

Acesta este primul volum publicat al Academiei Naționale de Informații „Mihai Viteazul” (ANIMV) care integrează lucrările prezentate în cadrul Conferinței Științifice *Intelligence și Cultura de Securitate 2022* (ICS2022). Scopul ICS2022 este de a oferi studenților un spațiu pentru dezbateri academice și promovare a rezultatelor obținute în demersurile de cercetare proprii.

Prezenta ediție a fost dedicată atât doctoranzilor, cât și studenților din cadrul programelor de studii de licență și master, iar domeniile de interes științific propuse au fost: intelligence, securitate națională, istorie și relații internaționale.

Realizarea Conferinței a fost posibilă prin implicarea doctoranzilor și a conducătorilor de doctorat din Școala Doctorală Informații și Securitate Națională a ANIMV. Așteptăm cu entuziasm următoarea ediție a Conferinței!



ISSN 2971-8139
ISSN-L 2971-8139

◆
INTELLIGENCE ȘI CULTURA DE SECURITATE

◆
CONFERINȚA ȘTIINȚIFICĂ STUDENȚEASCĂ



INTELLIGENCE ȘI CULTURA DE SECURITATE

CONFERINȚA ȘTIINȚIFICĂ STUDENȚEASCĂ
VOLUM DE PROCEEDINGS

VOLUMUL 1
2022

Editura Academiei Naționale de Informații
„Mihai Viteazul”

PERCEPȚII CU PRIVIRE LA SECURITATEA DATELOR CONFIDENȚIALE ÎN CADRUL REȚELELOR SOCIALE

Elena-Iuliana BULGARIU*

Abstract:

Nowadays, in a networked society, the culture of security on social media platforms involves not only understanding confidentiality and controlling data, but also complying with these rules of confidentiality about what, why and to whom information is shared. Understanding privacy influences how confidential data is disclosed and defines user behavior on Facebook and Instagram. The paper focuses on what motivates users to provide access to confidential data and the effects of this decision. We will look at the generational differences and analyze the reasons for Z, Y, X and Boomers generations to post confidential data on social networks. The inductive thematic analysis, conducted on the basis of the semi-structured individual interview that we used as a method of data collection, will help to identify users' attitudes towards data security. The research identified that the attitude of users towards data security is influenced by the behavior, lifestyle of the age segment, but also by the benefits that come with the disclosure of confidential data. We were able to identify that users concerned about privacy and personal data are more reluctant and either do not provide personal data or provide it incompletely. The higher the level of privacy concerns, the less personal data users provide. In other words, the higher the level of security culture on social networks, the lower the degree of exposure to confidential data. This paper is relevant because it provides an x-ray of the behavior of Z, Y, X and Boomers generations, users of social networks, to identify the level of security culture on Facebook and Instagram platforms in relation to understanding privacy and the limits of the social contract.

Keywords: security culture, privacy, confidential data, social contract, social networks.

Introducere

Într-o societate în rețea, controlul datelor nu este suficient pentru crearea și protejarea confidențialității în cadrul rețelelor de socializare. De aceea, conceptul de confidențialitate, în cadrul rețelelor de socializare, ia forma unui contract social. Această confidențialitate este

* Elena-Iuliana BULGARIU-student masterand în cadrul Facultății de Istorie și Filosofie, Universitatea „Babeș-Bolyai” Cluj-Napoca.

privită ca un construct complex, care schimbă societatea și impune utilizatorilor un anumit mod de a o folosi. În momentul în care, oamenii percep contractul social ca fiind unul fiabil, utilizatorii au mai multă încredere în el și sunt mai predispuși să partajeze informații personale; acest aspect crește interacțiunea din online. Cu toate acestea, atunci când utilizatorii percep contractul social a fi mai puțin fiabil, din cauza colectării sau utilizării informațiilor personale, acest lucru le poate influența negativ atitudinea față de securitatea datelor, dar și comportamentul în cadrul rețelelor de socializare. Astfel, atunci când un utilizator de Facebook și/sau Instagram percepe contractul social ca fiind mai puțin de încredere, își poate adapta comportamentul pentru a-și proteja confidențialitatea și implicit datele personale. Înțelegerea confidențialității influențează modul în care se divulgă datele confidențiale și influențează atitudinea față de securitatea datelor. Cultura de securitate, în cadrul platformelor de socializare, nu presupune doar înțelegerea confidențialității și controlul datelor, ci și respectarea acestor norme de confidențialitate cu privire la ce, de ce și cui sunt împărtășite informațiile. Astfel, decizia de a oferi acces la aceste date confidențiale atrage după sine efecte ale acestei atitudini și oferă o înțelegere a nivelului culturii de securitate, în cadrul rețelelor de socializare.

Cercetarea se concentrează pe ce anume îi determină, pe utilizatori, să ofere acces la datele personale și pe efectele acestei decizii. Vom urmări diferențele generaționale și vom analiza, în baza contractului social, perspective importante asupra motivației comportamentului, în cadrul rețelelor sociale. Vom discuta despre ce anume i-a motivat, să împărtășească aceste informații și cum influențează această decizie atitudinea din online, a generațiilor Z, Y, X și Boomers. Analiza va contribui la explicarea motivelor intrinseci și extrinseci, pe care utilizatorii platformelor de socializare le vor menționa în interviul individual semistructurat. De asemenea, vom identifica, pe baza binomului confidențialității și socializării, care stă la baza contractului social, faptul că, respectarea confidențialității implică și înțelegerea normelor de confidențialitate cu privire la ce, de ce și cui sunt împărtășite informațiile în cadrul rețelelor de socializare. Totodată, lucrarea va contribui la literatura, limitată, cu privire la efectele atitudinii față de securitatea datelor, în cadrul Facebook și Instagram.

Această lucrare se va baza pe o analiză tematică, în care constatările celor 28 de interviuri semistructurate vor fi interpretate și vor ajuta, la înțelegerea atitudinii oamenilor față de securitatea datelor

personale, în cadrul rețelelor de socializare. Pentru ca rezultatul interpretării datelor calitative să fie mai precis, am realizat o analiză a opiniilor utilizatorilor de Facebook și Instagram, pe categorii de vârstă, după cum urmează: 17-24 ani, 25-40 ani, 41-59 ani. Fiecare interval corespunde unei anumite generații. Generația Z se referă la populația născută de la sfârșitul anilor '97 până în anii 2012, Generația Y, născută 1981-1996 și Generațiile X (1965 și 1979/80) și Boomers (1946 și 1964), pe care le-am luat ca pe un singur segment în această cercetare, deoarece se raportează la fel, cu privire la datele confidențiale. Am ales să realizez o astfel de analiză, pe segmente de vârstă, întrucât fiecărei generații i se poate atribui un set de valori, din care se poate desprinde o percepție general valabilă, pentru un segment de vârstă și un anumit caracter în mediul online. Această lucrare va utiliza o abordare calitativă, întrucât oferă un context general și amplu pentru a observa și a înțelege realitatea. În cadrul cercetărilor calitative se urmărește o credință comună, conform căreia, înțelegerea cadrului general pune la dispoziție observarea atitudinii societății, din România, față de datele cu caracter personal din cadrul rețelelor de socializare Facebook, respectiv Instagram.

Am identificat faptul că, utilizatorii de rețele sociale sunt conștienți de faptul că divulgă date cu caracter personal, însă în schimbul nevoii de a face parte dintr-o comunitate, de a comunica, cedează datele personale în baza contractului social. Utilizatorii de rețele sociale cedează datele lor personale pentru că au beneficii de pe urma acestora, susținând faptul că protecția confidențialității în baza acestui contract încurajează o creștere a partajării datelor confidențiale fără a se teme că le poate fi atinsă securitatea datelor în vreun fel. Totodată, utilizatorii preocupați de confidențialitate și de datele cu caracter personal sunt mai susceptibili și fie nu furnizează date cu caracter personal, fie le furnizează incomplete. Cu cât este mai mare nivelul de preocupare asupra confidențialității, cu atât utilizatorii furnizează mai puține date cu caracter personal. Mai mult decât atât, înțelegerea eronată a confidențialității poate fi o reprezentare a paradoxului confidențialității, întrucât este o contradicție între două variabile: preferințele de confidențialitate și activitățile de protecție a confidențialității.

Lucrare este relevantă pentru că analizează modul în care oamenii înțeleg și folosesc rețelele de socializare. De asemenea, pentru că oferă o radiografiere, pe generații, a atitudinilor utilizatorilor de rețele de socializare în raport cu confidențialitatea și limitele contractului social. Cu alte cuvinte, se desprind percepțiile cu privire la securitatea

datelor confidențiale în cadrul rețelelor de socializare și se identifică nivelul culturii de securitate în cadrul acestora din urmă.

Obiectiv

Această secțiune se concentrează pe ce anume îi determină pe utilizatori să ofere acces la datele personale și efectele acestei decizii. Mai exact, am urmărit și desprins ipoteze de cercetare ce ne ajută la a răspunde întrebării de cercetare; întrebare ce urmărește efectele preocupărilor privind securitatea datelor cu caracter personal asupra deciziei de a oferi acces la datele confidențiale. Vom urmări diferențele generaționale și vom analiza, în baza contractului social, perspective importante asupra motivației comportamentului în cadrul rețelelor sociale. Vom discuta despre ce anume i-a motivat să împărtășească aceste informații și cum influențează această decizie atitudinea din online a generațiilor Z, Y, X și Boomers. Analiza va contribui la explicarea motivelor intrinseci și extrinseci, pe care utilizatorii platformelor de socializare le vor menționa în interviul individual semistructurat. De asemenea, vom identifica, pe baza binomului confidențialității și socializării, care stă la baza contractului social, faptul că, respectarea confidențialității implică și înțelegerea normelor de confidențialitate cu privire la ce, de ce și cui sunt împărtășite informațiile în cadrul rețelelor de socializare. Lucrarea va contribui la literatura, limitată, cu privire la efectele atitudinii față de securitatea datelor, în cadrul Facebook și Instagram.

Pe baza narațiunii contractului social utilizatorii se bucură de libertatea de a face parte dintr-o comunitate, de a socializa (Elgesem D, 1996, p. 51), de a face schimb de informații, având și un interes în colectarea informațiilor, precum și în schimbul de informații în mediul online (Singleton S, 1998, p. 30-32). Astfel spus, scopul/scopurile comunității în care sunt partajate informațiile primează și dictează, în fața confidențialității informațiilor colectate sau dezvăluite în cadrul rețelelor de socializare. Totodată, se poate observa faptul că, preocupările legate de pierderea identității sunt cel mai frecvent asociate cu utilizarea rețelelor sociale pentru a distribui și a afla informații despre ceilalți (Kelly Quinn, 2016, p. 63). Acest lucru înseamnă că, utilizatorii de rețele sociale sunt conștienți de faptul că, divulgă date cu caracter personal, însă, în baza contractului social, membrii împărtășesc implicit și responsabilitatea de a păstra informațiile personale partajate (Hartzog W, 2011, p. 46). De aici se poate extrage prima ipoteză și anume: părțile

bune sau beneficiile pe care le văd utilizatorii în platforme (Facebook și Instagram) influențează decizia acestora de a oferi date personale.

Pe de altă parte, persoanele divulgă informații în cadrul unei rețele de socializare, fără a se teme că aceste comportamente îi face vulnerabili. O a doua ipoteză face referire la faptul că, unele persoane divulgă datele confidențiale în cadrul acestor rețele de socializare, fără să se teamă că această decizie are implicații asupra securității datelor. Cu alte cuvinte, indiferența/neglijența, cu privire la confidențialitatea datelor de care dau dovadă utilizatorii, ne indică faptul că, suntem siguri de modul în care oamenii percep contractul social.

O a treia ipoteză statuează următorul lucru: cu cât este mai mare nivelul de preocupare asupra confidențialității, cu atât utilizatorii furnizează mai puține date cu caracter personal. Utilizatorii preocupați de confidențialitate și de securitatea datelor cu caracter personal sunt mai reticenți și fie nu furnizează date cu caracter personal, fie le furnizează incomplete (Baruh Lemi, 2017, pp. 4). Această îngrijorare a indivizilor pentru confidențialitatea informațiilor din cadrul rețelelor sociale ne indică faptul că, există o relație între preocupările legate de confidențialitate și percepțiile asupra riscurilor, pe de o parte, și adaptarea comportamentului oamenilor, privind securitatea datelor în cadrul rețelelor de socializare, pe de altă parte (Baruh Lemi, 2017, pp. 4).

Metoda de cercetare

Acest capitol va prezenta selecția cazului, datele și metodele utilizate, pentru a înțelege ce efect are atitudinea față de securitatea datelor asupra deciziei oamenilor de a oferi acces la datele confidențiale pe Facebook și Instagram.

Selecția cazurilor

Această lucrare se concentrează pe România, care poate fi considerată un studiu de caz unic, întrucât studiile de caz unic sunt selectate pentru a înțelege lumea în funcție de un caz individual dintr-o anumită populație (Seawright J, 2008, pp. 295). Totodată, studiile de caz unic implică un număr limitat și reprezintă o caracteristică sau un comportament al unei populație (Seawright J, 2008, pp. 295). România poate fi considerată un studiu de caz tipic, deoarece, în ansamblu, utilizarea unui studiu de caz tipic oferă o perspectivă a unui fenomen extins și este reprezentativ pentru o varietate de cazuri. Acest caz ajută la înțelegerea fenomenului în ansamblul său și determină, totodată, un set de valori reprezentative (Seawright J, 2008, pp. 295). În cazul de față,

împărțirea persoanelor intervievate pe generații, în cadrul acestui studiu, va reflecta cum se raportează indivizii de diferite vârste la securitatea datelor, cu precădere a datelor personale, în cadrul rețelelor de socializare. Vom analiza această atitudine în cadrul rețelelor Facebook, respectiv Instagram. Cazul tipic mai este folosit și pentru a identifica ce efect are această atitudine asupra deciziei indivizilor de a oferi acces la datele confidențiale de pe Facebook și Instagram.

România este un caz reprezentativ pentru analiză, din mai multe motive. În primul rând, numărul utilizatorilor de Facebook din România a atins punctul culminant în martie 2021, la 12,57 milioane de utilizatori, iar până în martie 2021 existau peste 5,3 milioane de utilizatori Instagram în România. În al doilea rând, pentru că utilizatorii acestor rețele de socializare generează și consumă informații în cadrul acestor platforme. Întrucât indivizii sunt entități sociale, aceștia își dezvăluie diferite imagini ale sinelui, în cadrul rețelelor de socializare. Mai degrabă, indivizii se adaptează mai multor euri pentru a se potrivi unui anumit mediu social, unei societăți și valorilor interumane. În acest context, indivizii care trăiesc într-o societate, în care rețelele de socializare joacă un rol foarte important, utilizatorii pot manifesta diferite comportamente pentru a-și exprima multiple aspecte ale sinelui, dezvăluind date confidențiale în cadrul rețelelor de socializare. În al treilea rând, ilustrează modul în care, generațiile se raportează la informațiile/datele cu caracter personal, din cadrul rețelelor de socializare.

Metoda de colectare a datelor

Această lucrare va utiliza o abordare calitativă, întrucât oferă un context general și amplu pentru a observa și a înțelege realitatea (Silverman, D, 2019, pp.30). În cadrul cercetărilor calitative se urmărește o credință comună, conform căreia, înțelegerea cadrului general pune la dispoziție observarea atitudinii, societății din România, față de datele cu caracter personal din cadrul rețelelor de socializare Facebook, respectiv Instagram. Pe lângă acest aspect, abordarea calitativă permite testarea ipotezelor (Chigbu U.E, 2019, pp. 1-3), evidențiind totodată, flexibilitatea metodelor calitative.

O metodă calitativă, pe care am folosit-o, este cea a interviurilor individuale semistructurate, ca metodă de bază pentru colectarea datelor. Interviuul semistructurat are trei caracteristici majore: capacitatea de a adresa întrebări clarificatoare, menținerea unei relații armonioase cu persoana intervievată și totodată, stabilirea unei relații

transparentă și empatică cu receptorul (Noaks L., Wincup, E, 2004, pp. 80). Acestea din urmă ne-au ajutat ca dialogul să fie unul activ. Interviuurile semistructurate s-au bazat pe un ghid, care ne-au permis să modelăm interviurile, oferindu-i în același timp respondentului un confort și libertate de răspuns (Bryman, A, 2016, p. 38). Interviuurile individuale au asigurat confidențialitatea, anonimatul și s-au desfășurat atât în format fizic, cât și telefonic. Interviuurile au reprezentat o metodă prin care, cu ajutorul întrebărilor de follow up, conversația să fie una eficientă (Brinkmann, S, 2014, pp. 278-300) și să ofere o clarificare asupra unor aspecte ale răspunsurilor celor intervievați (Brinkmann, S, 2014, pp. 278-300). Conversațiile apropiate și active i-au permis, de asemenea, respondentului să genereze introspecții și confesiuni autentice, verosimile; lucru ce a oferit date valide pentru cercetare (Bryman, A, 2016, p. 64). Pentru a putea obține date utile, ne-am folosit de „ascultarea activă”, în care am oferit interviuatului spațiu și libertatea de a discuta și de alocă semnificații. Punctul de vedere oferit de respondent mi-a permis, totodată, să înțeleg atitudini și decizia oamenilor de a oferi acces la datele personale (Brinkmann, S, 2014, pp. 278-300). Datele au fost codate și puse pe categorii, astfel încât, să dea impresia unor relatări tematice, ce prezintă realitatea interviuatorilor (Silverman, D, p. 217-218). Pe scurt, interviurile individuale semistructurate oferă o înțelegere aprofundată a opiniei, așteptărilor și experienței individuale (Propp, V.I., 1968, p. 321).

Pentru colectarea datelor am desfășurat 28 de interviuri semistructurate, aplicând interviurile pe eșantioane diferite, care să cuprindă mai multe categorii de vârstă sau chiar nivele de pregătire. Eșantioanele reprezentative mi-au permis să realizez inferențe mai ample. De exemplu: scopul cercetării calitative, așa cum am menționat în rândurile de mai sus, este să studieze un segment relativ mic al unei populații și de a-i cunoaște atitudinile și comportamentul (Arber, S., 1993, p. 38).

Pentru acest interviu s-a realizat împărțirea persoanelor interviuate pe generații. Acest fapt va arăta cum se raportează indivizii, de diferite vârste, la securitatea datelor personale în cadrul rețelelor de socializare, în speță Facebook și Instagram. Interviuul cu respondenții s-a realizat prin eșantionare deliberată, utilizând metoda bulgărelui de zăpadă. Prin urmare, participanții au trebuit să se identifice, cu criteriile precum: utilizarea rețelelor de socializare și furnizarea de date cu caracter personal în cadrul acestora.

Acesta reprezintă punctele de vedere ale bărbaților și femeilor, cu o pondere de 50%, și respectiv 50%. Anexa 1 va surprinde numărul respondenților, vârstele acestora, genul, studiile, dar și mediul de proveniență. Fiecare dintre acești respondenți a fost chestionat, în legătură cu atitudinea sa față de datele lor personale, dar și cu privire la decizia lor de a oferi acces, la datele confidențiale pe Facebook și Instagram. În urma răspunsurilor primite, am putut surprinde mai multe teme, pe care le vom discuta în secțiunea următoare.

Metoda de analiză a datelor

Analiza din cadrul acestei lucrări se va baza pe o analiză tematică inductivă. În cadrul acesteia, se va realiza o analiză a datelor în funcție de punctele comune, a relațiilor și diferențelor dintre acestea (William Gibson, 2009, p. 127). Încă din terminologie, ne putem da seama de faptul că, analiza se va baza pe temele agregate datelor, astfel „tematic” face referire la scopul analizei (William Gibson, 2009, p. 127).

Există trei seturi generale de obiective în analiza tematică: examinarea punctelor comune, examinarea diferențelor și examinarea relațiilor. În cadrul primului obiectiv, se vor examina punctele comune, identificând datele care fac parte din aceeași categorie. În continuare, se vor examina diferențele – particularitățile datelor și contrastul dintre ele. În cele din urmă, examinarea relațiilor presupune analiza felului în care, diferite categorii de coduri se raportează unele la altele sau cât de specifice sunt caracteristicile individuale sau diferențele dintre date (William Gibson, p. 128-129). Analiza tematică presupune atât crearea de teme, cât și și codificarea datelor în raport cu aceste teme. Acest proces necesită înțelegerea datelor și totodată, abstractizarea ideilor mai largi (Andrew J. B, 2019, p. 3). Codarea datelor, din punct de vedere inductiv, implică o abordare de jos în sus, în care temele sunt identificate de la bază, din cadrul datelor (Gareth Terry, 2017, p. 22). Analiza tematică implică interpretarea codurilor și a temelor în cadrul datelor (Clarke V, 2017, pp. 297-298). În primul rând, datele sunt înțelese și transcrise de cercetător (Clarke V, 2017, pp. 297-298). În continuare, cercetătorul dezvoltă coduri în cadrul fiecărei transcrieri, care se referă la întrebarea de cercetare, acestea fiind apoi compilate, pentru a dezvălui temele subiacente. În cele din urmă, temele sunt abordate și explorate pe baza întrebării de cercetare. (a se vedea tabelul 1).

Tabelul 1: – Un exemplu ilustrativ de codare a temelor

Tema	Coduri / Subteme	Propozițiile care se potrivesc codurilor
Beneficiile rețelelor de socializare	interconectivitate, comunicare, informare, dezvoltare personala și profesională, credibilitate, necesitate, felicitări/urări, promovarea unui anumit produs, serviciu, gaming, job, partajarea de fotografii	„un mediu benefic pentru a-ți dezvolta cunoștințele, părerile și a-ți ține relațiile de prietenie pe termen lung.” „pot comunica cu persoanele dragi mie găsesc anunțuri pentru casă și grădină, rețete culinare” „au revoluționat și felul în care facem afaceri” „în zona de marketplace pentru ca cumpărătorul sau vânzătorul cu care vrei sa faci o afaceres -ar uita de multe ori pe contul tău dacă pari credibil.”
Indiferență cu privire la securitatea datelor		„Momentan, nu folosesc nicio metodă..nici nu mă pricep foarte bine la tehnologie...” „Nu...nu consider că sunt predispus riscului de a mi se folosi datele personale” „O parte din termeni i-am citit...o parte nu...i-am omis...nu m-au interesat” „Nu mă consider o persoana atât de importantă ca cineva chiar să-mi urmărească profilul sau să mă afecteze cu ceva faptul că mi-ar folosi datele personale. Chiar sincer nu

		m-am gândit la asta niciodată”
Conștientizarea riscului divulgării datelor confidențiale	fraudă, șantaj, cont fals, furt de date, hărțuirea online, urmărire, monetizarea datelor, livrarea de date explicit online sau scurgeri de informații, pierderea conturilor bancare, a unor coduri, a unor parole, denigrarea imaginii	„s-ar efectua plăți utilizând cardul bancar...ăăă..în cadrul unor jocuri cu care m-am conectat la Facebook” „monetizarea datelor pentru ca în ziua de astăzi hackerii strâng date pentru monetizarea loc în criptomonede sau chiar în bani reali.” „exista unele linkuri dubioase care nu necesită accesare sau unele poze care pot interfera cu adresa de email sau nr de telefon.”
Necunoscători cu privire la securitatea datelor personale	neinformați	„nu mă pricep foarte bine la tehnologie” „Alte riscuri nu cunosc deocamdată. Nu folosesc nimic deocamdată.(ref la metoda de protejare a datelor personale”
Precauții cu privire la datele personale	restricționarea datelor personale	„Consider că nu ar trebui să dezvălui viața mea personală care s-ar putea încadra într-un anumit CV.” „încerc sa nu fac publice locațiile unde sunt ...să nu dăm check-in, să nu dăm un anunț ca am plecat din țara” „sunt de părere ca nu ar trebui publicate datele personale” „Prin folosirea și expunerea datelor doar prin rețele

		sigure...Nu am accesat rețele Wi-Fi în zone publice...pentru că și prin această metodă pot fi transferate date destul de ușor.”
Neîncrederea în rețelele de socializare		„Rețelele de socializare au luat o pantă descendentă,deoarece dezinformarea este foarte des vehiculată, cât și furtul de date și anumite ilicite prin care anumite persoane cum ar fi hackerii...ar dori să obțină aceste date personale în scopul monitorizării lor.” „Cred că indiferent de cât de mult spunem despre noi, oricum aceste platforme fac o analiză a comportamentului nostru în mediul online în funcție de urmărirea pe care le avem.” ”Uneori găsesc puțin impropriu modul lor de gestionare a datelor.”
soluționarea incidentelor sau posibilelor incidente de securitate	acțiuni, raport către Facebook/Instagram, acționare în instanță sau ar apela la Poliție, depinde de impact	„Aș invita și alte persoane din lista mea de prieteni să raporteze persoana respectivă, întrucât cu cât există mai multe asemenea raportări, contul respectiv va fi șters de către Facebook sau Instagram.” „Cred că într-o prima fază aș încerca să-mi închid contul, iar în momentul în

		care aş alege sa-mi deschid un nou cont pe aceeași platforma de socializare, cu siguranță aş fi ai atentă la datele pe care le-aş furniza. Iar dacă s-ar ajunge sa fiu victimă unui accident de amploare, cu siguranța s-ar ajunge la autorități.”
--	--	--

Pe scurt, selectarea cazului, colectarea datelor și metoda de analiză a datelor prezintă cadrul metodologic al acestei lucrări. Totodată, datele colectate și analizate mai apoi sunt cele pe baza cărora, pot obține răspuns la întrebarea de cercetare a acestei lucrări.

Rezultate

Acest capitol se va baza pe o analiză tematică în care constatările celor 28 de persoane chestionate pe baza unui interviu semistructurat vor fi interpretate prin intermediul temelor și codurilor pe care le-am identificat în capitolul anterior (conform Tabelului 1: Un exemplu ilustrativ de codare a temelor). Pentru înțelegerea atitudinii oamenilor față de securitatea datelor personale în cadrul rețelelor de socializare, vom interpreta opiniile populației din România. Astfel, se poate observa un set de valori și credințe reprezentative pentru a identifica modul în care se raportează un anumit segment de populație la datele personale de pe platformele de socializare (17-59 de ani-conform anexei 1). Pentru ca rezultatul interpretării datelor calitative să fie mai precis, am realizat o analiză a opiniilor cetățenilor pe categorii de vârstă după cum urmează: 17-24 ani, 25-40 ani, 41-59 ani. Fiecare interval corespunde unei anumite generații. Astfel, vom urmări Generația Z care se referă la populația născută de la sfârșitul anilor '97 până în anii 2012, Generația Y, născută 1981-1996 și Generațiile X (1965 și 1979/80) și Boomers (1946 și 1964) pe care le-am luat ca pe un singur segment în această cercetare, întrucât se raportează la fel cu privire la datele confidențiale. Am ales să realizez o astfel de analiză pe segmente de vârstă, deoarece fiecărei generații i se poate atribui un set de valori din care se poate desprinde o percepție general valabilă pentru un segment de vârstă/generație. Credințele, valorile și particularitățile fiecărei generații le-am clasificat, identificându-se astfel temele amintite în

capitolul anterior al acestei cercetări. Temele cuprind aspecte precum: beneficiile rețelelor de socializare, precauții cu privire la datele personale, indiferență cu privire la datele personale, conștientizarea riscului, soluționarea incidentelor sau posibilelor incidente de securitate. Analiza acestor teme servește la înțelegerea atitudinii oamenilor față de securitatea datelor personale în cadrul rețelelor de socializare. Acest aspect ne va ajuta să identificăm ce efect are atitudine față de securitatea datelor asupra deciziei utilizatorilor de a oferi acces la datele confidențiale de pe Facebook și Instagram.

Beneficiile rețelelor de socializare

Această temă, surprinsă din interviurile individuale semistructurate, confirmă prima ipoteza conform căreia, părțile bune sau beneficiile, pe care le văd utilizatorii în platforme (Facebook și Instagram) influențează decizia acestora de a oferi date personale. În schimbul nevoii de a face parte dintr-o comunitate, nevoii de comunicare, informare, dezvoltare personală și profesională, credibilitate, promovarea unui anumit produs, serviciu, sau chiar pentru gaming, pentru găsirea unui job, sau pentru partajarea de fotografii, utilizatorii sunt dispuși să-și expună datele personale în baza contractului social. Relațiile și interacțiunile dezvoltate sub forma unui acord reciproc în cadrul unei comunități de pe Facebook sau Instagram, cu privire la partajarea și utilizarea informațiilor/datelor personale ia forma unui contract social. Acest contract social, din mediul online, poate fi definit ca un acord de confidențialitate, în care utilizatorii rețelelor de socializare divulgă datele personale, în schimbul acestor beneficii pe care Facebook și Instagram le oferă. Protecția confidențialității, în baza contractului social încurajează o creștere a partajării datelor personale, deoarece obiectivul acestuia din urmă nu urmărește scopurile comunității: socializare și confidențialitate totodată. Datorită acestui lucru, se poate identifica o dorință de auto-divulgare și o nevoie de a împărtăși informații în cadrul acestor rețele întâlnită la 18/28 de persoane intervievate, care susțin faptul că, atât Facebook-ul, cât și Instagram-ul le aduc beneficii, odată cu partajarea datelor confidențiale: „Ideea în sine este că aceste rețele nu mă obligă să dau datele personale, ci eu aleg să fac asta. Eu am niște reguli cărora, în momentul în care accept să fac parte din comunitate, mă conformez; accept.” (R13).

Segmentul de populație, cu vârste cuprinse între 17-24 ani, folosește aceste rețele preponderent pentru socializare, dar și pentru dezvoltare personală și profesională, pentru gaming sau pentru

partajarea de fotografii. Așa cum se poate deduce din: „...un aspect pozitiv ar fi facilitarea comunicării cu persoanele care se află la distanță cum ar fi: familia, colegii, până și profesorii....ăăă...Site-urile de socializare, cum ar fi Facebook, acum sunt folosite și pentru grupuri de facultate și se pot posta anumite documente, cursuri, sau chiar și tematici, bibliografia. Acestea rămân stocate, iar accesul este foarte facil (...) în cadrul unor jocuri cu care m-am conectat la Facebook” (R8).

Preocuparea legată de partea profesională a acestui segment de populație este subliniată de „Consider că este o ocazie bună de a interacționa cu prietenii, cu colegi sau cu oameni noi din diferite medii, specializări, cu diferite viziuni.” (R10). De asemenea „iei la cunoștință evenimente care se desfășoară în apropierea orizontului tău local...hmm...iei legătura și cu alte persoane din domeniul tău de interes.” (R7), „dar și un mod prin care-ți poți promova un anumit produs, serviciu...sau o metodă de a face bani” (R5). Un beneficiu care vine odată cu dezvoltarea datelor confidențiale este redibilitatea „în zona de marketplace pentru că, cumpărătorul sau vânzătorul cu care vrei să faci o afacere s-ar uita de multe ori pe contul tău dacă pari credibil. Mai mult pentru credibilitate ar ajuta dezvoltarea anumitor informații personale (...) să vad cu cine fac afaceri; să văd dacă e o persoană cu care aș vrea să interacționez în business” (R26).

Segmentul de populație 25-40, la fel ca segmentul 17-24, recunoaște faptul că, partajează datele personale pentru a socializa, pentru a se dezvolta din punct de vedere profesional, dar și pentru unele beneficii oferite de Marketplace a Facebook-ului. După cum se poate observa: „Ele nu doar că ne ajută să fim în contact cu prietenii sau...cu cunoștințele...dar au revoluționat și felul în care facem afaceri...sau felul în care ne găsim un job.” (R25). Ceea ce diferențiază aceste două generații este faptul că, cea cuprinsă între 25-40 este mai interesată de evoluția situației mediului înconjurător, de aceea în schimbul divulgării datelor personale, aceștia preferă să li se facă un profil în cadrul rețelelor de socializare și să primească diferite articole, din domeniul în care lucrează: „în ceea ce privește partea profesională, încerc să caut anumite articole cu privire la profesia mea și să mă informez.” (R19), preferă să primească știri/informări locale, sau chiar doresc să primească articole pentru ceea ce înseamnă administrarea și îngrijirea locuinței, întrucât majoritatea respondenților au întemeiate familii. Aceștia mărturisesc faptul că: „văd știri, văd vremea și sunt...fac parte din diferite grupuri pentru activități de grădiniță” sau faptul că „mă ajută și la marketplace să-mi găsesc unelte de folos” (R2). Generația Y poate fi caracterizată de o

dorință de a avea stabilitate, lucru ce-i determină pe utilizatorii Facebook și Instagram din acest segment, să se realizeze în carieră, să-și construiască o casă, o familie. Lucrurile acestea îi schimbă interesele și prioritățile acestei generații, lucru ce se poate observa din motivele pentru care, aceștia folosesc rețelele de socializare și divulgă datele confidențiale în cadrul acestora.

Segmentul 41-59, la fel ca segmentul anterior, 25-40, susțin că, beneficiile distribuirii datelor confidențiale sunt pentru a primi știri sau pentru alte articole, ce țin de partea administrativă a locuinței: „găsesc anunțuri de casă și grădină sau rețete culinare” (R3). Acest segment de populație, la fel ca celelalte două menționate anterior, recunosc faptul că, un beneficiu ce survine odată cu dezvăluirea datelor este cel al conectării cu ceilalți, de a relaționa: „e o metodă de a face oamenii să socializeze” (R15). Un aspect ce nu-l întâlnim la celelalte generații, segmentul 41-59 susține că, dezvăluirea datelor personale i-a ajutat să-și regăsească unii prieteni și colegi din liceu „ca să mă întâlnesc cu foștii colegi” (R20).

Această temă a surprins, pe segmente de vârstă, percepția oamenilor, în legătură cu beneficiile postării datelor confidențiale în cadrul Facebook și Instagram. Ceea ce am putut surprinde este faptul că, beneficiile pe care le aduc Facebook și Instagram, în urma dezvăluirii datelor personale, primează și dictează în fața confidențialității informațiilor.

Indiferență cu privire la securitatea datelor din cadrul Facebook și Instagram

Narațiunea contractului social are în vedere binomul confidențialității și socializării, susține faptul că, protecția confidențialității contractului social încurajează o creștere a partajării datelor personale, însă, unii oameni sunt indiferenți cu privire la riscurile ce pot apărea și iau în calcul, doar beneficiile amintite în cadrul primei teme (Nicole B. Ellison, Danah M. Boyd, 2013, pp. 151-172). Tocmai, pentru că protecția confidențialității contractului social încurajează o creștere a partajării datelor personale, există o înțelegere eronată, cu privire la confidențialitatea în cadrul acestor rețele de socializare. Unele persoane divulgă datele confidențiale în cadrul acestor rețele de socializare, fără să se teamă că această decizie are implicații asupra securității datelor. Această supoziție va fi tratată în această temă, pe segmente de vârstă. Modul în care, indiferența față de securitatea datelor, poate influența decizia oamenilor de a oferi acces la datele confidențiale este o ipoteză ce se poate deduce din mărturiile respondenților.

Astfel, am putut deduce faptul că, segmentul de vârstă 25-40, dar și segmentul 41-59 sunt cele mai indiferente, cu privire la securitatea datelor în cadrul Facebook și Instagram, iar 7/15 persoane din aceste generații susțin că, pe lângă faptul că nu folosesc nicio metodă, prin care să-și securizeze datele confidențiale „Momentan nu folosesc nicio metodă” (R1) sau „Nu folosesc nimic deocamdată. Nu folosesc o metodă de protecție anume ” (R21), aceștia nu citează nici politica de utilizare a datelor a Facebook și Instagram: „Cine citește atâtea pagini și cu scris mărunt!” (R15). Acest lucru arată faptul că, aceste segmente de populație au o înțelegere eronată asupra confidențialității, divulgând date personale precum: „numele, locația, număr de telefon, email” (R18) sau „nume, prenume, studii, locul de munca, ăăăă...și locația, orașul, data nașterii...” (R22).

De asemenea, întrebarea 5: „Cum caracterizați nivelul dumneavoastră de securitate pe aceste platforme de socializare având în vedere datele personale expuse pe profilul de Facebook/Instagram?”, din cadrul interviului, am putut evalua nivelul de securitate al datelor, al persoanelor din cadrul acestui studiu. Rezultatele pot confirma permissa pe care am enunțat-o anterior, conform căreia, segmentele de vârstă 25-40 și 41-59 au un nivel mediu de securitate a datelor confidențiale. Pentru segmentul 25-41, 8/10 persoane menționează faptul că, au un nivel mediu spre scăzut, ceea ce înseamnă că, metodele folosite pentru protejarea datelor confidențiale nu sunt direct proporționale cu volumul datelor dezvăluite. Mai exact, riscurile la care se expun odată cu dezvăluirea unor astfel de date sunt mari, ceea ce înseamnă că, nivelul de securitate, așa cum l-au caracterizat respondenții, este mediu spre scăzut. „Cred că este vulnerabil...că-mi poate fura datele. Mă expun la riscuri...” (R1). Segmentul 41-59 afirmă faptul că, 4/6 persoane au un nivel mediu al securității datelor, iar 2/6 unul scăzut. De aici se poate deduce, așa cum a surprins și un respondent, faptul că, „Nivel foarte scăzut fiindcă nu am niciun control asupra datelor.” (R6). Ce am putut deduce, pe baza acestor răspunsuri, ale interviurilor individuale semistructurate este faptul că: cu cât indiferența este mai mare, cu atât nivelul de securitate al datelor este mai scăzut; ipoteza a putut fi dedusă pe baza răspunsurilor segmentului de populație 25-40, 41-59, utilizatori de Facebook și Instagram, ceea ce înseamnă că, acest aspect îi caracterizează întru totul. „Ăăă...Daaa...Nu mă consider o persoană atât de importantă ca cineva chiar să-mi urmărească profilul sau să mă afecteze cu ceva faptul că mi-ar folosi datele personale. Chiar, sincer, nu m-am gândit la asta niciodată. ...Mediu, cred eu.” (R22). Acest lucru

implică o expunere mai mare la riscurile și incidente de securitate, ce pot avea un impact mare asupra datelor confidențiale. Indiferența cu privire la securitatea datelor, pe care am putut-o desprinde pe baza interviurilor individuale semistructurate, este o atitudine general valabilă, reprezentativă pentru segmentele de populație 25-40, respectiv 41-59.

Conștientizarea riscului divulgării datelor confidențiale

Dacă segmentele de vârstă cuprinse între 23-40, respectiv 41-59 se identifică a fi mai indiferente, din cadrul acestui studiu cu privire la securitatea datelor confidențiale, segmentul de vârstă 17-22 este cel care, are un nivel de securitate a datelor ridicat și cel care, conștientizează cel mai bine riscurile divulgării datelor confidențiale. Totodată, se poate testa ipoteza conform căreia, cu cât este mai mare nivelul de preocupare asupra confidențialității, cu atât utilizatorii furnizează mai puține date cu caracter personal. Astfel, în baza răspunsurilor întrebării 5: „Cum caracterizați nivelul dvs. de securitate pe aceste platforme de socializare având în vedere datele personale expuse pe profilul de Facebook/Instagram?”, se poate observa faptul că, pentru segmentul 17-22, majoritatea celor intervievați au un nivel ridicat de securitate al datelor confidențiale. Majoritatea populației intervievate, care se încadrează în segmentul 17-22 menționează faptul că, nedeazăvălulirea datelor confidențiale în cadrul acestor platforme de socializare este cel mai important lucru, pentru a împiedica materializarea unui risc în incident de securitate. Nivelul de securitate al datelor pentru acest segment de vârstă este evaluat prin raportarea la volumul datele confidențiale, pe care îl alege să le ofere în cadrul rețelelor de socializare. „În decursul timpului nu am postat foarte multe lucruri personale. Am încercat să evit vârsta, data nașterii...informații cu...date cu caracter personal, informații bancare.” (R25). Majoritatea respondenților spun: „Susțin, și mai ales în grupurile de prieteni, familiale, susțin ideea conform căreia nedeazăvălulirea datelor este un beneficiu. Consider că o dată de naștere pe care tu o postezi pe social media sau o anumită locație în care te aflii poate să devină un dezavantaj în momentul în care o persoana poate să te urmărească și să încerce să-ți producă anumite daune.” (R9). De asemenea, segmentul de vârstă 17-24 menționează: „consider că nivelul de securitate este unul destul de ridicat, fiindcă totul este restricționat în așa fel încât să fie văzut doar de lista mea de prieteni” (R7).

Cu toate că generația aceasta consideră că, nivelul securității datelor personale din cadrul rețelelor de socializare, a putut identifica

riscuri, precum: monetizarea datelor, livrarea de date explicit online sau scurgeri de informații, pierderea conturilor bancare, a unor coduri. De exemplu: „s-ar efectua plăți utilizând cardul bancar...ăăă..în cadrul unor jocuri cu care m-am conectat la Facebook” (R8); „Riscuri în ceea ce privește..cum spuneam mai devreme...monetizarea datelor pt că în ziua de astăzi hackerii strâng date pt monetizarea lor în criptomonede sau chiar în bani reali. Cele mai multe date pot să spun că sunt cele provenind din mediul sănătății. Ele sunt cele mai bine căutate și cele mai bine plătite. După aceea vin datele personale cum ar fi : adresa, numărul de telefon, adresa de email.” (R9).

Necunoscători cu privire la securitatea datelor

Segmentele de vârstă cuprinse între 23-41 și 41-59 rămân cele pe care le putem caracteriza a fi necunoscătoare, în materie de rețele de socializare. Generația Y (23-41) și Generațiile X și Boomers (segmentul de vârstă 41-59) sunt necunoscătoare și neglijente în același timp, cu privire la securitatea datelor personale, întrucât aceste generații, când vine vorba de tehnologie, atât Baby Boomers, cât și Generațiile X și Y au cunoscut o educație diferită, au socializat diferit și și-au întreprins activitățile profesionale, în mare parte, fără mijlocirea tehnologiei în comparație cu Generația Z. Generațiile Boomers și X, de exemplu, utilizează tehnologia, pentru a-i ajuta să consume informațiile din cadrul rețelelor de socializare. „Să văd grupurile mele de prieteni, grupurile în care sunt înscris pe Facebook ...și cam atât.” (R16). Unii sunt de părere: „Personal, nu văd să aducă un plus consistent în relațiile dintre oameni. E ceva superficial.” (R20). Tehnologia, pentru Millennials (Generația Y) este utilizată mai mult sau mai puțin pentru conexiuni, interacțiuni și uneori socializare. Generațiile Boomers și X au adoptat cu succes noile tehnologii, dar nu sunt la fel de confortabile cu tehnologia, în comparație cu celelalte generații. În condițiile acestea, s-a putut observa din analiza temelor anterioare, faptul că, nivelul de indiferență/neglijență este cel care influențează decizia oamenilor de a-și securiza datele personale, din cadrul Facebook și Instagram. Pe lângă acestea, putem spune că, și nivelul studiilor influențează decizia oamenilor de a oferi acces la datele confidențiale. Un alt aspect este cel care evidențiază faptul că, nivelul studiilor este direct proporțional cu nivelul de securitate al datelor confidențiale, din cadrul Facebook. Astfel, cei cu studii medii, au mărturisit, că „Nu prea cunosc...” (R2) sau „Nu folosesc nimic deocamdată. Nu folosesc o metodă de protecție anume ” (R21), iar majoritatea nu știu să utilizeze foarte bine tehnologia. „nu mă pricep

foarte bine la tehnologie” (R2), „Mă conectez prin email, dar nu...nu l-am creat eu.” (R18). Așa cum a surprins și tema „Indiferență cu privire la securitatea datelor”, segmentul de vârstă 23-40, dar și segmentul 41-59 sunt cele mai indiferente cu privire la securitatea datelor, în cadrul Facebook și Instagram, pentru că 7/18 persoane din aceste generații susțin că, pe lângă faptul că majoritatea au probleme cu utilizarea tehnologiei, așa cum se poate observa din mărturiile respondenților, aceștia din urmă nu folosesc nicio metodă, prin care să-și securizeze datele confidențiale

Precauții cu privire la datele personale

Se poate observa faptul că, cei preocupați de confidențialitate și de datele cu caracter personal sunt mai reticenți și fie nu furnizează date cu caracter personal, fie le furnizează incomplete, sau într-un număr redus. O altă ipoteză, care se afirmă este: cu cât este mai mare nivelul de preocupare asupra confidențialității, cu atât utilizatorii furnizează mai puține date cu caracter personal. Răspunsurile primite în cadrul interviurilor semistructurate vin să demonstreze și să întărească acest lucru. De asemenea, segmentul de populație, care a identificat cele mai multe riscuri este conștient asupra pericolului la care se poate expune, de aceea este precaut, își ia măsuri, și astfel, nivelul de securitate al datelor în cadrul rețelelor de socializare, se poate caracteriza ca fiind unul ridicat. Cei cu vârste cuprinse între 17-24 (Generația Z-nativi digitali) este cel mai precaut segment de populație din studiul nostru, întrucât „consider că nu ar trebui să dezvălui viața mea personală care s-ar putea încadra într-un anumit CV” (R8) sau pentru că „sunt de părere ca nu ar trebui publicate datele personale” (R9). De aceea, „Nu am accesat rețele wi-fi în zone publice...pt că și prin această metodă pot fi transferate date destul de ușor.” (R13) sau „încerc să nu fac publice locațiile unde sunt” (R28).

Neîncredere în rețelele de socializare

Pe lângă faptul că, odată cu divulgarea datelor confidențiale utilizatorii beneficiază de avantaje de pe urma acestei decizii, există și persoane care își declară, în acest interviu, neîncrederea în rețelele de socializare. Acestea consideră, că „uneori găsesc puțin impropriu modul lor de gestionare al datelor” (R25). Pe baza acestei supoziții s-a putut desprinde o nouă ipoteză de cercetare: nivelul neîncrederii în rețelele de socializare influențează decizia oamenilor de a oferi acces la datele confidențiale. De aceea, „Cred că indiferent de cât de puțin spunem

despre noi, oricum aceste platforme fac o analiză a comportamentului nostru în mediul online, în funcție de urmărirea pe care le avem.” (R14).

Cultura de securitate în cadrul rețelelor de socializare

Cetățeanul, ca membru al societății civile, este generator, utilizator și apărător al securității atât la nivel național, dar și la nivelul organizațiilor, în a căror activitate este implicat. Aceste organizații trebuie să își protejeze datele, angajații și resursele, într-un mediu în care, competiția poate recurge la metode disimulate, pentru a-și păstra avantajele sau a profita de vulnerabilități (2021). Consolidarea culturii de securitate permite cetățenilor să înțeleagă rolul acestora în societate, plecând de la premisa că, securitatea este un bun comun.

Această lucrare a intenționat să exploreze variabilele ce influențează decizia oamenilor de a oferi acces la datele confidențiale de pe Facebook și Instagram, dar și identificarea nivelului culturii de securitate în cadrul rețelelor de socializare, în raport cu gradul expunerii datelor confidențiale și a metodelor de securizare al acestora. Aceste variabile/teme au fost identificate pe baza celor 28 de interviuri individuale semistructurate și ulterior, analizate în acest capitol, după cum urmează: Beneficiile rețelelor de socializare, indiferență cu privire la securitatea datelor, conștientizarea riscului divulgării datelor confidențiale, necunoscători cu privire la securitatea datelor personale, precauții cu privire la datele personale și neîncrederea în rețelele de socializare. În urma analizei acestor variabile am putut confirma două dintre ipotezele pe care le-am enunțat în fază incipientă: părțile bune sau beneficiile pe care le văd utilizatorii, în platformele Facebook și Instagram, influențează decizia acestora de a oferi date personale, dar și cu cât este mai mare nivelul de preocupare asupra confidențialității, cu atât utilizatorii furnizează mai puține date cu caracter personal; mai exact, cu cât nivelul de conștientizare este mai mare, cu atât volumul datelor confidențiale va fi mai mic. De asemenea, alte două ipoteze pe care le-am putut desprinde, în urma interpretării datelor calitative: cu cât indiferența față de securitatea datelor este mai mare, cu atât volumul de date personale este mai mare, dar și ipoteza conform căreia, nivelul studiilor influențează decizia utilizatorilor de a oferi acces la datele confidențiale de pe Facebook și Instagram.

Percepțiile asupra securității datelor personale din cadrul rețelelor de socializare, care stau să confirme sau să infirme aceste ipoteze menționate anterior, pot totodată, să determine nivelul culturii de securitate. Cercetarea a identificat faptul că, atitudinea utilizatorilor

față de securitatea datelor este influențată de apartenență, comportamentul și stilul de viață al segmentului de vârstă 17-24 – Generația X, segmentului de vârstă 25-40 – Generația Y și segmentului de vârstă-generațiile X și Boomers. Pentru că atât Baby Boomers, cât și Generațiile X și Y au cunoscut o educație diferită, în comparație cu Generația Z, acestea din urmă au adoptat cu succes noile tehnologii, dar nu sunt la fel de confortabile cu tehnologia, în comparație cu celelalte generații. Când vorbim despre generația Z, Gen Tech, post-Millennials, iGeneration, tehnologia și rețelele de socializare fac parte din viața lor. Aceștia au mărturisit că, prin divulgarea datelor confidențiale, în cadrul Facebook și Instagram, pot beneficia de dezvoltare personală și profesională. Cu toate acestea, generația Z este cea care are un nivel de securitate al datelor ridicat și cel care conștientizează cel mai bine riscurile divulgării datelor confidențiale. 17-24 de ani este cel mai precaut segment de populație din studiul nostru, și majoritatea își iau măsuri pentru a-și proteja datele personale din cadrul Facebook și Instagram, îndemnând și alte persoane să facă același lucru. Generația Z menționează faptul că, nedeazăluirea datelor confidențiale, în cadrul acestor platforme de socializare, este cel mai important lucru pentru a împiedica materializarea unui incident de securitate. Generația Y poate fi caracterizată de o dorință de a avea stabilitate, aspect ce influențează interesele și prioritățile acestei generație. Tendința aceasta se poate desprinde din motivele pentru care aceștia folosesc rețelele de socializare și divulgă datele confidențiale în cadrul acestora. Segmentul 41-59, la fel ca segmentul anterior, 25-40, susțin că, beneficiile distribuirii datelor confidențiale sunt pentru a primi știri sau pentru alte articole ce țin de partea administrativă a locuinței. Dacă, pentru Generația Z, securitatea datelor este un deziderat în cadrul rețelelor de socializare, Generațiile Y, X și Boomers sunt mai indiferente și neglijente, cu privire la securitatea datelor în cadrul Facebook și Instagram. Majoritatea dintre aceștia mărturisesc faptul că, nu folosesc nicio metodă prin care să-și securizeze datele confidențiale și nici nu citesc politica de utilizare a datelor a Facebook și Instagram. În condițiile acestea, s-a putut observa, din analiza temelor anterioare, faptul că, nivelul de indiferență este cel care influențează atât decizia oamenilor de a oferi acces la datele personale, dar și securitatea datelor confidențiale din cadrul Facebook și Instagram. Tot din cauza indiferenței utilizatorii ajung să fie necunoscători, cu privire la securitatea datelor personale, întrucât influențează dorința de a ști ce metode să utilizezi pentru a proteja datele sau pentru a soluționa o amenințare sau un incident de securitate.

Se poate desprinde faptul că, protecția confidențialității, în baza contractului social, încurajează o creștere a partajării datelor personale, deoarece obiectivul acestuia din urmă urmărește scopurile comunității: socializare și confidențialitate totodată. Datorită acestui lucru, se poate identifica o dorință de auto-divulgare și o nevoie de a împărtăși informații, în cadrul acestor rețele, întâlnită la toate categoriile de vârstă. De asemenea, nevoile psihologice fundamentale modelează comportamentul, și crește interacțiunea din online. Altfel spus, conform teoriei autodeterminării, ce combină diferențele individuale cu motivația, se afirmă faptul că, satisfacerea nevoilor psihologice fundamentale modelează comportamentul, și crește interacțiunea din online. Teoria susține că, nevoile individuale ale unui individ se încadrează în trei categorii principale: competență (dorința de stăpânire), relaționare (dorința să aibă grijă de alții și să aibă o relație cu alții) (Richard M Ryan, Edward L Deci, 2000, p. 68-78). Prin cele spuse se demonstrează că, utilizarea rețelelor sociale crește sentimentele de conectivitate și satisface nevoile individuale de relaționare. Tocmai pentru că protecția confidențialității contractului social încurajează o creștere a partajării datelor personale, există o înțelegere eronată cu privire la confidențialitatea, în cadrul acestor rețele de socializare. Unele persoane divulgă datele confidențiale în cadrul acestor rețele de socializare, fără să se teamă că această decizie are implicații asupra securității datelor. Modul în care, indiferența față de securitatea datelor poate influența decizia oamenilor de a oferi acces la datele confidențiale, poartă numele de paradoxul confidențialității, în literatura de specialitate sau discrepanța, dintre pretenția oamenilor de a se preocupa de confidențialitatea lor și comportamentul lor real online, care nu reflectă aceste preocupări afirmă că, persoanele în cauză continuă să împărtășească informații personale și nu se angajează să-și protejeze confidențialitatea (Philip Fei Wu, 2018, pp. 212-215). Mai precis, este un paradox al modului în care, rețelele de socializare au posibilitatea de a-i face pe oameni să se simtă mai conectați unul cu celălalt, să-și divulge datele personale și sinele propriu, care pot crește stima de sine și sentimentele de fericire .

Concluzii

Cercetarea a identificat faptul că, atitudinea utilizatorilor față de securitatea datelor este influențată de comportamentul, stilul de viață al segmentului de vârstă, dar și de beneficiile venite odată cu dezvoltarea datelor confidențiale. Astfel, am putut identifica faptul că, indiferența cu

privire la securitatea datelor confidențiale influențează decizia de a oferi acces la acestea, în cadrul rețelelor de socializare. De asemenea, cei care conștientizează riscurile la care se supun odată cu divulgarea datelor personale, pe platformele de socializare, au un nivel de date mic expuse în cadrul acestora. Această atitudine îi determină pe unii dintre utilizatori, să ia anumite măsuri pentru protecția datelor în cadrul Facebook și Insagram. Mai mult decât atât, la unii dintre utilizatori se întâlnește o oarecare precauție, cu privire la decizia de a oferi acces la datele confidențiale.

Cu toate că internetul a devenit un element definitoriu caracteristic generației Z, care mai este recunoscută a fi generația Tech sau cea a nativilor digitali, aceasta din urmă are o atitudine activă. Tinerii sunt cei mai precauți în mediul online, conștientizând riscurile la adresa securității datelor confidențiale. Tot aceștia sunt cei care își iau cele mai multe măsuri de protecție, îndemnând și alte persoane să-și protejeze datele. Generația Z menționează faptul că, nedeazăvăluirea datelor confidențiale în cadrul acestor platforme de socializare este cel mai important lucru, pentru a împiedica materializarea unui risc în incident de securitate. Generația Y poate fi caracterizată de o dorință de a avea stabilitate, Segmentul 41-59, la fel ca segmentul anterior, 25-40, susține că, beneficiile distribuirii datelor confidențiale sunt pentru a primi știri sau pentru alte articole ce țin de stilul de viață și de preocupările acestora. Pentru că generațiile acestea nu au cunoscut încă de mici tehnologia, acest fapt îi determină să aibă o înclinație mai mare de a recupera perioada aceasta, observând o dependență față de social media, care contribuie activ, partajează, caută și consumă conținut pe platformele de socializare. Pe lângă faptul, că sunt activi în cadrul rețelelor, divulgă o cantitate foarte mare de date confidențiale, cum ar fi numărul de telefon, email, locația, studiile și conținut media. Această atitudine pe care o au față de securitatea datelor, se poate caracteriza a fi una de neglijență, întrucât majoritatea dintre aceștia mărturisesc faptul că, nu folosesc nicio metodă prin care să-și securizeze datele confidențiale și nici nu citesc politica de utilizare a datelor a Facebook și Instagram. În condițiile acestea, s-a putut observa din analiza temelor anterioare, faptul că, nivelul de indiferență este cel care influențează atât decizia oamenilor de a oferi acces la datele personale, dar și securitatea datelor confidențiale din cadrul Facebook și Instagram.

Pentru segmentul 17-22, majoritatea celor intervievați au un nivel ridicat de securitate al datelor confidențiale, întrucât menționează faptul că, nedeazăvăluirea datelor confidențiale în cadrul acestor platforme

de socializare este cel mai important lucru, pentru a împiedica materializarea unui incident de securitate. Nivelul de securitate al datelor, pentru acest segment de vârstă, este evaluat prin raportarea la volumul datele confidențiale, pe care îl alege să le ofere în cadrul rețelelor de socializare. Tot acest segment al populației este cel care conștientizează și identifică riscurile din cadrul rețelelor de socializare. Acest fapt este datorat înțelegerii de către aceștia a securității și a riscurilor, vulnerabilităților și amenințărilor din cadrul rețelelor de socializare. Cu toate că Generațiile Boomers și X au adoptat cu succes noile tehnologii, acestea nu se simt confortabile cu tehnologia, în comparație cu celelalte generații. În condițiile acestea, s-a putut observa, din analiza temelor anterioare, faptul că, nivelul de indiferență/neglijență este cel care influențează atât de mult decizia oamenilor de a-și securiza datele personale din cadrul Facebook și Instagram.

De aceea consider că, este util ca și celelalte generații să cunoască implicațiile unei atitudini neglijente cu privire la datele confidențiale, întrucât amenințările, riscurile și vulnerabilitățile pot avea impact la nivel individual, societal, național chiar.

Un nivel ridicat al culturii de securitate poate preveni materializare vulnerabilităților în amenințări și, totodată, prevenirea trecerii unui astfel de eveniment de la nivelul individului la nivel național.

Traietoriile cercetărilor viitoare, care pot fi făcute pe baza constatărilor din lucrarea aceasta, sunt cele legate de Generația Z, întrucât, doresc să urmăresc modul în care, aceste percepții cu privire la securitatea datelor confidențiale în cadrul rețelelor de socializare au un impact asupra mediului în care își desfășoară activitatea profesional.

Referințe bibliografice:

Cărți și articole

1. Andrew J. B. Fugard, Henry W. W. Potts, "Thematic Analysis", în: Paul Atkinson et al., *Sage Research Methods Foundations*, vol. 1, 2019, p. 3.
2. Arber, S., "The research process", în: N. Gilbert (ed.), *Researching Social Life, London, Sage*, 1993, pp. 38.
3. Baruh Lemi, Secinti Ekin, Cemalcilar Zeynep, "Online Privacy Concerns and Privacy Management: A Meta-Analytical Review", în: *Journal of Communication*, vol. 67, nr. 1, 2017, pp. 4.

4. Brinkmann, S., "Unstructured and Semi-Structured Interviewing", in Leavy, P. (ed.) *The Oxford Handbook of Qualitative Research*. Oxford: Oxford University Press, 2014, pp. 278-300.
5. Brinkmann, S., "Unstructured and Semi-Structured Interviewing", în: Leavy, P., Ed. *The Oxford Handbook of Qualitative Research*. Oxford: Oxford University Press, 2014, pp. 278-300.
6. Bryman, A., "Social Research Methods", în: Oxford: Oxford University Press., 2016, p. 64.
7. Bryman, A., *Social Research Methods*, Oxford, Ed. Oxford University Press, 2016, p. 38.
8. Chigbu U.E., "Visually Hypothesising in Scientific Paper Writing: Confirming and Refuting Qualitative Research Hypotheses Using Diagrams", în: *Publications*, vol. 7, nr.22, 2019, pp. 1-18.
9. Clarke, V. and Braun, V., "Thematic analysis", în: *The Journal of Positive Psychology*, vol. 12, nr.3, 2017, pp. 297-298.
10. David SILVERMAN, *Interpretarea datelor calitative*, CA Publishing, 2018, p. 51.
11. Elgesem D., "Privacy, respect for persons, and risk", în: C. Ess (Ed.), *Philosophical perspectives on* Fried C., "Privacy", în: *The Yale Law Journal*, 1968, pp. 476-493.
12. Gareth Terry, Nikki Hayfield, Victoria Clarke, Virginia Braun, "Thematic analysis" în: Carla, Sage Publications Ltd, London Willig, Wendy Stainton Rogers, *The SAGE Handbook of Qualitative Research in Psychology*, vol. 2, 2017, p. 22.
13. Hartzog W., "Chain-Link Confidentiality", în: *Georgia Law Review*, vol. 657, 2011, p. 46.
14. Kelly Quinn, "Why We Share: A Uses and Gratifications Approach to Privacy Regulation in Social Media Use", în: *Journal of Broadcasting, Electronic Media*, 2016, pp. 61-86.
15. Nicole B. Ellison, Danah M. Boyd, "Sociality through Social Network Sites", în: W. H. Dutton (Ed.), *The Oxford Handbook of Internet Studies*, 2013, pp. 151-172.
16. Noaks L., Wincup, E., *Criminological Research: Understanding Qualitative Methods*. London, Ed. Sage, 2004, pp. 80.
17. Philip Fei Wu, "The privacy paradox in the context of online social networking: A self-identity perspective", în: *Journal of the Association for Information Science and Technology*, vol. 70, nr. 6221, 2018, pp. 207-217.
18. Propp, V.I., "Morphology of the Folktale, second revised edition", ed. L.A. Wagner. Austin, TX: University of Texas Press, 1968, pp. 321.
19. Richard M Ryan, Edward L Deci, "Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development and Well-Being", în: *American Psychologist*, vol. 55, nr. 1, 2000, pp. 68-78.
20. Seawright J., Gerring, J., "Case Selection Techniques in Case Study Research,,", în: *Political Research Quarterly*, vol. 61, nr. 2, 2008, pp. 295.

21. Silverman, D., *Doing Qualitative Research*, London, Sage, 2010, pp.217-218.
22. Silverman, D., *Interpreting Qualitative Data*, London, Ed. Sage Publications, 2019, pp.30.
23. Singleton S., "Privacy as censorship: A skeptical view of proposals to regulate privacy in the private sector", în: Cato Institute, 1998, pp.30-32.
24. William Gibson, Andrew Brown, *Working with Qualitative Data*, London, Sage, 2009, p. 127.

Surse web

25. Revista de Intelligence, *Parteneriatul cu societatea civilă. Educația de securitate*, <https://intelligence.sri.ro/parteneriatul-cu-societatea-civila-educatia-de-securitate/>, accesat la data de 14.04.2022.

Anexa 1**Prezentare generală a participanților**

Interviewat	Gen	Vârstă	Nivel de pregătire	Mediul de proveniență
1	Feminin	26	Studii medii	Rural
2	Masculin	35	Studii medii	Rural
3	Feminin	45	Studii medii	Rural
4	Feminin	17	Studii medii	Rural
5	Masculin	19	Studii medii	Rural
6	Masculin	49	Studii medii	Rural
7	Feminin	21	Studii superioare	Urban
8	Feminin	21	Studii superioare	Rural
9	Feminin	21	Studii superioare	Rural
10	Masculin	22	Studii superioare	Urban
11	Feminin	21	Studii superioare	Urban
12	Feminin	23	Studii superioare	Rural
13	Masculin	21	Studii superioare	Urban
14	Feminin	35	Studii superioare	Urban

15	Masculin	46	Studii superioare	Urban
16	Masculin	43	Studii superioare	Rural
17	Feminin	31	Studii medii	Rural
18	Feminin	59	Studii medii	Rural
19	Masculin	24	Studii superioare	Urban
20	Masculin	50	Studii superioare	Urban
21	Masculin	33	Studii medii	Urban
22	Feminin	40	Studii superioare	Rural
23	Feminin	31	Studii medii	Urban
24	Feminin	31	Studii medii	Urban
25	Masculin	31	Studii superioare	Urban
26	Masculin	21	Studii superioare	Urban
27	Masculin	21	Studii superioare	Urban
28	Masculin	21	Studii superioare	Urban