BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Riscuri, amenințări și vulnerabilități legate de platformele social media și motoarele de căutare. Reglementări și cadre juridice naționale

Risks, threats, and vulnerabilities related to social media platforms and search engines. Regulations and national legal frameworks

Dr. Dănuț MAFTEI*
Masterand Lorin Nicolae BOGDAN-DUICĂ**
*Directoratul Național de Securitate Cibernetică, București, România
e-mail: dn.maftei@gmail.com
**Directoratul Național de Securitate Cibernetică, București, România
e-mail: bogdanduicalorin@yahoo.com

Abstract

Platformele de socializare online și motoarele de căutare sunt utilizate din ce în ce mai mult de persoane violente, infractori, infractori cibernetici și alți actori răuvoitori statali sau nonstatali, implicați în activități specifice amenințărilor hibride și interferenței străine, generând provocări pentru copii, fete, femei, cetățeni, societăți, economii, servicii critice, democrație și securitatea națională. Neglijarea proliferării online a activităților ilegale nu numai că erodează încrederea în aceste platforme, ci și pune în pericol securitatea și viața privată a utilizatorilor. Pentru a contracara eficient toate provocările, sunt necesare urgent noi măsuri legale. Reglementările ar trebui aplicate platformelor social media, motoarelor de căutare și serviciilor care permit utilizatorilor să posteze conținut online sau să interacționeze între ei.

Online social media platforms and search engines are used more and more by violent people, criminal offenders, cybercriminals, and other state or non-state malicious actors, who are involved in activities connected to hybrid threats and foreign interference, causing challenges for children, girls, women, citizens, societies, economies, critical services, democracy, and homeland security. Neglecting the proliferation of illegal activities not only erodes trust in online platforms but also places at risk the security and privacy of its users. To counter efficiently all the challenges, urgent new regulatory frameworks are needed. The regulations should be applied to social media platforms, search engines, and services that allow users to post content online or to interact with each other.

Cuvinte-cheie:
platforme social media; securitate națională; democrație; actori rău intenționați; interferențe străine; informații false; violență; fraude.

Keywords:
social media platforms; national security; democracy; malicious actors; foreign interference; false information; violence; frauds.

Info articol
Primit: 14 noiembrie 2024; Evaluat: 2 decembrie 2024; Acceptat: 6 decembrie 2024; Disponibil online: 17 ianuarie 2025
Citare: Maftei, D. și L.N. Bogdan-Duică. 2024. „Riscuri, amenințări și vulnerabilități legate de platformele social media și motoarele de căutare. Reglementări și cadre juridice naționale". *Buletinul Universității Naționale de Apărare „Carol I"*, 13(4): 197-214. https://doi.org/10.53477/2065-8281-24-48

Apariția social media a marcat o nouă eră, facilitând evoluția umanității. În prezent, există diverse platforme de social media (PSM), motoare de căutare și servicii care permit utilizatorilor să interacționeze rapid între ei sau să posteze conținut online. Acestea includ o varietate de pagini web, de aplicații și de alte servicii, inclusiv de social media, platforme de partajare video, site-uri de stocare și partajare în cloud a fișierelor de consum, forumuri online, servicii de mesagerie instantanee online și de întâlniri. Ele pot fi utilizate pentru a viziona videoclipuri, pentru a dobândi noi cunoștințe, pentru a împărtăși momente speciale ori pentru a relua legătura cu prietenii.

Pe de altă parte, aceste servicii populare online și platforme social media au și o latură negativă, deoarece pot fi un focar pentru înșelăciuni, fraude, violențe, propagandă și vehicularea de informații false. Platformele online și noile tehnologii au facilitat, au ieftinit și au accelerat mai mult ca oricând punerea în practică a activităților malițioase de către diverși actori statali și nonstatali, naționali și străini. În plus, anonimatul, lipsa controlului și a mecanismelor eficiente de verificare facilitează răspândirea conținutului dăunător și identificarea atacatorilor. În paralel, frecvența și complexitatea tacticilor, tehnicilor și procedurilor (TTP), utilizate de actorii rău intenționați pentru a exploata vulnerabilitățile platformelor și pe cele ale utilizatorilor, cresc neîncetat.

Platformele social media permit diseminarea rapidă și pe scară largă a informațiilor false și a altor forme de interferență străină care amenință principiile și valorile democratice. Se poate observa că acestea sunt utilizate inclusiv pentru a planifica și a afișa acte violente sau pentru a răspândi știri false și mesaje dăunătoare. Activitățile desfășurate prin folosirea PSM pot afecta democrația, pot polariza opiniile, pot incita la violență, pot submina încrederea în instituții, pot alimenta discriminarea și marginalizarea și pot eroda coeziunea socială, impactul asupra societății fiind profund și complex. De exemplu, în cazul persoanelor care nu folosesc social media în scopuri violente, acestea vor fi implicate și ele în violențe diverse, din cauza algoritmilor care sunt setați să promoveze acest tip de conținut și să încurajeze acte care conduc la violență în viața reală.

Fraudele realizate prin anunțurile false, postate pe rețelele sociale, au crescut, de asemenea, în mod dramatic. Chiar și anunțurile legale sunt clonate și utilizate în scopuri malițioase, iar utilizatorilor finali le este dificil să afle dacă anunțul este legal fără a-l accesa (Alexander 2024).
Numărul preluărilor de conturi de social media este în creștere, iar conținutul nu este neapărat verificat, motiv pentru care nimeni nu poate fi sigur că interacționează cu cineva cunoscut. Utilizatorii ar trebui să abordeze toate interacțiunile din social media cu o doză adecvată de scepticism, indiferent dacă este vorba despre un tweet, o postare sau un mesaj direct, fiind dificil să recunoască dacă o aplicație poate fi sau nu de încredere. De exemplu, întrucât **escrocheriile online** (Stathis 2024a) și **fraudele din Facebook Marketplace** sunt atât de răspândite (Alexander 2024), ar fi indicat ca utilizatorii să învețe cum să identifice un escroc (Stathis 2024b).

Actorii rău intenționați, în special cei statali, folosesc platformele social media ca mijloace de desfășurare a operațiunilor de război hibrid. Cercetătorii au remarcat în special evoluția doctrinei rusești privind războiul informațional, împreună cu „rădăcinile sale adânci în practica sovietică de lungă durată” (Giles 2016; Snegovaya 2015). Gândirea militară rusă recentă pune accent pe războiul hibrid, pe care îl consideră ca fiind o nouă realitate persistentă, cu „sfera informațională” și „războiul informațional” ca un spațiu de luptă critic.

Așa-numiții „trolli” și „roboți” par să joace un rol-cheie în răspândirea știrilor false și a dezinformării prin intermediul platformelor social media. Trollii profesioniști gestionează conturi pe rețelele sociale pentru a provoca sau pentru a răspândi dezinformări și știri false. Pe de altă parte, roboții sunt implicați în gestionarea unor conturi automate care combină conținutul generat de oameni cu postările computerizate. Pentru a-și atinge obiectivele, sunt create și utilizate rețele mari de conturi false, acestea jucând un rol central în promovarea știrilor false.

Metodele utilizate de companiile de social media pentru identificarea conturilor automate și a campaniilor coordonate de știri false, conduse de actori statali, sunt diferite, iar rezultatele sunt, de asemenea, diverse. Deși platformele au implementat unele măsuri de moderare a conținutului, acestea sunt, adesea, insuficiente și întârzie să răspundă cererilor de eliminare a conținutului dăunător. Situația prezentată este cauzată parțial atât de volumul mare de conținut, generat de utilizatori, cât și de lipsa de stimulente suficiente pentru a acționa rapid și eficient. De exemplu, în pofida resurselor imense și a abilităților tehnologice, *Meta for Business* a fost criticată pentru răspunsul său inadecvat la proliferarea paginilor de phishing pe Facebook. Algoritmii companiei și mecanismele de moderare a conținutului sunt, adesea, considerate deficitare în identificarea și eliminarea acestor pagini înșelătoare în timp util, răspunzând în mod repetat, la solicitarea utilizatorilor, cu mesaje stereotipe, precum *„conținutul nu contravine standardelor comunitare”* sau *„conținutul este sigur”*. Această situație expune milioane de utilizatori riscurilor asociate cu escrocheriile de tip phishing și ridică întrebări serioase cu privire la angajamentul Meta față de siguranța utilizatorilor (Qureshi 2023).

Efecte negative ale mesajelor malițioase, postate pe platformele de socializare

Cercetarea științifică a evidențiat că mesajele malițioase de diverse tipuri, postate pe platformele de socializare, au, în general, un impact negativ atât asupra utilizatorilor individuali, cât și asupra securității naționale, democrației și stabilității societale.
Actorii străini intenționează să creeze condițiile necesare pentru manipulare sau pentru alt gen de interferență prin erodarea încrederii publice, prin destabilizarea sistemelor politice, prin subminarea normelor democratice și slăbirea rezilienței statelor democratice. Pe termen lung, acest lucru poate deteriora capacitatea democrațiilor de a rezista amenințărilor externe sau de a menține o guvernanță eficientă.

Unul dintre cele mai dăunătoare efecte ale *Manipulării și Interferenței Informațiilor Străine* (FIMI)[1] este erodarea încrederii publice în instituțiile democratice. Dezinformarea, știrile false și discursul instigator la ură, care vizează inclusiv minoritățile etnice, religioase și sexuale, amplifică diviziunile sociale, conduc la creșterea discriminării și a violenței împotriva minorităților, alimentând polarizarea politică și culturală.
În paralel, este erodată încrederea în instituții și în mass-media tradițională, acest fapt conducând la creșterea scepticismului și la apariția unor dificultăți în a distinge între informațiile reale și cele false.

[1] Foreign Information Manipulation and Interference.

Prin exacerbarea diviziunilor existente în societate, campaniile FIMI amplifică polarizarea discursului politic, făcând mai dificil, pentru societățile democratice, angajarea lor în dezbateri constructive sau identificarea într-un numitor comun cu privire la problemele critice cu care se confruntă. Această polarizare slăbește capacitatea instituțiilor democratice de a funcționa eficient, procesul legislativ fiind transformat în blocaj partizan și în extremism politic.

Platformele social media, dezinformarea, discursul instigator la ură, știrile false și atacurile cibernetice, utilizate pentru a manipula opinia alegătorilor, dar și pentru a crește tensiunile sociale și nivelul actelor violente înainte, în timpul și după alegerile electorale pot influența rezultatul acestora. Astfel de activități pot avea consecințe profunde, deoarece pot conduce la alegerea unor candidați care sunt mai favorabili intereselor străine sau, dimpotrivă, pot afecta perspectivele candidaților considerați ostili acestor interese.
Femeile și adolescentele cad pradă diferitelor forme de violență sexuală online (hărțuire cibernetică, videoclipuri care prezintă violuri, amenințări și distribuirea de imagini sexuale fără consimțământ). Aceste forme de violență pot deveni reale și pot interfera cu capacitatea femeilor de a se simți în siguranță la locul de muncă sau în public.

Pe de altă parte, popularitatea și ușurința de a utiliza PSM au facilitat accesul extremiștilor la alte persoane cu viziuni similare, crearea de rețele teroriste, recrutarea de noi membri, răspândirea ideologiilor extremiste și incitarea la violență. Algoritmii PSM pot amplifica conținutul extremist, expunându-i pe utilizatori la mesaje periculoase care contribuie la radicalizarea lor.
Interferența străină prin dezinformare care vizează sănătatea (de exemplu, referitor la vaccinuri, pandemii etc.) are un impact negativ asupra sănătății publice, crescând riscul de îmbolnăvire și de deces prematur.
Totodată, dezinformarea și știrile false pot afecta negativ economiile naționale și internaționale prin manipularea piețelor financiare, prin generarea de prejudicii financiare, prin subminarea încrederii întreprinderilor și răspândirea panicii. Provocări deosebite sunt generate și de traficul de persoane în scopuri de muncă sau sexuale, victimele traficului fiind cel mai adesea copiii și chiar adolescenții și tinerii.

Tactici, tehnici și proceduri utilizate online de actorii rău intenționați pentru a desfășura activități frauduloase

Zi de zi pot fi observate TTP atât vechi, cât și noi, utilizate de escroci pentru a înșela oamenii. Cu tot mai multe fraude online realizate zilnic, fiecare nouă fraudă este și mai complexă, mai inteligentă și mai puțin detectabilă decât ultima (Stathis 2024a). În prezent, utilizatorii PSM sunt victimele mai multor tipuri de amenințări, acestea fiind prezentate succint în continuare.

Atacurile de tip phishing (Adrien 2023) sunt atacuri efectuate online. Scopul lor este de a fura date personale sau de a obține controlul asupra conturilor de social media. Phishingul este o formă de criminalitate informatică în care actorii rău intenționați pretind a fi entități demne de încredere, adesea pentru a atrage utilizatorii prin promoții false, concursuri frauduloase sau știri inventate, ori pentru a-i determina să acceseze linkuri rău intenționate sau să dezvăluie informații sensibile, cum ar fi date personale, credențiale de conectare, informații despre carduri de credit, date financiare etc. Activitățile de phishing reprezintă la momentul actual una dintre cele mai frecvente forme de inginerie socială, cu peste 3 miliarde de e-mailuri spam, trimise zilnic.

Potrivit statisticilor, milioane de conturi de afaceri Facebook din întreaga lume sunt vizate de mesaje de phishing, cu o rată de succes de aproape una din 70 de victime infectate (Petkauskas 2023). Escrocii impersonalizează diverse PSM în atacurile de phishing, acestea fiind menite să instaleze pe ascuns programe software malițioase (spyware sau ransomware) pe calculatoarele personale, să fure credențiale și, eventual, date personale (Rosenkrantz 2024).

Deși phishingul rămâne popular, în prezent putem observa noi tehnici, precum *spear-phishing, whaling, compromiterea e-mailurilor de afaceri, smishing, https phishing, phishing cu clone, pop-up phishing, angler phishing, evil twin phishing, search engine phishing, watering hole phishing, vishing* etc. (Chin 2024). În plus, infractorii cibernetici folosesc instrumente generative de inteligență artificială pentru a-și redacta mesajele electronice, ceea ce le îmbunătățește rata de succes în phishing.

Hackerii folosesc o rețea masivă de conturi false și compromise pentru a transmite milioane de mesaje de phishing în platforma Messenger, acestea vizând conturile de afaceri Facebook cu programe malware care fură parole (Toulas 2023b). Potrivit rapoartelor, specialiștii avertizează că aproximativ unul din șaptezeci de conturi vizate este, în cele din urmă, compromis, ceea ce se traduce prin pierderi financiare masive (Zaytsev 2023).

Aplicațiile frauduloase pot fi reprezentate de reclame pentru aplicații sau funcții pe PSM, care pretind că permit utilizatorilor să verifice cine le-a vizualizat profilul (Budgar 2024).

În cazul fraudelor de pe **Facebook Marketplace** (Alexander 2024), se poate observa că un număr foarte mare de utilizatori cumpără și vând bunuri în fiecare zi, dar și

că escrocii folosesc această platformă de cumpărături online pentru a înșela oamenii și a le fura banii. Escrocii le pot solicita utilizatorilor să plătească sau să discute detalii suplimentare, dar prin utilizarea unor terțe canale de comunicare, în timp ce alții ar putea lista închirieri false, cadouri sau diverse produse.

În cadrul **fraudelor bancare**, mulți escroci oferă cadouri false pentru a-i determina pe utilizatori să divulge diverse informații personale (card de credit, numere de asigurări sociale etc.) sau să acceseze linkuri prin care ar putea descărca viruși pe calculatorul personal (Bradford 2024).

În cazul **atacurilor de tip spoofing**, hackerii pot accesa ilegal contul unei persoane și pot trimite mesaje sau postări false prietenilor acesteia, solicitându-le bani sau cadouri (Alexander 2023). Mesajele au rolul de a-l emoționa ori panica pe utilizator și apoi de a-l determina să ofere bani, fără a analiza bine situația. În plus față de utilizarea profilului unui prieten pentru a efectua un atac de tip spoofing, escrocii ar putea să impersonalizeze persoane sau organizații cunoscute.

Sextortion este o înșelătorie de inginerie socială, în care o victimă (de obicei, de sex masculin) se împrietenește cu o escroacă de sex feminin. Victima este convinsă să furnizeze imagini sau clipuri video cu caracter sexual explicit persoanei false, care amenință apoi că va publica în direct materialul compromițător, dacă nu i se transferă o anumită sumă de bani (Schappert 2024).

Atacatorii pot folosi și **scheme de tip "Secret Santa"**, prin care oamenii trebuie să trimită unei persoane un cadou de 10 $, urmând să primească și ele unul de la alte trei persoane. Nu există însă nicio garanție că victima va primi banii înapoi în aceste fraude, realizate pe Facebook, deoarece, dacă nimeni nu dă curs trimiterii cadoului, ar putea să nu primească nimic în schimb. Actorii malițioși ar putea folosi adresa de domiciliu a victimei pentru a efectua atacuri de tip *doxxing*[2] (Alexander 2022), iar partajarea altor informații personale ar putea dezvălui răspunsurile la întrebările de securitate ale parolelor, conturile personale fiind astfel vulnerabile în fața hackerilor.

Informațiile eronate (*"misinformation"*[3]) sunt informații false, înșelătoare sau extrase din context, diseminate de o persoană *care crede că sunt adevărate*, fără intenția de a provoca prejudicii. *Misinformation* are puterea „dovezii sociale" în a convinge persoanele să dea credibilitate acestor informații false. Oamenii vor accepta mai rapid știrile ca fiind adevărate atunci când sunt difuzate de prieteni, cunoștințe și de surse presupus credibile, dar și dacă aceste știri sunt mai populare (Hindman 2018).

[2] Doxxing sau doxing reprezintă furnizarea în mod public de informații personale identificabile despre persoane sau organizații, de obicei online și fără consimțământul acestora, ca formă de pedeapsă sau răzbunare.
[3] Denumire preluată din limba engleză.

Dezinformarea se referă la informații false (sau narațiuni ori fapte manipulate, propagandă) despre care *propagatorul știe că sunt false*. Este o minciună deliberată, intenționată, menită să manipuleze, să provoace daune și să îndrume oamenii, organizațiile și statele într-o direcție greșită, să genereze neîncredere în instituțiile statului democratic pentru a provoca prejudicii ori pentru a obține câștiguri politice, personale sau financiare (PakVoices 2023).

Dezinformarea implică mai multe părți interesate, este coordonată și dificil de urmărit. Acțiunile specifice dezinformării pot include videoclipuri modificate, articole de știri false sau postări amplificate artificial pe rețelele de socializare. Acestea conțin, adesea, calomnii sau discursuri instigatoare la ură împotriva anumitor grupuri de persoane și sunt adesea polarizante, incitând la furie și alte emoții puternice, putând determina oamenii să promoveze idei extremiste, teorii ale conspirației, fără loc de compromisuri.
Noile tehnologii emergente sunt utilizate din ce în ce mai mult pentru a discredita informațiile factuale. Inteligența artificială (IA) și IA generativă pot fi utilizate pentru a răspândi informații false și înșelătoare, cum ar fi "*deepfake*".

"Mal-information"[4] se referă la *informații bazate pe realitate*, folosite pentru a afecta persoane, grupuri sociale, organizații sau națiuni (ITU 2021). *Mal-information* implică fapte, deci nu falsuri. Datele personale și scurgerile de e-mailuri, dezvăluite prin *doxxing*, sunt exemple de mal-information. Hărțuirea, discursul instigator la ură și pornografia din răzbunare fac parte, de asemenea, din această categorie.

[4] Denumire preluată din limba engleză.

Știrile false sunt *informații intenționat elaborate*, senzaționale, încărcate emoțional, înșelătoare sau total fabricate, care imită tiparul știrilor importante (Saint Francis University 2023). Acestea sunt legate de distribuirea online de informații false, deghizate în știri legitime. Motivațiile din spatele știrilor false pot fi personale (pentru a afecta reputația unei persoane sau a unei organizații), financiare (pentru a mări traficul pe internet și/sau veniturile din publicitate) ori politice (pentru a influența punctul de vedere/ideologia publicului).

***

Desigur, există o mulțime de alte variante ale provocărilor cu care se pot confrunta oamenii pe PSM, precum ar fi *atacuri malware, mesaje spam, conturi clonate, colectări de fonduri medicale false, escrocherii de tip „clickbait", fraude cu coduri de cupon false, cu chestionare Facebook, escrocherii romantice, cu locuri de muncă, strângeri de fonduri false, hărțuire cibernetică, "internet banging", abuz sexual asupra copiilor, control sau comportament coercitiv, violență sexuală extremă, pornografie extremă, vânzare de droguri sau de arme ilegale, exploatare sexuală, fraudă, infracțiuni de ordine publică, agravate din motive rasiale sau*

religioase, imigrație ilegală și trafic de persoane, promovarea sau facilitarea sinuciderii, abuz de imagini intime (pornografie din răzbunare), terorism etc.

Se impune ca factorii de decizie să înțeleagă cu claritate că toate aceste tipuri de TTP prezintă enorm de multe variante de acțiune care pot fi folosite cu succes de către diverși actori malițioși pentru desfășurarea complexă de atacuri online cu rezultate grave. În urma unor scanări detaliate a victimelor pentru identificarea vulnerabilităților lor specifice, atacurile vor fi, ulterior, organizate, adaptate și personalizate în funcție de specificul fiecărei ținte, combinat cu alte metode și tehnologii de vârf, astfel încât șansele de succes să fie maxime. Ca atare, în condițiile menționate, statele au nevoie să se adapteze rapid prin modificarea cadrului legal și să dezvolte strategii de lucru eficiente pentru contracararea unor astfel de provocări complexe.

Măsuri specifice, adoptate de autoritățile naționale, pentru combaterea activităților ilegale, desfășurate prin utilizarea platformelor social media

UE și diferite state de pe mapamond acordă, de ani de zile, atenție activităților rău intenționate desfășurate online și impactului pe care acestea îl au asupra securității naționale, democrației, instituțiilor statului, infrastructurii critice, societății, întreprinderilor și cetățenilor. Cercetarea științifică actuală a evidențiat și unele măsuri, luate de autoritățile naționale, împotriva provocărilor reprezentate de actorii rău intenționați prin utilizarea PSM, prezentate în continuare.

Platforma TikTok:

Începând cu anul 2020, **Platforma TikTok** a fost blocată/restricționată în state precum Afganistan, Armenia, Azerbaidjan, Bangladesh, India, Iran, SUA, motivele care au stat la baza acestor decizii fiind legate de securitatea națională, de nivelul ridicat al terorismului, de conflictele de la graniță etc. (Gordon 2024). În baza Regulamentului privind Serviciile Digitale[5], Comisia Europeană a inițiat proceduri împotriva TikTok privind lansarea *TikTok Lite* în Franța și în Spania (Comisia Europeană 2024).

În 2023, TikTok a fost interzisă pe dispozitivele deținute de instituțiile de stat în Austria, Belgia, Canada, Estonia, Franța, SUA, din cauza riscului pentru securitate și confidențialitate, precum și din cauza presupuselor legături existente între Partidul Comunist Chinez și companie, TikTok fiind acuzată de colectarea și partajarea de date personale cu serviciile de informații chineze (Lakshmanan 2024).

În mai 2023, în România, Directoratul Național de Securitate Cibernetică – DNSC (organism specializat al administrației publice centrale, aflat sub

[5] Regulamentul privind Serviciile Digitale impune platformelor digitale să își asume o mai mare responsabilitate pentru conținutul partajat pe platformele lor. Această legislație urmărește să limiteze răspândirea dezinformării dăunătoare, asigurând, în același timp, respectarea libertății de exprimare.

autoritatea Guvernului și responsabil cu asigurarea securității cibernetice a spațiului cibernetic civil național), a emis o recomandare instituțiilor statului și organismelor publice să nu descarce, să nu instaleze sau utilizeze TikTok pe rețelele și sistemele lor informatice (DNSC 2023b).
În Taiwan, TikTok fusese interzisă pe dispozitivele guvernamentale încă din decembrie 2022. Motivul deciziei a fost legat de preocupările privind utilizarea informațiilor de către China pentru desfășurarea unui „război cognitiv" împotriva Taiwanului.

Rapoartele tehnice despre TikTok menționează existența multor *riscuri și vulnerabilități de securitate cibernetică specifice instalării și utilizării acestei aplicații* (**colectarea de date personale, dispozitive utilizate, sistem de operare, IP, SSID Wi-Fi, număr de serie, ID SIM, IMEI, citirea SMS-urilor, adresă MAC, localizare GPS, conturi de utilizator, acces la clipboard, istoric, inutilitatea setării Do Not Track, servicii/aplicații utilizate, profilarea personală a utilizatorului, partajarea datelor colectate cu alți „parteneri", control la distanță etc**.) (Baiaș 2023).

Totodată, a fost luată în considerare și legislația chineză, aceasta obligând cetățenii și entitățile să coopereze cu serviciile de informații și cu instituțiile de stat pentru furnizarea de date și informații în scopuri „naționale" (***Legea Securității Statului*, 2015; *Legea Securității Cibernetice*, 2016; *Legea Activităților de Informații de Stat*, 2017; *Legea Activităților de Contrainformații de Stat*, 2023**).

***Platforma Facebook**:*
Încă din 2015, platforma Facebook a fost blocată în Etiopia, Bangladesh, Myanmar și Sri Lanka pentru a preveni răspândirea dezinformării și discursurilor de ură, pentru a controla fluxul de informații și a suprima disidența, pe motive de securitate națională ori din cauza conținutului, considerat ofensator pentru islam.
Pe de altă parte, Facebook a fost supus restricțiilor și cenzurii în China, Iran și Coreea de Nord, unde accesul la platformă este fie complet blocat, fie strict restricționat.

***Instagram**:*
Platforma Instagram a fost blocată în China din 2014 ca parte a eforturilor guvernului chinez de a controla fluxul de informații și de a limita accesul la platformele de socializare occidentale. De asemenea, platforma a fost blocată intermitent în Iran, în timpul unor tulburări politice și proteste, pentru a preveni și a stopa răspândirea informațiilor și coordonarea demonstrațiilor. Și Turcia a blocat temporar accesul la Instagram și la alte rețele sociale după o tentativă de lovitură de stat, pentru a preveni răspândirea dezinformării și panica (2016).

În 2020, India a interzis Instagram și alte aproximativ 60 de aplicații chinezești, invocând motive de securitate națională și confidențialitatea datelor. În același an, Federația Rusă a blocat Instagram, ca răspuns la decizia Meta de a permite utilizatorilor din anumite țări să posteze mesaje de incitare la violență împotriva soldaților ruși, în contextul războiului din Ucraina.

Totodată, Instagram a fost supus restricțiilor și cenzurii în Coreea de Nord și Turkmenistan, unde accesul la internet este strict controlat de guvernul național.

Cadrul legal actual al UE/statelor membre ale UE și al celor non-UE, emis pentru reglementarea platformelor de social media

Uniunea Europeană și mai multe state din întreaga lume au acordat atenție cadrului legal și de reglementare astfel încât utilizarea serviciilor de internet să fie mai sigură pentru cetățeni, organizații și companii, dar și pentru a face mai responsabile platformele sociale. Aceste legi impun obligații privind transparența, moderarea conținutului și răspunsul la solicitările autorităților. În plus, au fost înființate autorități responsabile cu activitățile rețelelor sociale. În contrast, în alte țări, legislația necesară reglementării platformelor de social media este inadecvată sau inexistentă. În aceste condiții, autoritățile nu dețin instrumente eficiente prin care să constrângă platformele să își asume responsabilitatea pentru conținutul găzduit și să răspundă prompt solicitărilor de eliminare a conținutului dăunător.

În **Uniunea Europeană**, Serviciul European de Acțiune Externă lucrează, încă din 2015, la combaterea FIMI, inclusiv a dezinformării, precum și la consolidarea comunicărilor strategice în ceea ce privește Parteneriatul Estic, Vecinătatea Sudică și Balcanii de Vest (EEAS 2024). În acest scop, au fost elaborate *Regulamentul General privind Protecția Datelor (GDPR)* din 2016 (EUR-Lex 2016), *Regulamentul privind Serviciile Digitale (DSA)* din 2020 (EUR-Lex 2022b)[6], precum și *Regulamentul privind Piețele Digitale (DMA)* din 2020 (EUR-Lex 2022a)[7].

Și **Germania** a manifestat interes pentru adaptarea legislației la provocările curente. În acest scop, în 2017 a fost adoptată *Legea privind Aplicarea Rețelelor (NetzDG)* (bundesjustizamt.de 2018). Legea NetzDG este una dintre cele mai stricte reglementări din Europa pentru combaterea discursului de ură online și a dezinformării. Aceasta conține prevederi care obligă platformele de socializare, care au peste două milioane de utilizatori în Germania, să elimine conținutul ilegal în termen de 24h, în caz contrar, riscând amenzi de până la 50 de milioane de euro. Deși nu este axată exclusiv pe dezinformarea de origine străină, NetzDG joacă un rol esențial în prevenirea răspândirii conținutului manipulator străin.

Totodată, Germania a înființat *Centrul Național de Apărare Cibernetică*. Această instituție are în componență reprezentanți din agențiile federale, inclusiv *Oficiul Federal pentru Securitatea Informațiilor* (BSI), *Serviciul Federal de Informații* (BND) și *Oficiul Federal pentru Protecția Constituției* (BfV),

[6] Regulamentul (UE) 2022/2065 privind o piață unică pentru serviciile digitale.
[7] Regulamentul (UE) 2022/1925 privind piețele contestabile și echitabile din sectorul digital.

acesta fiind serviciul intern de informații german. Centrul coordonează răspunsul Germaniei la amenințările cibernetice, care includ FIMI și utilizarea instrumentelor cibernetice pentru răspândirea dezinformării.
Pe de altă parte, BfV a dezvoltat programe specializate pentru monitorizarea FIMI în alegeri, concentrându-se în special pe campaniile de dezinformare din Rusia și China. Înaintea alegerilor federale din 2021, BfV a emis avertismente și și-a intensificat monitorizarea rețelelor sociale și a grupurilor finanțate din străinătate, implicate în răspândirea dezinformării.

Franța a adoptat, în 2018, *Legea contra manipulării informațiilor (Loi contre la manipulation de l'information)*, ca răspuns la creșterea îngrijorărilor legate de interferența FIMI în alegeri. Cunoscută sub denumirea de „*Legea Fake News*", aceasta permite judecătorilor să acționeze rapid în timpul alegerilor prin eliminarea/blocarea dezinformării din sursele media, dacă se poate demonstra că acestea difuzează informații în mod deliberat pentru a manipula rezultatele alegerilor. De asemenea, legea impune rețelelor sociale să dezvăluie sponsorii în campaniile electorale, pentru a evita manipularea finanțată din străinătate.

Totodată, *Consiliul Superior al Audiovizualului (CSA)*, organism de reglementare media din Franța, a primit puteri sporite pentru a supraveghea platformele media și diseminarea conținutului. În perioadele electorale, CSA poate acționa împotriva platformelor care permit răspândirea dezinformării sau manipularea provenind de la actori străini. De asemenea, CSA poate impune sancțiuni asupra surselor care nu respectă standardele de transparență privind publicitatea politică.
Pentru reglementarea platformelor de social media, **SUA** fac uz de *Secțiunea 230 din Legea privind Decența în Comunicații a SUA*, promulgată în 1996 (LLI 1996).

În **Australia**, începând cu anul 2021, funcționează *Codul de Negociere a Presei de Știri*.

În **Regatul Unit al Marii Britanii și Irlandei de Nord** a fost promulgată *Legea Siguranței Online 2023* (GOV.UK 2023a). Această lege complexă protejează copiii și adulții în mediul online, include reglementări stricte pentru platformele de social media și motoarele de căutare, impunându-le obligații de a proteja utilizatorii de conținut dăunător, de a elimina rapid conținutul ilegal și de a implementa sisteme și procese necesare reducerii riscurilor asociate cu activități ilegale sau malițioase. Legea mai conține și prevederi referitoare la *Ofcom* (*Autoritatea de reglementare independentă pentru Siguranța Online*), care elaborează recomandări pentru respectarea normelor și care are competențe extinse pentru a evalua și aplica conformitatea platformelor.

Obligațiile legii se aplică serviciilor/motoarelor de căutare și serviciilor care permit utilizatorilor să posteze conținut online sau să interacționeze între ei. Aceasta include o serie de site-uri, servicii de mesagerie instantanee online, aplicații și alte servicii, servicii de social media, site-uri de stocare și partajare în cloud a fișierelor

pentru consumatori, forumuri online, platforme de partajare video și servicii de întâlniri. Legea tratează serviciile legate de Regatul Unit, chiar dacă societățile care le furnizează sunt din afara țării (GOV.UK 2023b). Infracțiunile penale introduse de lege se aplică direct persoanelor care se fac vinovate și acoperă încurajarea sau sprijinirea autovătămării grave, cyberflashing, comunicări amenințătoare, transmiterea de informații false, menite să provoace un prejudiciu care nu este de mică importanță, abuzul de imagini intime, trollingul epileptic.

Conținutul ilegal specific și activitățile de care platformele trebuie să protejeze utilizatorii includ abuzul sexual asupra copiilor, violența sexuală extremă, comportamente de control sau constrângere, pornografie extremă, fraudă, incitarea la violență, infracțiuni de ordine publică agravate rasial sau religios, imigrația ilegală și traficul de persoane, promovarea sau facilitarea sinuciderii, vânzarea de droguri sau de arme ilegale, abuzul de imagini intime (revenge porn), exploatarea sexuală și terorismul. Legea impune, de asemenea, platformelor să elimine rapid conținutul ilegal legat de sinucidere și de autovătămare și să protejeze proactiv utilizatorii împotriva conținutului ilegal, conform *Legii sinuciderii* din 1961.

În Regatul Unit a fost înființată, în 2019, *Unitatea de Combatere a Dezinformării* (CDU), aceasta având scopul de a monitoriza conținutul online care prezintă riscuri pentru sănătatea publică, siguranța publică și securitatea națională, precum și de a răspunde la riscurile de dezinformare, inclusiv pe tema Covid-19. CDU analizează tentativele de dezinformare și poate acționa pentru a dezminți informațiile false pe social media, pentru a desfășura campanii de conștientizare și pentru a încuraja platformele să promoveze surse autoritare de informații. În prezent, CDU se concentrează pe dezinformarea legată de invazia ilegală a Rusiei în Ucraina și a contracarat deja dezinformarea rusă cu privire la Ucraina. CDU a fost convocată de peste 200 de ori în Parlamentul britanic.

În **Canada** funcționează *Legea privind daunele online*, aceasta având în atenție combaterea conținutului online dăunător, inclusiv discursul care incită la ură, dezinformarea și abuzul sexual asupra copiilor.

Singapore a promulgat, în 2019, *Legea pentru protecția împotriva informațiilor false și manipulării online* (POFMA), în baza căreia guvernul poate ordona corectarea sau eliminarea informațiilor false/dăunătoare de pe platformele sociale (Singapore.gov 2019).

Și **Brazilia** are în atenție activitatea online prin *Legea cadru pentru drepturile civile pe internet* din 2014, care stabilește principiile de utilizare a internetului în Brazilia, inclusiv neutralitatea rețelei și protecția datelor personale (Secretaria-Geral 2014).

În **India** regulile privind tehnologia informației (*Orientări privind intermediarii și Codul de etică pentru mediile digitale*) sau „*Regulile IT*" au intrat în vigoare în 2021, în acest context fiind stabilite cerințe specifice de conformitate pentru intermediarii din mediile sociale (Indian.gov 2021). *Regulile IT* au fost introduse pentru a verifica

răspândirea știrilor false, a discursului instigator la ură, a hărțuirii online, unele dintre aspectele semnificative fiind următoarele:

- PSM/alți intermediari trebuie să dea dovadă de diligență, depunând eforturi rezonabile pentru a determina utilizatorii să nu găzduiască, să nu afișeze, să nu încarce, să nu modifice, să nu publice, să nu transmită, să nu stocheze, să nu actualizeze sau să nu partajeze informații care (1) sunt dăunătoare copiilor (2), care încalcă marca comercială, drepturile de autor, brevetul sau alte drepturi de proprietate (3), care sunt defăimătoare, obscene, invazive pentru viața privată a unei alte persoane, care sunt inacceptabile din punct de vedere rasial sau etnic (4), care se dau drept o altă persoană (5), care încalcă orice alte legi.
- Regulile oferă un mecanism eficient de despăgubire prin care utilizatorii/ victimele pot depune o plângere împotriva încălcării normelor IT. Responsabilul cu reclamațiile trebuie să acționeze în timp util după primirea unei plângeri prin care se solicită eliminarea unei informații sau a unei legături de comunicare.
- Este obligatoriu ca toate PSM semnificative să numească un *Chief Compliance Officer* și un *Nodal Officer*, disponibili 24*7, pentru coordonarea cu agențiile de aplicare a legii.

În **România** DNSC a emis, în mai 2023, o recomandare către instituțiile statului și organismele publice, potrivit căreia acestea nu trebuie să descarce, să instaleze sau să utilizeze TikTok în rețelele și sistemele lor informatice. Totodată, autoritățile române au în atenție noi prevederi legale care vizează reglementări mai stricte pentru rețelele sociale, crearea unui mediu online mai sigur și mai responsabil, desemnarea de puncte de contact/reprezentanți naționali pentru rețelele sociale din România, introducerea unor sancțiuni pentru nerespectarea obligațiilor de moderare a conținutului.

Concluzii

Platformele online și motoarele de căutare le permit utilizatorilor să dezvolte rețele globale, acestea reprezentând, la momentul actual, cel mai popular mediu în rândul creatorilor de conținut. Conceptul din spatele lor pare inofensiv, însă accesibilitatea facilă și oportunitățile oferite implică și unele riscuri. Abuzul de proprietate intelectuală, furtul de date personale și bancare, dezinformarea, răspândirea de știri false, conținutul obscen, violența sau discursurile instigatoare la ură sunt câteva dintre provocări.

Atât activitățile malițioase, desfășurate, pe platformele social media, de către actorii statali și nonstatali, cât și alte forme de interferență străină constituie o amenințare la adresa principiilor și valorilor democratice, având un impact negativ asupra securității naționale, democrației, instituțiilor statului, infrastructurii critice, societății, mediului de afaceri și cetățenilor. Unii dintre cei mai expuși la conținutul online dăunător și inadecvat sunt copiii, femeile, fetele, dar și persoanele vârstnice.
Prezenta cercetare științifică atestă că atât utilizatorii obișnuiți, cât și autoritățile naționale se confruntă cu probleme legate de lipsa cadrului legal de reglementare

a procedurilor formale sau a posibilității de a-i contacta direct pe reprezentanții platformelor de social media atunci când este nevoie, pentru a lua măsuri în vederea blocării/eliminării/modificării în timp util a unor astfel de activități ilegale sau mesaje inadecvate. Studiul atestă inclusiv existența mai multor plângeri referitoare la lipsa unei reacții adecvate din partea PSM la rapoartele și cererile utilizatorilor pentru blocarea/eliminarea vectorilor de atac.

Pe de altă parte, platformele de social media se confruntă cu provocări continue în moderarea conținutului online dăunător. Unele dintre platforme au implementat diverse măsuri pentru a contracara provocările cu care se confruntă (moderarea conținutului, creșterea transparenței cu privire la moderarea conținutului, îmbunătățirea algoritmilor pentru a detecta automat conținutul dăunător, clasificarea conținutului, colaborarea cu fact-checkeri), însă acestea sunt adesea insuficiente și lente. Situația prezentată se datorează parțial volumului mare de conținut generat de utilizatori, dar și lipsei unor stimulente și sancțiuni suficiente pentru a acționa rapid și eficient.

A sosit momentul ca platformele de social media să își asume responsabilitatea, să investească în măsuri de securitate robuste, să abordeze proactiv această problemă și să prioritizeze siguranța utilizatorilor în era digitală. Obligațiile legale ar trebui aduse în atenția tuturor radiodifuzorilor și platformelor de social media pentru a oferi publicului informații imparțiale și obiective, prezentând faptele și evenimentele corect și cu respect pentru libertatea de exprimare.

În urma acestui studiu, se poate concluziona că **statele au nevoie de cadre și de politici de reglementare eficiente pentru a face utilizarea serviciilor de internet mai sigură**. Acestea ar trebui **să fie aplicate platformelor de social media, motoarelor de căutare și serviciilor care permit utilizatorilor să posteze conținut online sau să interacționeze între ei**: o gamă de site-uri, mesagerie instant online, forumuri online, aplicații de servicii și alte servicii, inclusiv cele de social media, site-uri de stocare și partajare de fișiere cloud pentru consumatori, platforme de partajare video, servicii de întâlniri etc. Legislația ar trebui să fie echilibrată, să protejeze libertatea de exprimare, dar și să se asigure că platformele online își asumă responsabilitatea pentru conținutul găzduit și contribuie la un mediu online mai sigur și mai sănătos, pentru a proteja utilizatorii de conținutul dăunător, pentru a elimina rapid conținutul ilegal, pentru a implementa sisteme și procese necesare reducerii riscurilor legate de serviciile oferite, atunci când sunt utilizate pentru activități malițioase.

Având în vedere contextul actual și experiența internațională, țările din întreaga lume ar putea reflecta asupra adoptării de măsuri legislative în următoarele domenii, pentru a reglementa mai eficient platformele social media, motoarele de căutare și serviciile care permit utilizatorilor să posteze conținut online social, dar și pentru a-i proteja pe aceștia. Analizând cadrul actual, **transparența și responsabilitatea** platformelor online reprezintă un element esențial. Acestea ar trebui să numească un reprezentant național în statele în care funcționează, care să răspundă de comunicarea cu autoritățile și de asigurarea conformității cu legislația locală. De asemenea, este

necesar ca utilizatorii să aibă la dispoziție mecanisme simple și accesibile pentru a raporta conținutul dăunător și/sau a contesta deciziile de moderare. În același timp, se impune ca platformele online să publice periodic rapoarte detaliate privind măsurile luate pentru a modera conținutul, numărul de plângeri primite și modul în care au fost soluționate.

În ceea ce privește, **moderarea conținutului**, platformele social media, motoarele de căutare și serviciile care permit utilizatorilor să posteze conținut online sau să interacționeze între ei ar trebui să fie obligate să elimine conținutul ilegal într-un termen scurt de la notificare. Totodată, este necesar ca acestea să colaboreze mai bine cu organizații independente de fact-checking și cu experți în drepturile omului pentru a îmbunătăți moderarea conținutului. Pe de altă parte, platformele ar trebui încurajate să utilizeze tehnologii avansate, precum inteligența artificială, pentru a identifica și a elimina cu celeritate, în mod automat, conținutul dăunător.

Referitor la **protecția utilizatorilor**, este important să se implementeze măsuri speciale pentru protejarea copiilor de conținutul dăunător, precum restricții de vârstă și instrumente de control parental. Platformele de social media ar trebui să ia măsuri eficiente pentru a limita răspândirea dezinformării, punând accent pe etichetarea conținutului fals sau înșelător și promovarea surselor de informații credibile. Este necesar ca legislația privind protecția datelor personale să fie respectată strict, iar utilizatorii să dețină controlul asupra modului în care datele lor sunt colectate și utilizate.

În vederea sprijinirii acestor măsuri, **se impune înființarea unor organisme de supraveghere și reglementare**. Astfel de organisme sunt necesare pentru a supraveghea activitatea platformelor social media, motoarelor de căutare și serviciilor care permit utilizatorilor să posteze conținut online sau să interacționeze între ei. De asemenea, entitățile în cauză ar trebui să aibă atribuții pentru a putea lua măsuri împotriva companiilor sau platformelor care permit realizarea online a acțiunilor de tip FIMI ori a altor activități ilegale, iar totodată, să impună sancțiuni, în cazul încălcării legilor și normelor stabilite.

În ceea ce privește **sancțiunile**, platformele online care nu respectă obligațiile legale ar trebui sancționate cu amenzi proporționale cu gravitatea încălcării și cu cifra de afaceri a companiei. În situații deosebite, se impune ca autoritățile naționale să aibă posibilitatea de a suspenda temporar sau de a bloca serviciile furnizate de platformele online și motoarele de căutare, oricând când situația o va cere.

Referințe

Adrien, Claudia. 2023. "Phishing Attacks Target Facebook, Microsoft, Making Them Most Impersonated Brands". https://www.channelfutures.com/security/phishing-attacks-target-facebook-microsoft-making-them-most-impersonated-brands.

Alexander, Brooke Nelson. 2022. "What Is Doxxing, and How Does It Set You Up to Be Hacked?" https://www.rd.com/article/what-is-doxxing/.

—. 2023. "What Is Spoofing, and How Can You Spot It?". https://www.rd.com/article/spoofing/.

—. 2024. "14 Facebook Marketplace Scams to Watch Out For". https://www.rd.com/article/facebook-marketplace-scams/.

Baiaș, Ionuț. 2023. „Directoratul Național de Securitate Cibernetică recomandă interzicerea TikTok pe dispozitivele instituțiilor publice". https://hotnews.ro/directoratul-national-de-securitate-cibernetica-recomanda-interzicerea-tiktok-pe-dispozitivele-institutiilor-publice-64785.

Bradford, Alina. 2024. "8 Common Bank Scams to Watch Out For". https://www.rd.com/list/bank-scams/.

Budgar, Laurie. 2024. "Can You Really See Who Viewed Your Facebook Profile Recently?". https://www.rd.com/article/who-viewed-my-facebook-profile/.

bundesjustizamt.de. 2018. "Network Enforcement Act Regulatory Fining Guidelines". https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/NetzDG/Leitlinien_Geldbussen_en.pdf?__blob=publicationFile&v=3.

Chin, Kyle. 2024. "19 Most Common Types of Phishing Attacks in 2024". https://www.upguard.com/blog/types-of-phishing-attacks.

Comisia Europeană. 2024. "Commission opens proceedings against TikTok under the DSA regarding the launch of TikTok Lite in France and Spain". https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2227.

DNSC. 2023a. „ALERTA: Tentative de fraudă promovate prin anunțuri sponsorizate pe rețelele sociale". https://www.dnsc.ro/citeste/alerta-tentative-de-frauda-promovate-prin-anunturi-sponsorizate-social-media.

—. 2023b. "Press release." https://dnsc.ro/vezi/document/comunicat-de-presa-dnsc-recomanda-autoritatilor-si-institutiilor-publice-din-romania-interzicerea-descarcarii-instalarii-si-utilizarii-a-aplicatiei-tiktok-pe-dispozitivele-de-serviciu-pdf.

EEAS. 2024. "Tackling Disinformation, Foreign Information Manipulation & Interference". https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en.

EUR-Lex. 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data". https://eur-lex.europa.eu/eli/reg/2016/679/oj.

—. 2022a. "Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector". https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022R1925.

—. 2022b. "Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services". https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

Giles, Keir. 2016. "Handbook of Russian Information Warfare". https://www.ndc.nato.int/news/news.php?icode=995.

Gordon, Anna. 2024. "Here's All the Countries With TikTok Bans as Platform's Future in U.S. Hangs In Balance". https://time.com/6971009/tiktok-banned-restrictions-worldwide-countries-united-states-law/.

GOV.UK. 2023a. "Online Safety Act 2023." https://www.legislation.gov.uk/ukpga/2023/50/enacted.

—. 2023b. "What the Online Safety Act does." https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer#:~:text=The%20Online%20Safety%20Act%202023,users'%20safety%20on%20their%20platforms.

Hindman, Matthew. 2018. "Disinformation, 'Fake News' and Influence Campaigns on Twitter." https://knightfoundation.org/reports/disinformation-fake-news-and-influence-campaigns-on-twitter/.

Indian.gov. 2021. "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code)." https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28updated%2006.04.2023%29-.pdf.

ITU. 2021. "Session 5: Disinformation, misinformation, malinformation and Infodemics: Ways to handle". https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events/2021/ASP%20Regional%20Dialogue%20on%20Digital%20Transformation/Session%20Pages/RD-Session-5.aspx.

Justia. 2021. "Gonzalez v. Google, LLC, No. 18-16700 (9th Cir. 2021)." https://law.justia.com/cases/federal/appellate-courts/ca9/18-16700/18-16700-2021-06-22.html.

Lakshmanan, Lavie. 2024. "Canada orders TikTok to shut down Canadian operations over security concerns". https://thehackernews.com/2024/11/canada-orders-tiktok-to-shut-down.html?m=1.

LLI. 1996. "47 U.S. Code § 230 – Protection for private blocking and screening of offensive material." https://www.law.cornell.edu/uscode/text/47/230.

PakVoices. 2023. "Disinformation impacts on digital sphere in Pakistan (May-July 2023)." https://pakvoices.pk/?p=13745.

Petkauskas, Vilius. 2023. "Facebook Messenger phishing attack pumps out 100K+ weekly messages". https://cybernews.com/news/facebook-messenger-phishing-attack/.

Qureshi, Anees. 2023. "Meta Neglecting the Proliferation of Phishing Scam Pages on Facebook, Leaving Millions of Users Vulnerable". https://www.linkedin.com/pulse/meta-neglecting-proliferation-phishing-scam-pages-facebook-qureshi-dsizf/.

Rosenkrantz, Holly. 2024. "What Is Phishing, and How Can You Prevent This Cyberattack?". https://www.rd.com/article/what-is-phishing/.

Saint Francis University. 2023. "Misinformation, Disinformation, and Fake News". https://libguides.francis.edu/fake-news.

Sasnauskas, Mantas. 2023. "We uncovered a Facebook phishing campaign that tricked nearly 500,000 users in two weeks". https://cybernews.com/security/we-uncovered-a-facebook-phishing-campaign-that-tricked-nearly-500000-users-in-two-weeks/.

Schappert, Stefanie. 2024. "Meta deletes 63K sextortion scam accounts from Instagram, Facebook".https://cybernews.com/news/meta-deletes-63k-sextortion-scam-accounts-instagram-facebook/.

Secretaria-Geral. 2014. "LEI Nº 12.965, DE 23 DE ABRIL DE 2014." http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

Singapore.gov. 2019. "Protection from Online Falsehoods and Manipulation Act 2019." https://sso.agc.gov.sg/Act/POFMA2019.

Snegovaya, Maria. 2015. "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare, Institute for the Study of War." https://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare.

Stathis, Jaime. 2024a. "14 Online Scams You Need to Be Aware Of—and How to Avoid Them". https://www.rd.com/list/how-to-avoid-online-scams/.

—. 2024b. "9 Red Flags You're About to Click on a Fake Social Media Ad". https://www.rd.com/list/fake-ads-on-social-media/.

Toulas, Bill. 2023a. "Facebook disrupts new NodeStealer information-stealing malware." https://www.bleepingcomputer.com/news/security/facebook-disrupts-new-nodestealer-information-stealing-malware/.

—. 2023b. "Facebook Messenger phishing wave targets 100K business accounts per week". https://www.bleepingcomputer.com/news/security/facebook-messenger-phishing-wave-targets-100k-business-accounts-per-week/.

Zaleznik, Daniel. 2021. "*Facebook and Genocide: How Facebook contributed to genocide in Myanmar and why it will not be held accountable*". https://systemicjustice.org/article/facebook-and-genocide-how-facebook-contributed-to-genocide-in-myanmar-and-why-it-will-not-be-held-accountable/.

Zaytsev, Oleg. 2023. "«MrTonyScam» — Botnet of Facebook Users Launch High-Intent Messenger Phishing Attack on Business Accounts". https://labs.guard.io/mrtonyscam-botnet-of-facebook-users-launch-high-intent-messenger-phishing-attack-on-business-3182cfb12f4d.