor și documentelor, potrivit aceluiași chestionar prezent.

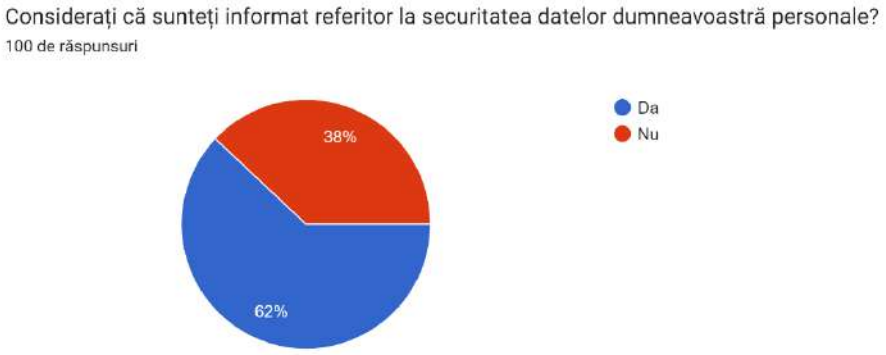

Fig. 16. Informarea personală a respondenților cu privire la securitatea datelor lor personale

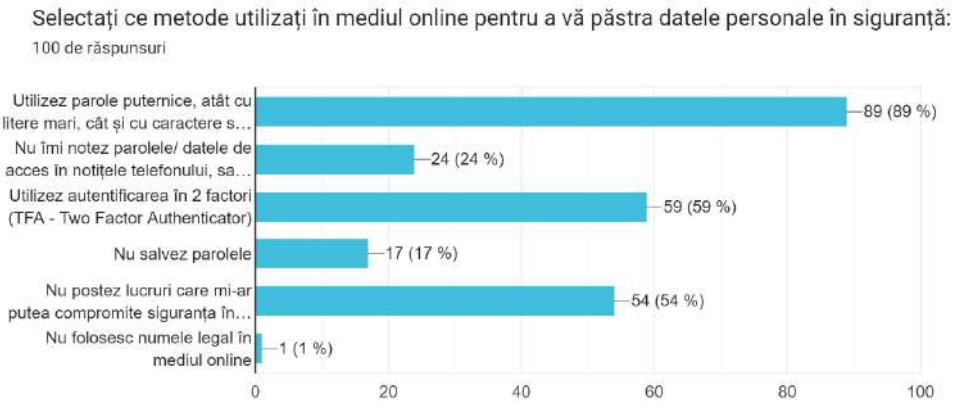

Fig. 17. Metodele de securitate utilizate de respondenți pentru a-și păstra datele în siguranță

Observăm în urma figurilor 16 și 17 că respondenții, în proporție de 62% au cunoștințe în materie de securitatea informațiilor personale și că 89% utilizează parole puternice, atât cu litere mari, cât și cu caractere speciale. 59% dintre aceștia nu își notează undeva la îndemână credențialele[10] unui cont, iar ceea ce personal am regăsit foarte adecvat, chiar dacă se regăsește în proporție de 1% – nu folosesc numele legal în mediul online, ceea ce ne trimite cu gândul la o securitate avansată, metodă utilizată, firește, fără scopul furtului de identitate despre care am amintit în capitolele anterioare.

În urma unui scenariu propus în chestionarul pentru studiul de caz: *Să presupunem prin absurd că datele dumneavoastră au fost compromise pe un site al unei instituții publice. Ce măsuri considerați că trebuie să luați pentru a rezolva problema?*, respondenții și-au arătat intenția, în proporție de 59% că se vor adresa conducătorului instituției respective, fiind împuterniciți de lege, iar 58% au declarat că vor depune o plângere la organele abilitate în vederea soluționării incidentului posibil apărut.

La întrebarea *Având în vedere răspunsurile dumneavoastră de până acum, în relația cu instituțiile publice preferați să completați documente online sau să rămâneți la metoda tradițională, cunoscută sub denumirea populară de „dosar cu șină”?* respondenții au preferat, într-un număr semnificativ (89%) completarea documentelor prin intermediul digital, urmând ca ceilalți să aleagă metoda tradițională. Rugați să motiveze alegerea făcută, aceștia au afirmat că în intermediul online funcționarii publici se pot ocupa mult mai rapid de anumite cereri și pot înregistra mult mai ușor anumite documente și, cel mai important în opinia acestora – timpul de așteptare este semnificativ redus. De cealaltă parte, metoda tradițională rămâne, în continuare,

[10] Credențiale – elemente utilizate pentru accesul la anumite informații sau resurse. Termenul, în general acoperă informații-pereche, precum nume de utilizator-parolă, număr de telefon-parolă, etc. [70]

pentru cei 11% dintre respondenți o metodă sigură, clară și eficientă, întrucât persoana respectivă poate vedea în timp real procesul și felul cum sunt gestionate documentele de către funcționarii publici. O motivație prezentă a unui respondent, se încadrează în limbajul colocvial cu afirmația „negru pe alb", ceea ce ne trimite cu gândul ca atunci când documentele sunt semnate în format fizic, nu există îndoiala că autorul este însuși persoana semnatară.

Întrebați dacă au fost victimele unor atacuri cibernetice în trecut, respondenții, în proporție de 18% au afirmat că au experimentat un asemenea lucru, motivându-și răspunsurile prin acțiuni de hacking asupra conturilor de social media prin metoda social engineering, amenințări din partea unor persoane necunoscute care cumva, au reușit să identifice adresa de IP, atacuri de tip ransomware, respectiv furt de identitate.

În ceea ce privește îmbunătățirea procesului de colectare a datelor cu caracter personal, respondenții au considerat absolut necesară pregătirea și formarea profesională a angajaților instituțiilor publice din România, dar și sortarea și verificarea periodică a datelor colectate. Celelalte răspunsuri s-au concentrat asupra metodelor tehnologice de a monitoriza acest proces, cât și asupra procedurilor adoptate la nivel de instituție.

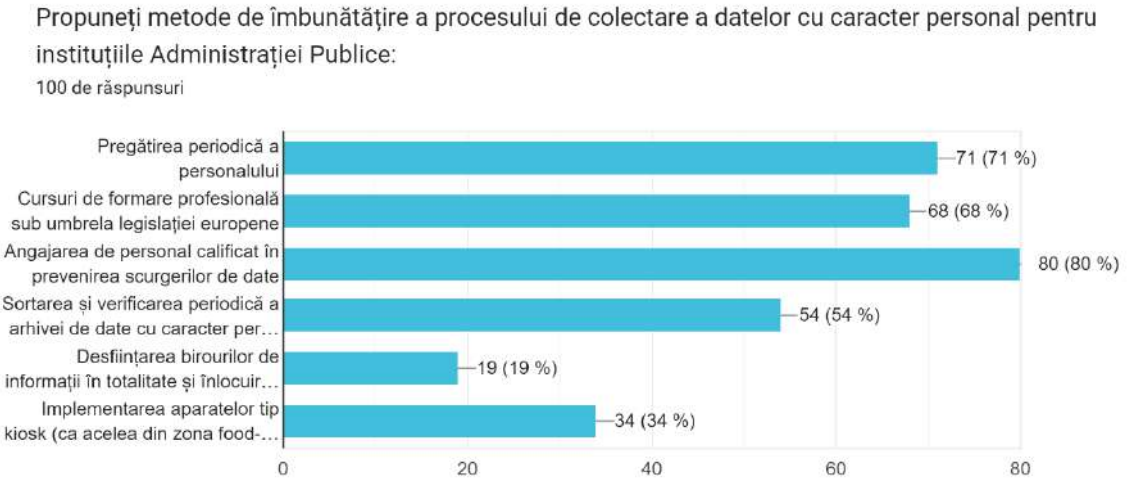

Fig. 18. Metode propuse de respondenți pentru îmbunătățirea procesului de colectare a datelor cu caracter personal

3.1. Conștientizarea cetățenilor cu privire la datele colectate de către entitățile administrației publice

Coroborând toate aspectele prezentate anterior, este deosebit de important ca cetățenii României să fie conștienți și să fie de acord cu privire la datele colectate de către entitățile administrației publice din mai multe motive fundamentale. Nu ne putem rezuma doar la aspectele legislative, ci ne putem îndrepta și către aspectele sensibile, precum transparența ca principal atu, ori securitatea, din punct de vedere al tehnologiei informație. Regăsim, astfel, câteva principii pe care cetățenii se pot baza atunci când optează să apeleze la un serviciu oferit de administrația publică, prin prisma documentelor și a procedurilor scrise:

1. Respectarea drepturilor individuale: Cetățenii au dreptul la confidențialitate și protecția datelor personale conform legislației în vigoare, cum ar fi Regulamentul General privind Protecția Datelor (GDPR). Prin conștientizarea și consimțământul cu privire la datele colectate, cetățenii își pot exercita aceste drepturi și pot avea control asupra informațiilor lor personale. Ba mai mult, respectarea drepturilor individuale în ceea ce privește confidențialitatea și protecția datelor personale este un principiu fundamental al legislației privind protecția datelor, întărit, după cum am menționat anterior, de Regulamentul General privind Protecția Datelor în Uniunea

Europeană. Acest aspect este esențial pentru un stat pentru a se asigura că cetățenii au control asupra informațiilor lor personale și că aceste informații sunt tratate în mod corespunzător și în conformitate cu normele legale [22] [24]. Ne bazăm, de asemenea și pe următoarele drepturi:

- Dreptul la confidențialitate: Cetățenii au dreptul fundamental de a-și păstra informațiile personale în siguranță și de a decide cine are acces la aceste informații. Prin respectarea confidențialității datelor personale, este de așteptat ca entitățile administrației publice să protejeze intimitatea și viața privată a cetățenilor [28].
- Dreptul la protecția datelor personale: Acest drept implică asigurarea că datele personale ale cetățenilor sunt colectate și prelucrate în mod legal, corect și transparent. Protecția datelor personale include măsuri pentru prevenirea accesului neautorizat, pierderii, distrugerii sau deteriorării datelor [19].

Prin conștientizarea și consimțământul cu privire la datele colectate, cetățenii devin informați cu privire la modul în care informațiile lor personale sunt utilizate și pot decide în mod activ asupra acestui aspect. Acest lucru le oferă posibilitatea de a-și exercita drepturile individuale, cum ar fi dreptul de acces la datele lor, dreptul de rectificare a informațiilor incorecte sau incomplete, dreptul de ștergere a datelor („dreptul de a fi uitat"), dreptul la portabilitatea datelor și altele [24].
Prin obținerea consimțământului adecvat, entitățile administrației publice demonstrează respectarea drepturilor individuale ale cetățenilor și le oferă posibilitatea de a avea control asupra informațiilor lor personale. Acest proces contribuie la consolidarea încrederii între cetățeni și autorități și la promovarea unei culturi a respectării confidențialității și protecției datelor personale [22].

3. **Transparența și responsabilitatea**: Prin obținerea consimțământului cetățenilor, entitățile

administrației publice demonstrează transparență și responsabilitate în gestionarea datelor personale. Acest lucru contribuie la construirea încrederii între cetățeni și autorități și a unui echilibru între serviciile furnizate și activitatea funcționarilor publici. Transparența și responsabilitatea sunt două principii fundamentale în ceea ce privește colectarea și prelucrarea datelor personale [35]. Aceste aspecte constituie o bază temeinică pentru a asigura încrederea cetățenilor în modul în care sunt gestionate informațiile lor personale și pentru a respecta standardele legale și etice relevante. Transparența se referă la obligația entităților administrației publice de a comunica deschis și clar cu cetățenii cu privire la colectarea, stocarea și utilizarea datelor personale. Prin transparență, cetățenii sunt informați cu privire la scopul colectării datelor lor, categoriile de date colectate, modul în care vor fi prelucrate și dacă vor fi partajate cu terțe părți [23]. O comunicare transparentă contribuie la construirea încrederii și la consolidarea relației de încredere între cetățeni și autorități. De cealaltă parte, responsabilitatea se referă la obligația entităților administrației publice de a acționa în conformitate cu legislația privind protecția datelor și de a asigura că datele personale sunt tratate în mod corespunzător și în conformitate cu standardele etice [1]. Aceasta implică implementarea măsurilor de securitate adecvate pentru protejarea datelor personale împotriva accesului neautorizat sau utilizării neadecvate. Totodată, responsabilitatea include și respectarea drepturilor individuale ale cetățenilor în ceea ce privește protecția datelor lor personale [34] [23].

4. **Evitarea abuzurilor și utilizării neautorizate**: Acest lucru ajută la prevenirea abuzurilor și utilizării neautorizate a informațiilor personale. Evitarea abuzurilor și utilizării neautorizate a datelor personale este un aspect ce nu trebuie ignorat în protejarea confidențialității și securității informațiilor individuale. Prin obținerea consimțământului informat, cetățenii sunt informați cu privire la scopul colectării datelor lor și modul în care aceste informații vor fi utilizate [22]. Această transparență și claritate în comunicare sunt esențiale pentru prevenirea abuzurilor și utilizării neautorizate a datelor personale. De exemplu:

- Scopul colectării datelor: Prin consimțământul informat, cetățenii sunt informați cu privire la motivul pentru care datele lor personale sunt colectate. Este important ca entitățile administrației publice să ofere explicații clare și detaliate cu privire la scopul colectării datelor, astfel încât cetățenii să înțeleagă de ce informațiile lor sunt necesare [26].

- Utilizarea datelor: Cetățenii trebuie să fie informați cu privire la modul în care datele lor personale vor fi utilizate. Acest lucru include informații despre cum vor fi prelucrate datele, cine va avea acces la ele, dacă vor fi partajate cu alte terțe părți (acolo unde este cazul) și în ce scopuri vor fi utilizate informațiile [24].

- Prevenirea abuzurilor: Prin furnizarea unei descrieri clare a modului în care vor fi utilizate datele personale, se reduce riscul de abuzuri sau utilizări neautorizate. Cetățenii în cunoștință de cauză pot decide dacă doresc să ofere consimțământul pentru colectarea și utilizarea informațiilor lor, având astfel control asupra propriilor date. Acest lucru este aplicabil și în materie de campanii publicitare, de marketing, sau electorale [16].

- Protecția informațiilor personale: Obținerea consimțământului informat nu numai că ajută la prevenirea abuzurilor, dar și la protejarea datelor personale împotriva utilizării neautorizate. Cetățenii pot fi mai atenți și mai vigilenți în ceea ce privește informațiile pe care le furnizează, cunoscând în detaliu scopul și modalitatea de utilizare a acestora [16].

5. **Securitatea datelor**: Securitatea datelor reprezintă un aspect crucial în protejarea tuturor

informațiilor sensibile ale cetățenilor și în menținerea încrederii în modul în care entitățile administrației publice gestionează și protejează datele personale. Consimțământul cu privire la datele colectate poate include și aspecte legate de securitatea acestor date, ceea ce înseamnă informarea cu privire la măsurile de securitate luate pentru a proteja informațiile lor sensibile [16] [23]. Pentru a evidenția acest aspect, este nevoie să înțelegem:

- Importanța securității datelor: Securitatea datelor este deosebit de importantă pentru protejarea informațiilor personale ale cetățenilor împotriva accesului neautorizat, utilizării necorespunzătoare sau a pierderii acestora. Protejarea datelor sensibile este crucială pentru menținerea confidențialității și integrității informațiilor personale, precum datele de identificare, informațiile financiare sau de sănătate, care pot fi expuse riscului în absența unor măsuri adecvate de securitate [36] [27].

- Măsuri de securitate luate pentru protejarea datelor: Entitățile administrației publice pot implementa diverse măsuri de securitate pentru a proteja datele sensibile ale cetățenilor. Aceste măsuri pot include:

    - Criptarea datelor: Transformarea datelor într-un format codificat pentru a le proteja împotriva accesului neautorizat [34] [16].

    - Controlul accesului: Limitarea accesului la datele sensibile doar către persoanele autorizate și implementarea unor politici stricte de securitate [1].

    - Monitorizarea și auditarea: Supravegherea continuă a accesului la date, înregistrarea activităților și auditarea sistemelor pentru identificarea potențialelor amenințări sau incidente de securitate [8].

- Backup și recuperare a datelor: Realizarea de copii de rezervă ale datelor pentru a preveni pierderea acestora și pentru a asigura disponibilitatea informațiilor în caz de incidente [5].

6. **Personalizarea serviciilor și îmbunătățirea calității**: Prin colectarea datelor cu consimțământul cetățenilor, entitățile administrației publice pot oferi servicii personalizate și îmbunătăți calitatea acestora în funcție de nevoile și preferințele individuale [5].

- Personalizarea serviciilor se referă la adaptarea și furnizarea de servicii personalizate în funcție de preferințele, nevoile și comportamentul fiecărui cetățean în parte. Prin personalizarea serviciilor, entitățile administrației publice pot oferi o experiență mai individualizată și relevantă pentru cetățeni, ceea ce duce la o mai mare satisfacție și implicare din partea acestora. Aceasta poate include oferirea de recomandări personalizate, adaptarea interacțiunilor și comunicării în funcție de preferințele individuale, precum și furnizarea de servicii personalizate în funcție de nevoile specifice ale fiecărui cetățean [8] [16].

- Îmbunătățirea calității se referă la procesul continuu de evaluare, ajustare și optimizare a serviciilor oferite pentru a asigura o experiență mai bună pentru cetățeni [1]. Prin monitorizarea și analiza constantă a feedback-ului cetățenilor, entitățile administrației publice pot identifica punctele slabe, pot implementa îmbunătățiri și pot optimiza procesele pentru a oferi servicii de calitate superioară. Îmbunătățirea calității implică și dezvoltarea continuă a competențelor angajaților, implementarea de tehnologii inovatoare și adaptarea la schimbările din mediul extern pentru a răspunde eficient nevoilor și așteptărilor cetățenilor [1] [13].

Astfel, prin personalizarea serviciilor și îmbunătățirea calității, entitățile administrației publice pot crea o relație mai solidă și mai eficientă cu cetățenii, pot oferi servicii mai relevante și mai bine adaptate nevoilor acestora, și pot contribui la creșterea satisfacției și încrederii în instituțiile publice. Aceste aspecte sunt esențiale în asigurarea unei guvernări eficiente și orientate către cetățeni [1] [11].

7. **Conformitatea cu reglementările legale**: Conformitatea cu reglementările legale în ceea

ce privește protecția datelor este un aspect deosebit de important în contextul colectării și prelucrării informațiilor personale [39]. Respectarea cerințelor legale referitoare la protecția datelor este esențială pentru a asigura că entitățile administrației publice acționează în conformitate cu normele și reglementările stabilite pentru a proteja confidențialitatea și securitatea datelor personale ale cetățenilor. Obținerea consimțământului cetățenilor reprezintă un pilon fundamental al conformității cu legislația în vigoare, cum ar fi Regulamentul General privind Protecția Datelor (GDPR) în Uniunea Europeană sau alte legi naționale privind protecția datelor. Acest consimțământ trebuie să fie liber, informat și specific, iar cetățenii trebuie să fie complet conștienți de modul în care datele lor vor fi colectate, stocate, prelucrate și utilizate [22] [27].

Prin obținerea consimțământului adecvat, entitățile administrației publice demonstrează că respectă drepturile individuale ale cetățenilor în ceea ce privește protecția datelor lor personale. Acest lucru include informarea clară a cetățenilor cu privire la scopul colectării datelor, categoriile de date colectate, durata stocării acestora, drepturile pe care le au în legătură cu datele lor personale și alte aspecte relevante [46] [36].

În plus, obținerea consimțământului este un element esențial al responsabilității și transparenței în gestionarea datelor personale. Prin respectarea cerințelor legale și obținerea consimțământului adecvat, entitățile administrației publice pot construi încrederea cetățenilor în modul în care sunt

tratate datele lor și pot evita posibilele sancțiuni sau consecințe negative asociate nerespectării legislației privind protecția datelor. [19] [28]

În acest fel, conformitatea cu reglementările legale și obținerea consimțământului cetățenilor reprezintă un cadru legal și etic esențial pentru protejarea datelor personale și menținerea relației de încredere între cetățeni și entitățile administrației publice [34] [13]. Este un aspect crucial în era digitală actuală, în care protecția datelor personale este din ce în ce mai importantă [16].

3.2. Perspective și evaluare

Pentru că cetățenii sunt principalul obiectiv într-o societate modernă [61], se conturează importanța înțelegerii protecției în materie de procesare și stocare a datelor cu caracter confidențial și sensibil [35].

Populația României și-a exprimat în ultimii ani democratici (1990-2024 prezent) [62] o ușoară spre foarte puternică neîncredere în ceea ce privește factorul decizional din procesul politic. Această neîncredere este cauzată de mișcarea deosebit de rapidă și de influentă a mass-mediei, care are capacitatea de a afecta alegerile politice și gândirea cetățenilor la nivel politic și administrativ [62].

Din această cauză, putem să înțelegem că există o serie de perspective negative și pozitive pe care cetățenii se bazează atunci când aleg să intre în relații, contractuale sau nu, cu instituțiile publice ale statului român. [18].

Pe de-o parte, analizăm transparența instituțiilor publice ca fiind o virtute pe care acestea trebuie cu orice preț să o adopte și pe care să se bazeze în relația cu cetățenii [13]. Aceștia din urmă pot solicita în orice moment, de exemplu, informații referitoare la datele lor procesate [22]. Legea 52 din 2003 ne relatează prin intermediul articolului 3, alineatul d) faptul că entitățile publice cu capacitate decizională sunt obligate să ia în considerare recomandările survenite din partea oricărei persoane fizice interesate de procesul decizional, sau în procesul elaborării actelor normative [63].

Pe de altă parte, o responsabilitate crescută și o asumare puternică și validă din partea conducătorilor politici care guvernează, totodată, activitățile instituțiilor publice este așteptată de cetățeni, totul pentru a întări relația și pentru a fructifica dorințele ambelor părți implicate în procesul decizional și cel de protecție a datelor personale [18].

De menționat este și faptul că îngrijorarea cu privire la confidențialitate a cetățenilor este survenită tocmai din această posibilă dezinformare din mass-media [61] care ia cu asalt credințele și preferințele acestora în materie de proces decizional public sau politic.

Având în vedere tot ceea ce determină un cadru moral etic pentru cetățeni, în raport cu studiul de caz de la punctul **3** al prezentei lucrări, consider că toți cei ce au întreținut raporturi cu instituțiile publice din cadrul administrației publice din România necesită o mai puternică aprofundare a drepturilor lor în materie de protecție a datelor cu caracter personal. Fiind un aspect ce nu poate fi neglijat, ori lăsat la voia întâmplării, oamenii trebuie să posede informații relevante pe care să le poată folosi ulterior în relația cu statul român, pentru a putea determina dacă la un moment dat s-au produs, sau nu erori în ceea ce privește o scurgere de date sensibile sau informații care prin natura lor aduc un prejudiciu persoanei vătămate.

Discuții/ Concluzii

Într-o eră în care tehnologia a devenit omniprezentă în activitățile administrative [35], protecția datelor cu caracter personal reprezintă un aspect critic în administrația publică din România [16]. Această protecție nu este doar o necesitate legală impusă de reglementările europene și

naționale, cum ar fi Regulamentul General privind Protecția Datelor (GDPR), ci și un imperativ moral și social. Concentrarea asupra importanței protejării datelor personale în contextul administrației publice din România, subliniind consecințele pozitive și negative ale unei abordări adecvate sau deficitare în acest sens, reflectă o mai bună imagine de ansamblu asupra credințelor pe care cetățenii români le au.

Protecția datelor cu caracter personal reprezintă un pilon al respectării drepturilor individuale și a intimității cetățenilor. Într-o societate democratică, fiecare individ are dreptul la confidențialitate și la controlul informațiilor sale personale. Administrația publică trebuie să se asigure că datele colectate sunt utilizate în mod legal și transparent și că indivizii au posibilitatea de a-și exercita drepturile privind datele personale, cum ar fi dreptul la acces, rectificare sau ștergere [22] [48].

Protecția datelor este esențială pentru menținerea încrederii cetățenilor în instituțiile publice [34], cea ce trimite cu gândul, din nou, asupra transparenței decizionale. Atunci când cetățenii au încredere că datele lor sunt gestionate în mod responsabil și în conformitate cu standardele de securitate și confidențialitate, ei sunt mai predispuși să interacționeze cu instituțiile publice și să participe la procesele guvernamentale. O pierdere a încrederii poate afecta grav relația dintre guvern și cetățeni, subminând legitimitatea instituțiilor publice.

Fiind un element cheie pentru asigurarea eficienței și calității serviciilor publice, comportamentul și conștientizarea funcționarilor publici în ceea ce privește gestionarea unui volum mare de date confidențiale, reprezintă baza pe care cetățenii o iau în considerare atunci când au decizia de a colabora cu oricare dintre instituțiile administrației publice. Datele personale sunt adesea utilizate în procesele administrative, de la evidența populației și serviciile sociale, până la gestionarea dosarelor fiscale sau acordarea de ajutoare de stat. O gestionare corectă a acestor date contribuie la îmbunătățirea eficienței proceselor administrative și la furnizarea unor servicii publice mai eficiente și mai personalizate [2].

Romania este obligată să respecte reglementările stricte în ceea ce privește protecția datelor cu caracter personal, inclusiv GDPR-ul. Administrația publică trebuie să se conformeze acestor reglementări pentru a evita sancțiuni legale și pentru a asigura respectarea drepturilor cetățenilor. Neconformitatea cu GDPR poate atrage cu sine amenzi substanțiale și poate afecta negativ imaginea și credibilitatea instituțiilor publice și cu atât mai mult, imaginea conducătorilor politici.

Protecția datelor cu caracter personal nu trebuie să fie privită ca un obstacol pentru inovare și dezvoltare tehnologică, ci dimpotrivă, poate stimula inovarea responsabilă. Atunci când instituțiile publice investesc în soluții tehnologice care respectă principiile protecției datelor, ele demonstrează angajamentul față de respectarea drepturilor individuale și construiesc încrederea cetățenilor în utilizarea tehnologiei în scopul îmbunătățirii serviciilor publice [64].

Așadar, protecția datelor cu caracter personal în administrația publica din România este esențială pentru respectarea drepturilor cetățenilor, menținerea încrederii în instituțiile publice, eficientizarea serviciilor publice, conformitatea cu reglementările legale și promovarea inovării responsabile. O abordare adecvată în acest sens nu numai că respectă principiile fundamentale ale democrației și drepturile individuale, dar poate contribui și la construirea unei societăți digitale mai sigure, mai transparente și mai progresiste în Romania.

Iar dacă ne raportăm din punct de vedere contractual, ori în raporturile de muncă, securitatea datelor personale și respectarea regulamentului GDPR sunt deosebit de importante din mai multe motive esențiale [65]:

- În primul rând, persoana care prestează activitatea în baza unui contract este pe deplin îndreptățită să își cunoască drepturile și obligațiile în raporturile de muncă, iar dreptul de a fi informat cu privire la acțiunile pe care angajatorul le va întreprinde pe toată

perioada contractului este un drept esențial, care poate facilita transparența în ceea ce privește activitatea desfășurată [65].

- Vorbim despre o confidențialitate care trebuie să fie absolut respectată, întrucât prevenirea abuzurilor sau posibile scurgeri de date nu sunt excluse în cadrul unei unități care activează cu mai mult de 10 angajați/ lucrători, caz în care este necesară și impunerea unui contract colectiv de muncă [66].
- Departamentul de Resurse Umane, fiind structura din organizație care are acces la cele mai multe date personale, fie că discutăm despre domeniul privat sau cel public, operează totodată și cele mai complexe procese de prelucrare [65]. Acest departament trebuie să se angajeze în aceste procese cu o responsabilitate sporită, pentru a evita orice prelucrare abuzivă. Personal, activând într-o organizație care oferă servicii de resurse umane, volumul de informații pe care îl prelucrez este semnificativ cantitativ, iar în eventualitatea în care s-a produs o greșeală este necesară o documentație în prealabil pentru a justifica eroarea respectivă. Fiind departamentul care cunoaște absolut toate detaliile angajaților, acesta deține informații precum: nume, prenume, adresă de domiciliu (la semnarea contractului este necesară procesarea cărții sau a buletinului de identitate), sexul, cetățenia, data și locul nașterii, datele din actele de stare civilă, informații despre copii, sau persoanele pe care angajatul le are în grijă, e-mail, număr de telefon, situație familială, date din permisul de conducere indiferent de categorie, situația economică și financiară și, după caz, situația militară sau preferințe politice/ religioase.

Referitor la subiectul securității naționale, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) activează în raport cu Carta Drepturilor Fundamentale a Uniunii Europene, asigurându-se astfel de conformitatea normelor pe care organizațiile le pun în practică atunci când gestionează un număr mare de date și informații sensibile [67]. ANSPDCP joacă un rol deosebit de important în ceea ce privește gestiunea corectă a acestor informații, monitorizând companii de telefonie mobilă, de unde se consideră ca fluxul de date ar fi cantitativ crescut față de alte instituții abilitate cu legislația națională și europeană [64]. Organul se ocupă și cu informarea cetățenilor în materie de viață privată și încălcarea drepturilor fundamentale guvernate de politicile europene [64]. Constituția României și legislația derivată, inclusiv Codul Civil și Codul Penal, consacră protecția vieții private. Articolele 26 și 28 din Constituție subliniază respectarea și protejarea vieții intime, familiale și private, inclusiv inviolabilitatea corespondenței [68]. În contextul actual geopolitic și al amenințărilor teroriste, statul român a adoptat măsuri pentru securitatea cibernetică și a comunicațiilor, afectând direct viața privată a cetățenilor [64]. Măsurile constau în creșterea semnificativă a numărului mandatelor de interceptare emise de Serviciul Român de Informații (SRI) din ultimii ani, fapt ce a generat preocupări privind libertățile individuale. Cu toate acestea, legislația prevede măsuri stricte pentru protejarea datelor obținute prin interceptări, acestea fiind utilizate doar în scopul probării infracțiunilor și distruse ulterior dacă nu sunt relevante pentru caz. Procurorii sunt obligați să informeze subiecții interceptărilor și să asigure confidențialitatea datelor, așa cum am menționat în capitolele anterioare [64].

În concluzie, asistăm la un progres semnificativ în ceea ce privește traseul evoluției procedurilor de protecție a datelor cu caracter personal, începând cu anul 1990, după perioada regimului comunist [64]. Acest lucru se datorează faptului că până în anul 1989 inclusiv, practicile totalitariste de la acea vreme încălcau pe deplin drepturile și libertățile cetățenilor – de la interceptarea apelurilor telefonice fără vreo documentație în prealabil (așa cum se practică astăzi în rândul proceselor penale, de exemplu), până la urmărirea persoanelor vizate, fără ca acestea să cunoască acest aspect. Odată cu instaurarea regimului democratic în România, conducătorii au dorit să se alinieze cu standardele europene și să pună în lumină protejarea tuturor drepturilor și libertăților oamenilor – inclusiv protecția datelor cu caracter personal [64].

Anexa A. Întrebările adresate participanților la chestionar

Secțiunea I – Acordul pentru prelucrarea datelor personale

1. *Am citit şi sunt de acord cu prelucrarea datelor cu caracter personal în scopuri academice şi am luat la cunoştinţă că acestea vor fi folosite doar în scopul cercetării temei prezentate anterior*.

Secțiunea II – Întrebări comune pentru clasificarea respondenților

1. Selectați categoria de vârstă în care vă încadrați.
2. Selectați genul dumneavoastră
3. Selectați mediul dumneavoastră de proveniență
4. Selectați ocupația dumneavoastră

Secțiunea III – Întrebările destinate cercetării și studiului de caz

1. În ce măsură sunteți dispus să vă împărtășiți informațiile personale cu instituțiile publice în scopuri diverse (de exemplu: sănătate, impozite, educație, etc.)?
2. Ce documente ați semnat în relația cu entitățile statului român pentru obținerea unor altor documente, bunuri sau servicii? Selectați tot ceea ce vi se potrivește
3. Ce fel de informații ați completat în documentul/ documentele bifate anterior?
4. În documentele pe care le-ați completat ați fost informat referitor la procedura de utilizare și stocare a datelor personale?
5. Cât de încrezător vă simțiți în ceea ce privește protecția confidențialității informațiilor dumneavoastră personale de către instituțiile publice?
6. Aveți încredere în capacitatea instituțiilor publice de a gestiona și proteja informațiile dumneavoastră personale în sistemul digital?
7. Motivați răspunsul anterior
8. În opinia dumneavoastră, care credeți că sunt măsurile de securitate pentru protejarea informațiilor personale abordate de instituțiile publice în mediul online?
9. Dar în realitate?
10. Ați avut vreodată experiențe negative legate de divulgarea inadecvată a informațiilor personale de către instituțiile publice?
11. Dacă ați răspuns cu ***DA*** la întrebarea anterioară, vă rog să detaliați pe scurt incidentul
12. Considerați că oamenii în general sunt destul de conștienți cu privire la drepturile lor legate de confidențialitate în interacțiunile cu instituțiile publice?
13. Considerați că sunteți informat referitor la securitatea datelor dumneavoastră personale?
14. Selectați ce metode utilizați în mediul online pentru a vă păstra datele personale în siguranță
15. Să presupunem prin absurd că datele dumneavoastră au fost compromise pe un site al unei instituții publice. Ce măsuri considerați că trebuie să luați pentru a rezolva problema?
16. Considerați că ar trebui să existe pedepse mai aspre pentru instituțiile publice care nu respectă confidențialitatea informațiilor personale ale cetățenilor?
17. Având în vedere răspunsurile dumneavoastră de până acum, în relația cu instituțiile publice preferați să completați documente online sau să rămâneți la metoda tradițională, cunoscută sub denumirea populară de ,,dosar cu șină”?
18. Motivați alegerea făcută
19. Considerați că este necesară aprofundarea informațiilor referitoare la protecția datelor personale?
20. Citiți termenii și condițiile în momentul în care semnați un document electronic/ vă abonați la un newsletter plasați o comandă on-line?
21. Ați fost până acum victima unui atac cibernetic de orice fel?
22. Dacă ați răspuns ***DA*** la întrebarea anterioară, vă rog detaliați experiența
23. Propuneți metode de îmbunătățire a procesului de colectare a datelor cu caracter personal pentru instituțiile Administrației Publice

Anexa B. Model cerere

CERERE-TIP

Denumirea autorităţii sau instituţiei publice _____

Sediul/Adresa _____

Data _____

Stimate domnule/Stimată doamnă _____,

Prin prezenta formulez o cerere conform Legii nr. 544/2001 privind liberul acces la informaţiile de interes public. Doresc să primesc o copie de pe următoarele documente (petentul este rugat să enumere cât mai concret documentele sau informaţiile **solicitate)**: _____

_____

_____

_____

_____

Doresc ca informaţiile solicitate să îmi fie furnizate, în format electronic, la următoarea adresă de e-mail (opţional): _____ .

Sunt dispus să plătesc taxele aferente serviciilor de copiere a documentelor solicitate (dacă se solicită copii în format scris).

Vă mulţumesc pentru solicitudine,

_____

(semnătura petentului)

Numele şi prenumele petentului _____

Adresa _____

Profesia (opţional) _____

Telefon (opţional) _____

Fax (opţional) _____

Anexa C. Model de declarație din timpul pandemiei de COVID-19, pe durata stării de urgență

DECLARAȚIE PE PROPRIE RĂSPUNDERE

Nume, prenume: _____ _____

Data nașterii: ____ ____ _____

Adresa locuinței: _____

_____

Se va completa adresa locuinței în care persoana locuiește în fapt, indiferent dacă este identică sau nu cu cea menționată în actul de identitate.

Locul/locurile deplasării:

_____

Se vor menționa locurile în care persoana se deplasează, în ordinea în care aceasta intenționează să-și desfășoare traseul.

Motivul deplasării:

- ◯ 1.interes profesional, inclusiv între locuință/gospodărie și locul/locurile de desfășurare a activității profesionale și înapoi
- ◯ 2.asigurarea de bunuri care acoperă necesitățile de bază ale persoanelor și animalelor de companie/domestice
- ◯ 3.asistență medicală care nu poate fi amânată și nici realizată de la distanță
- ◯ 4.motive justificate, precum îngrijirea/ însoțirea unui minor/copilului, asistența persoanelor vârstnice, bolnave sau cu dizabilități ori deces al unui membru de familie
- ◯ 5.activitate fizică individuală (cu excluderea oricăror activități sportive de echipă/ colective) sau pentru nevoile animalelor de companie/domestice, în apropierea locuinței
- ◯ 6.realizarea de activități agricole

- ◯ 7.donarea de sânge, la centrele de transfuzie sanguină
- ◯ 8.scopuri umanitare sau de voluntariat;
- ◯ 9.comercializarea de produse agroalimentare (în cazul producătorilor agricoli)
- ◯ 10. asigurarea de bunuri necesare desfășurării activității profesionale.

Se va bifa doar motivul/motivele deplasării dintre cele prevăzute în listă, nefiind permise deplasări realizate invocând alte motive decât cele prevăzute în Ordonanța Militară nr. 3/2020.

Data declarației ..... Semnătura .....

Persoanele care au împlinit vârsta de 65 de ani completează doar pentru motivele prevăzute în câmpurile 1-6, deplasarea fiind permisă zilnic doar în intervalul orar 11.00 – 13.00.

Anexa D. Model de contestație

CENTRUL DE EXAMEN _____

Nr. _____/_____

Domnule Președinte,

Subsemnatul/ Subsemnata, _____

absolvent(ă) al/a _____

_____,

solicit reevaluarea lucrării scrise pentru Evaluarea Națională, sesiunea iunie-iulie 2021, la disciplina _____, la care am obținut nota (în cifre și litere) _____.

Declar că am luat la cunoștință prevederile art. 11, alin (1) din OMEC nr. 5455/2020, *cu modificările și completările ulterioare*, conform cărora nota acordată ca urmare a soluționării contestației poate modifica nota inițială, prin creștere sau descreștere, după caz.

Data

Semnătura părinte/ reprezentant legal* Semnătura candidat

Domnului Președinte al Centrului de Examen_____

- În cazul candidatului minor, declarația este semnată și de către părinte/reprezentant legal al acestuia
- La depunerea on-line a cererii, se atașează fișierul cu scanarea CI a elevului, respectiv fișierul cu scanarea CI a părintelui/tutorelui legal, în cazul elevului minor

Anexa E. Model de împuternicire

S-a cerut autentificarea prezentului înscris: timbru sec

P R O C U R Ă

Subsemnatul_____, **în calitate de mandată, ÎMPUTERNICESC,** prin prezenta pe_____**, în calitate de mandatar, ca în numele si pentru mine să**_____.

În vederea executării prezentului mandat mandatarul meu va face orice fel de cereri şi declaraţii necesare, mă va reprezenta cu depline puteri în faţa autorităților/instituţiilor competente, precum și în fața oricăror persoane fizice sau juridice implicate în realizarea prezentului mandat (Primăria competentă, Direcţia de Impozite și Taxe Locale, Oficiul de Cadastru și Publicitate Imobiliară competent, Biroul de cadastru și publicitate imobiliară, biroul notarial, instituție bancară etc.), va solicita și ridica documentația_____, va solicita şi va ridica orice document necesar, va negocia toate clauzele, va achita taxele şi impozitele aferente și va întreprinde toate formalitățile necesare pentru îndeplinirea mandatului.

Pentru aducerea la îndeplinire a mandatului, mandatarul meu va semna în numele meu și pentru mine, oriunde va fi necesar, în limitele prezentului mandat, semnătura sa fiindu-mi pe deplin opozabilă.

Prezentul mandat este gratuit şi netransmibil, fiind valabil până la aducerea sa la îndeplinire sau până la încetarea acestuia prin revocare sau în celelalte cazuri prevăzute de lege.

Anexa F. Model de cerere pentru căsătorie către instituția religioasă a statului, Biserica

Înalt Preasfințite Mitropolit,

Subsemnatul, [redacted], absolvent al Facultății de Litere, Istorie și Teologie, din localitatea Timișoara, cu fiască supunere, vă rog să-mi acordați arhiereasca binecuvântare, pentru a putea să păşesc la Taina Sfintei Cununii, cu tânăra, [redacted], din parohia Coşava, Arhiepiscopia Timişoara.

În acest sens anexez următoarele acte:

- Adeverință de botez;
- Recomandarea preotului paroh;
- Fişa de studii;

Asigurându-vă de deplina dragoste şi supunere duhovnicească, vă rog să dispuneți.

Timişoara

15.05.2009

Înalt Preasfinției Sale,
Dr. Nicolae Corneanu,
Arhiepiscopul Timişoarei
şi Mitropolitul Banatului.

Referințe bibliografice

[1] C. Manda, „Digitalizarea administratiei publice din Romania–intre nevoile si aspiratiile unei societati moderne a secolului XXI,” *Smart Cities International Conference (SCIC) Proceedings,* pp. 41-48, 2021.

[2] O. L. Olga Cerbu, „POLITICA DE SECURITATE A TEHNOLOGIILOR INFORMAŢIONALE ÎN ADMINISTRAŢIA PUBLICĂ CENTRALĂ,” *Teoria şi practica administrării publice,* pp. 414-416, 2014.

[3] ANSPDCP, Legea 102 din 3 mai 2005 Publicată în Monitorul Oficial cu numărul 947 din data de 9 noiembrie 2018, Municipiul București: Monitorul Oficial, 2005.

[4] S. Ruxandra, Protecția datelor personale în era digitală. Trecut, prezent, viitor., București: https://www.academia.edu/about, 2021.

[5] S. D. Șchiopu, „CONSIDERAŢII ASUPRA INFORMĂRII PERSOANEI VIZATE CU PRIVIRE LA PERIOADA DE STOCARE A DATELOR CU CARACTER PERSONAL,” *Universul Juridic via ceeol.com,* nr. 04/2019, pp. 97-106, 2019.

[6] V. Pițigoi, „Ziua când s-au cautat în premieră amprentele la locul crimei,” https://ziare.com/, București, 2013.

[7] Ș. Dragoș și B. Ligia, Un Mijloc de Probă Revoluționar - Amprenta Genetică, București: Dreptul, 2001.

[8] A. Watson, „Biometrics: easy to steal, hard to regain identity,” Nature, Cambridge, Regatul Unit al Marii Britanii, 2007.

[9] M. C. Adrian, Furtul de identitate săvârșit prin intermediul internetului, Târgu-Mureș: http://revcurentjur.ro/old/.

[10] E. A. Maria și E. M. Alexandru, Calitate Terminologie Comentată, București: Editura Tehnică, 2000.

[11] C. Maria, Aspecte teoretice ale sistemului de management al documentelor. Strategii şi politici de management în economia contemporană, Chișnău: Catedra „Management”, ASEM, Chișinău, Republica Moldova, 2015.

[12] P. României, „https://legislatie.just.ro/,” Portalul N-Lex, 12 10 2001. [Interactiv]. Available: https://legislatie.just.ro/public/detaliidocument/31413. [Accesat 10 02 2024].

[13] M. C. Corneliu, Elemente de Ştiinţa Administraţiei, București: Editura Universul Juridic, 2012.

[14] C. Vrabie, Elemente de E-Guvernare [E-Government Fundamentals], București: Pro Universitaria, 2016.

[15] Ș. Dragoș, „Transparența în Activitatea Administrației Publice,” în *Transparența în Activitatea Administrației Publice*, Chișnău, Republica Moldova, Studii Juridice Universitare, 2009, pp. 211-216.

[16] E. Bădărău, „SECURITATEA NAŢIONALĂ ŞI DIMINUAREA RISCURILOR CIBERAMENINŢĂRILOR,” în *ECONOMIE ŞI SOCIOLOGIE*, Institutul de Relații Internaționale din Moldova, 2015, pp. 85-103.

[17] T. C. Ionel, „NECESITATEA ECONOMICĂ A STRUCTURĂRII INFORMAŢIILOR STATISTICE LA NIVEL MICROZONAL,” în *BULETIN ȘTIINȚIFIC*, Bacău, Universitatea „George Bacovia”, 2004, pp. 319-322.

[18] R. A. Elena, „Accesul la informaţiile de interes public–obligaţie legală în sarcina autorităţilor administraţiei publice. Studiu de caz privind gradul de accesibilitate al informațiilor de interes public comunicate din oficiu,” în *Accesul la informaţiile de interes public–obligaţie legală în sarcina autorităţilor administraţiei publice. Studiu de caz privind gradul de accesibilitate al informațiilor de interes public comunicate din oficiu*, Revista Transilvană de Ştiinţe Administrative, 2014, pp. 98-113.

[19] C. Europeană, „Ce sunt datele cu caracter personal?,” European Comission, [Interactiv]. Available: https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_ro#:~:text=Datele%20cu%20caracter%20personal%20sunt%20orice%20informa%C8%9Bii%20care,persoane%20constituie%20%C8%99i%20ele%20date%20cu%20caracter%20personal..

[20] C. Jugastru, „Tradiție și inovație în materia protecției datelor cu caracter personal,” *Universul Juridic,* vol. II, pp. 74-84, 2017.

[21] CEDO, „Convenția Europeană a Drepturilor Omului,” [Interactiv]. Available: https://www.echr.coe.int/documents/d/echr/Convention_RON.

[22] O. Beneș, „CEDO şi protecţia datelor cu caracter personal,” *Studii Juridice Universitare,* Vol. %1 din %2I-II, pp. 32-37, 2015.

[23] ANSPDCP, „Broșură de prezentare,” vol. Protecția datelor cu caracter personal, pp. 3-18, 2008.

[24] A. Murillo, A. Kramm, S. Schnorf și A. D. Luca, „“If I press delete, it’s gone” - User Understanding of Online Data,” *Proceedings of the Fourteenth Symposium on Usable Privacy and Security,* pp. 329-339, 2018.

[25] C. Jugastru, „PROCEDURI ŞI AUTORITĂŢI ÎN NOUL DREPT EUROPEAN AL PROTECŢIEI DATELOR CU CARACTER PERSONAL (I),” *Universul Juridic via ceeol.com,* nr. 06/2017, pp. 112-129, 2017.

[26] C. Timofte, „Ofițerul de conformitate – noul „gardian” al prelucrărilor de date cu caracter personal,” Data Privacy Blog, București, 2017.

[27] M. C. Mitrea, „Certificatul digital al UE privind COVID: garanții și riscuri în domeniul protecției datelor cu caracter personal,” *Universul Juridic via ceeol.com,* Vol. %1 din %2Starea excepțională și alerta ordinii de drept. Implicații juridice ale crizei sanitare generată de pandemia Covid-19, pp. 227-243, 2021.

[28] T. Dușcov, „PROTECȚIA DATELOR CU CARACTER PERSONAL AL CONSUMATORILOR ÎN RAPORTURILE CONTRACTUALE,” în *Reglementări naționale și standarde juridice internaționale în domeniul protecției drepturilor consumatorului*, Chișnău, Academia „Ștefan cel Mare” a MAI al Republicii Moldova,

2021, pp. 159-164.

[29] E. Comission, „Intersoft Consulting,” [Interactiv]. Available: https://gdpr-info.eu/art-5-gdpr/. [Accesat 03 2024].

[30] ICO, „LegalUp,” [Interactiv]. Available: https://legalup.ro/legalitatea-echitatea-si-transparenta/#:~:text=Articolul%205%20alineatul%20%281%29%20din%20RGPD%20statueaz%C4%83%20c%C4%83%3A,la%20legalitate%20%C8%99i%20la%20%E2%80%9Etemeiul%20juridic%20pentru%20prelucrare%E2%80%9D.. [Accesat 03 2024].

[31] M. Maxim, „Processing Personal Data by Cookies,” *Revista de Științe Politice via ceeol.com,* nr. 49, pp. 66-76, 2016.

[32] Google, „Șterge, permite și gestionează cookie-urile în Chrome,” [Interactiv]. Available: https://support.google.com/chrome/answer/95647?hl=ro&co=GENIE.Platform%3DDesktop. [Accesat 03 2024].

[33] M. Călin, „Ce este o adresă IP și de ce este important IP-ul,” calculatorescu.ro, 01 02 2024. [Interactiv]. Available: https://calculatorescu.ro/ce-este-o-adresa-ip/. [Accesat 26 03 2024].

[34] D. Chirică, „Bazele de date personale, obiect al convenţiilor oneroase încheiate de către operatorii de date,” *Universul Juridic,* nr. 1, 2021.

[35] Ș. Adriana-Maria și Ș. D. Mihail, „Protecția și securitatea datelor personale în educația digitală,” în *Educația digitală*, Editura Polirom, 2020, pp. 1-11.

[36] D.-M. Șandru, „Imposibila coexistenţă între protecţia datelor și comunitățile virtuale? Ce urmează?,” în *Pandectele române nr. 1/2018*, 2018, pp. 17-25.

[37] Statista.com, „Most used social media platforms in Romania in 2024,” 22 03 2024. [Interactiv]. Available: https://www.statista.com/statistics/1172720/romania-most-used-social-media-platforms/. [Accesat 26 03 2024].

[38] M. Mills, „Consolidarea securității contului dvs. online: sfaturi esențiale pe care ar trebui să le urmați,” ITIGIC, 02 10 2023. [Interactiv]. Available: https://itigic.com/ro/strengthening-your-online-account-security/?expand_article=1. [Accesat 03 2024].

[39] E. Comission, „Articolul 4 UE Regulamentul general privind protecția datelor, „Definiții”,” [Interactiv]. Available: https://www.privacy-regulation.eu/ro/4.htm. [Accesat 26 03 2024].

[40] M. M. Xavier de Carné de Carnavalet, „From Very Weak to Very Strong: Analyzing Password-Strength Meters,” *Concordia Institute for Information Systems Engineering,* pp. 1-19, 2014.

[41] D. Demeter, „Cum să-ți securizezi conturile online ca să fii sigur că nu vor fi sparte,” Playtech, 01 02 2019. [Interactiv]. Available: https://playtech.ro/2019/cum-securizezi-conturi-online/. [Accesat 03 2024].

[42] C. Neagu, „Întrebări simple: Ce este autentificarea cu doi factori sau verificarea în doi pași?,” Digitalcitizen.ro, 29 11 2018. [Interactiv]. Available: https://www.digitalcitizen.ro/intrebari-simple-este-verificarea-ori-autentificarea-doi-pasi/#:~:text=Verificarea%20%C3%AEn%20doi%20pa%C8%99i%20este%20un%20proces%20de,un%20serviciu%20%28e-mail%2C%20re%C8%9Bea%20social%C4%83%2C%20proces%20bancar%2C%20etc.%. [Accesat 03 2024].

[43] A. Dmitrenko, C. Liebchen, C. Rossow și A.-R. Sadeghi, „On the (In)Security of Mobile Two-Factor Authentication,” în *International Conference on Financial Cryptography and Data Security*, 2014.

[44] Google, „Când este posibil să-ți trimită Google un mesaj text,” Google Inc., [Interactiv]. Available: https://support.google.com/accounts/answer/3367674?hl=ro. [Accesat 03 2024].

[45] A. M. Dragomir, „AMENINȚĂRI DE TIP SOCIAL ENGINEERING, PRIN INTERMEDIUL REȚELELOR DE SOCIALIZARE,” în *Buletinul Universităţii Naţionale de Apărare Carol I*, București, 2018, pp. 63-67.

[46] P. D. Sia, „About privacy and phishing on social networks and the case of Facebook,” în *About privacy and phishing on social networks and the case of Facebook*, Poland, e-methodology via ceeol.com, 2018.

[47] G. României, „STRATEGIE din 30 decembrie 2021,” legislatie.just.ro, 03 01 2022. [Interactiv]. Available: https://legislatie.just.ro/Public/DetaliiDocument/250235. [Accesat 26 03 2024].

[48] E. Comission, „Securitatea cibernetică a rețelelor și a sistemelor informatice,” EUR-Lex, 2022. [Interactiv]. Available: https://eur-lex.europa.eu/RO/legal-content/summary/cybersecurity-of-network-and-information-systems-2022.html#:~:text=Directiva%2C%20cunoscut%C4%83%20sub%20numele%20de%20NIS%202%2C%20stabile%C8%99te,cooperarea%2C%20schimbul%20de%20informa%C8%9Bii%2C%20sup. [Accesat 26 03 2024].

[49] P. European, „Securitate cibernetică: principalele amenințări,” Agenția UE pentru securitate cibernetică (Enisa), 2022. [Interactiv]. Available: https://www.europarl.europa.eu/topics/ro/article/20220120STO21428/securitate-cibernetica-principalele-amenintari. [Accesat 03 2024].

[50] G. Costiță, „Un grup de hackeri ruși revendică atacurile cibernetice asupra site-urilor guvernamentale din România,” Europa Liberă, 29 04 2022. [Interactiv]. Available: https://romania.europalibera.org/a/atacuri-cibernetice-de-amploare-asupra-site-urilor-guvernamentale-din-rom%C3%A2nia/31826541.html. [Accesat 27 03 2024].

[51] E. Liberă, „Atac cibernetic asupra spitalelor din România oprit de DIICOT și SRI,” Europa Liberă, 15 05 2020. [Interactiv]. Available: https://romania.europalibera.org/a/atac-cibernetic-asupra-spitalelor-din-romania-oprit-de-diicot-si-sri/30614118.html. [Accesat 27 03 2024].

[52] G. Marina, „Haos în 18 spitale după un atac cibernetic de tip ransomware. MS: Sistemul e nefuncțional. Măsuri de prevenție pentru celelalte spitale,” Digi24, 12 02 2024. [Interactiv]. Available: https://www.digi24.ro/stiri/actualitate/un-atac-cibernetic-a-blocat-15-spitale-care-nu-mai-pot-inregistra-serviciile-medicale-camerele-de-garda-

sunt-pline-cu-pacienti-2683955. [Accesat 27 03 2024].

[53] P. Krapp, „Terror and play, or what was hacktivism?,” în *Grey Room*, 2005, pp. 70-93.

[54] I. Coman, „Descinderi DIICOT la grupări de hackeri. Aceștia ar fi atacat site-urile mai multor instituții publice,” Digi24, 29 06 2023. [Interactiv]. Available: https://www.digi24.ro/stiri/actualitate/descinderi-diicot-la-grupari-de-hackeri-acestia-ar-fi-atacat-site-urile-mai-multor-institutii-publice-2405053. [Accesat 27 03 2024].

[55] V. Tomco și K. J. Pashaj, „Enhancing investment through cyber security policies – Case of Albania,” *SCRD Journal,* vol. IV, nr. 1, pp. 95-102, 2020.

[56] FRISPA, „Conferinţa Ştiinţifică Națională ”Ştiinţa politică şi societatea în schimbare”, ediția a II-a,” YOUTUBE, 03 2023. [Interactiv]. Available: https://youtu.be/rfVEkSPVe30. [Accesat 01 05 2024].

[57] D. Online, „DEx Online,” DEx Online, 2024. [Interactiv]. Available: https://dexonline.ro/definitie/cerere.

[58] M. PĂUN, „Cererea,” *Academia de Studii Economice din București,* Vol. %1 din %2Suport de curs - cererea, pp. 1-6, 2023.

[59] D. online, „DEx online,” DEx online, 2024. [Interactiv]. Available: https://dexonline.ro/definitie/contesta%C8%9Bie.

[60] D. E. Român, „DEx Online,” DEx Online, 2024. [Interactiv]. Available: https://dexonline.ro/definitie/declara%C8%9Bie.

[61] I. F. Niculina Parosanu, „UNELE TEORII PRIVIND RESPONSABILITATEA ADMINISTRATIEI PUBLICE ÎN RELAŢIILE CU CETĂŢENII,” *REVISTA NAŢIONALĂ DE DREPT,* vol. XI, pp. 81-82, 2007.

[62] I. Condea, „Mass-media si democratia in Romania,” *Revista de Studii Media,* nr. 7, pp. 101-105, 2018.

[63] P. României, „LEGE nr. 52 din 21 ianuarie 2003 privind transparenta decizionala in administratia publica,” Monitorul Oficial, Bucuresti, 2003.

[64] A. Opre, „PROTECŢIA DATELOR CU CARACTER PERSONAL ÎN CADRUL PROCESULUI DECIZIONAL ADMINISTRATIV - ÎNTRE NECESITATEA ASIGURĂRII DREPTULUI LA VIAŢĂ PRIVATĂ ŞI NECESITATEA APLICĂRII MĂSURILOR PENTRU ÎNTĂRIREA SECURITĂŢII NAŢIONALE,” *Revista Univers Strategic,* nr. 18/2014, pp. 111-123, 2014.

[65] F. Păscăluță, „OBLIGAȚIILE DEPARTAMENTULUI RESURSE UMANE ÎN DOMENIUL PRELUCRĂRII DATELOR PERSONALE ALE SALARIAȚILOR,” *Conferința științifică națională cu participare internațională „Integrare prin cercetare și inovare”, USM, 10-11 noiembrie 2021,* pp. 280-282, 2021.

[66] Sedona, „Contractul colectiv de munca: ce este, lege si cand se incheie,” Codul Muncii actualizat, 2020. [Interactiv]. Available: https://www.aparaturafiscala.ro/blog/contractul-colectiv-de-munca-ce-este-si-cand-se-incheie/. [Accesat 2024].

[67] ANSPDCP, „Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal,” Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, 2024. [Interactiv]. Available: https://www.dataprotection.ro/.

[68] C. Deputaților, „CONSTITUȚIA ROMÂNIEI,” CAMERA DEPUTAȚILOR, 2024. [Interactiv]. Available: https://www.cdep.ro/pls/dic/site.page?id=339.

[69] C. Vrabie, Elemente de IT pentru administrația publică, Bucharest: Editura Pro Universitaria, 2024.

[70] H. Advisor, „Ce sunt credentialele?,” Hacker Advisor, 2024. [Interactiv]. Available: https://www.hackeradvisor.com/ce-sunt-credentialele/.