PROVOCĂRILE VIITORULUI: CRIMINALITATEA CIBERNETICĂ ORGANIZATĂ. IMPLICAȚII GLOBALE ȘI LOCALE

COSMIN ROBERT POPESCU*, COSTIN-LUCIAN GHEORGHE**

ABSTRACT

THE CHALLENGES OF THE FUTURE: ORGANIZED CYBERCRIME. GLOBAL AND LOCAL IMPLICATIONS

Organized crime is undergoing various transformations in the digital era, evolving from hierarchical, territorially bound groups into flexible, technologically mediated networks capable of operating across multiple jurisdictions while relying on minimal physical infrastructure. This article examines the phenomenon of digital organized crime in Romania, situating it within broader theoretical perspectives. The article draws on the analysis of academic sources from the fields of sociology, criminology, economic criminology, and cybercrime studies in order to trace the conceptual evolution of organized crime. It outlines the typologies and effects of digital organized crime at the global level and how these manifest within the Romanian context. In this article, we argue that criminal dynamics in Romania have evolved in the direction of digitalization, driven by the technical sophistication of the population and of cyber infrastructure. Moreover, this evolution has been fueled by socio-economic vulnerabilities and gaps in institutional response. The conclusions highlight the need for policy and legislative responses that include regional cooperation and AI-assisted law enforcement.

Keywords: cross-border organized crime, money laundering, drug trafficking, cyber racketeering, ransomware.

INTRODUCERE

Convergența dintre tehnologia digitală și crima organizată reprezintă una dintre cele mai importante evoluții din criminologia contemporană, cu repercursiuni asupra vieții individuale și a instituțiilor. În ultimele trei decenii, adoptarea

* Associate Researcher, Institute of Sociology of the Romanian Academy, e-mail address: *rcosminp@gmail.com.*

** PhD Candidate, Faculty of Sociology and Social Work, e-mail address: *gheorghecostinlucian@yahoo.com*.

„Revista română de sociologie”, serie nouă, anul XXXVII, nr. 3–4, p. 213–241, Bucureşti, 2026

DOI: 10.59277/RJSoc.2026.3-4.04

internetului, a platformelor de comunicare criptate, a criptomonedelor și a inteligenței artificiale a modificat *modus operandi* al organizațiilor criminale, nu doar prin furnizarea de noi instrumente, ci și prin reconfigurarea a însăși structurii și a puterii organizațiilor criminale (Sullivan, 2023; Di Nicola, 2022).

Evoluția conceptuală a crimei organizate, de la definițiile clasice (Maltz, 1976) la cadrul Convenției ONU (Zabyelina, 2023), a fost puternic influențată de digitalizare. Literatura recentă documentează tipologii și efecte specifice crimei organizate digitale la nivel global (Grabosky, 2007; Choo, 2008; Di Nicola, 2022), a căror manifestare în contextul românesc rămâne insuficient studiată (Racoveanu, 2024; Nicolae, 2017; Lusthaus și Varese, 2017). Cadrele criminologice clasice, dezvoltate în principal în jurul paradigmelor crimei organizate americane și italiene de la mijlocul secolului al XX-lea, au presupus un set de caracteristici definitorii precum ierarhie, control teritorial, violență, corupție și longevitate, variabile care nu reușesc să explice realitatea grupurilor criminale contemporane (Maltz, 1976; Lusthaus, 2013; Whelan *et al*., 2024). Mai mult, grupurile infracționale rămân puțin înțelese, în ciuda dimensiunilor macroeconomice la care au ajuns, din cauza absenței datelor și a cadrelor analitice capabile să măsoare impactul și adevărata lor amploare (Costa, 2021).

Di Nicola (2022) studiază „crima organizată digitală" printr-o abordare spectrală a organizării activităților criminale, care variază de la grupuri de criminalitate cibernetică pur online la organizații tradiționale *offline*, mediate din ce în ce mai mult de tehnologiile digitale, completând astfel limitările abordărilor tradiționale asupra crimei organizate. Grupurile care practică *ransomware* (ex: LockBIt, Akira, CI0p), rețelele de spălare de bani bazate pe criptomonede, operațiunile de fraudă asistate de IA și piețele de pe *dark web* coexistă acum cu întreprinderile criminale tradiționale și adesea se confundă cu acestea în moduri care pun la încercare atât claritatea definițiilor, cât și capacitatea de răspuns instituțional (Whelan *et al*., 2024; Tung, 2021; Racoveanu, 2024).

România constituie un caz deosebit în acest peisaj. Ca stat postcomunist membru al Uniunii Europene, România se remarcă printr-o activitate considerabilă de activități de criminalitate cibernetică. Explicațiile acestei evoluții includ competențele tehnice ridicate ale populației sale, vulnerabilitățile instituționale și situația economică. Importanța cazului românesc, recunoscută de EUROPOL, FBI și DIICOT în rapoarte operaționale succesive sau în anchete concrete, solicită o atenție academică mai intensă, având în vedere noile provocări presupuse de statutul de membru Schengen dar și de războiul de la graniță, care se manifestă atât pe plan fizic, prin conflict armat, cât și pe plan cibernetic.

Acest articol completează studiul infracțiunilor digitale din România printr-o analiză a 31 de surse academice. Articolul începe cu o trecere în revistă a literaturii existente privind criminalitatea organizată și criminalitatea organizată cibernetică, urmând apoi descrierea metodologiei. În continuare, prezintă cadrul teoretic al crimei organizate la nivel global, iar în secțiunile ulterioare acest cadru este aplicat contextului românesc. În partea finală sunt prezentate concluziile și recomandările pentru comunități și instituții.

LITERATURA DE SPECIALITATE

Studiul academic al crimei organizate, încă de la începuturile sale, a fost caracterizat prin lipsa unui consens general asupra definiției crimei organizate. Maltz (1976) a identificat un paradox, subliniat de utilizarea inconsecventă a termenului „crimă organizată" pentru a se referi atât la acte criminale, cât și la organizații criminale, ceea ce a dus la incoerență conceptuală. Deceniile următoare au produs numeroase definiții, tipologii și cadre teoretice concurente, o diversitate pe care Zabyelina (2023) o atribuie tensiunii nerezolvate dintre studiile privind criminalitatea în domeniul economic și cercetarea privind grupările infracționale în cadrul mai larg al criminologiei economice.

O parte a literaturii s-a concentrat asupra caracteristicilor organizaționale ale grupurilor criminale. Rider (1993) a identificat continuitatea, urmărirea profiturilor mari, folosirea sistematică a corupției, izolarea de efectele legii a conducerii organizației criminale și diversificarea activităților ilegale și cuplarea acestora cu afaceri legale, ca trăsături definitorii ale întreprinderii criminale organizate. Aceste caracteristici fac din cercetarea financiară bazată pe active (urmărirea veniturilor provenite din activități criminale) cel mai eficient instrument de investigație disponibil forțelor de ordine. Această perspectivă se bazează pe lucrări anterioare privind economia crimei, precum studiul lui Hann (1971), care a propus un cadru de analiză economic cu ajutorul căruia criminalitatea este înțeleasă ca o activitate ce produce efecte economice negative necompensate, „diseconomy" (un cost pentru victimă care nu a fost acceptat de aceasta și pentru care nu a fost compensată).

Costa (2010) a extins acest cadru economic la nivel transnațional. Oficialul ONU a studiat amploarea macroeconomică a crimei organizate în traficul de droguri, traficul de persoane, comerțul cu arme, contrafacerea și criminalitatea cibernetică, și a militat pentru dezvoltarea unei discipline formale a economiei crimei organizate.

Relația dintre structurile infracționale și cele politice a fost examinată din perspective multiple. Barnes (2017) a contestat separarea convențională dintre violența politică și cea criminală, propunând conceptul de „politică criminală" și o tipologie în patru părți a relațiilor dintre crimă și stat, anume confruntare, aplicare-evaziune, alianță și integrare, care situează organizațiile criminale în contextul mai larg al violenței politice și al funcționării statale. Arias (2018) a completat această analiză concentrându-se pe factorii micro-sociali care influențează elaborarea politicilor, demonstrând prin cercetarea de teren desfășurată în Rio de Janeiro, Medellin și Kingston că organizațiile criminale influențează politica locală prin fricțiuni, diviziuni și mediere, în funcție de relația lor cu oficialii statului. Felbab-Brown (2017) a dezvoltat și mai mult modelul, prin observarea relației complexe și adesea contraintuitive dintre economiile ilicite, rețelele de tip mafiot și reprezentanții instituțiilor. Astfel, Felbab-Brown prezintă, printre altele, modul în care politicile menite să suprime economiile ilicite pot consolida, în mod involuntar, legitimitatea

politică a grupurilor criminale. Aceste politici ineficiente ajută grupurile infracționale să se poziționeze în rolul de protectori ai comunității locale.

Caracterul transfrontalier al crimei organizate a fost teoretizat în mai multe studii. Singh *et al.* (2025) urmăresc patru faze istorice ale evoluției crimei organizate transnaționale, de la era decolonizării până la perioada post-Război Rece, rețelele sofisticate din punct de vedere tehnologic din anii 2000 și faza pandemiei de COVID-19. Pe lângă aceste intervale care marchează evoluția crimei organizate, cercetătorii studiază și impactul economiilor criminale transfrontaliere asupra națiunilor în curs de dezvoltare, cu clasă politică și instituții slabe.

Cubides-Cardenas *et al.* (2025) susțin că rețelele de delincvență extinsă funcționează ca un guvern paralel, îndeplinind funcții sociale, economice și coercitive alocate în mod tradițional statului. Astfel, răspunsurile eficiente la această situație necesită o cooperare regională largă și mecanisme colective de informare.

Schonenberg și Heinrich-Boll-Stiftung (2013) consideră organizația infracțională ca o trăsătură inerentă globalizării economice, nu doar o latură întunecată a acesteia, subliniind amenințarea pe care o reprezintă pentru procesul democratic, prin potențialul de corupție a capitalului obținut ilicit.

Un contrapunct critic la cadrele de globalizare este oferit de Hobbs (1998), care susține că discursul privind crima organizată transnațională constituie o panică morală post-Război Rece utilă intereselor bugetare ale agențiilor de securitate (*intelligence*) occidentale aflate în declin. Hobbs susține că rețelele infracționale se constituie și se manifestă în principal la nivel local, iar globalizarea a intensificat, în mod paradoxal, caracterul distinctiv al specificului local al acestor filiere. Se creează astfel o dinamică „glocală", în care fluxurile de capital sau activitățile criminale globale sunt întotdeauna mediate prin celule infracționale locale.

Tranziția către era digitală a generat un nou tip de crimă organizată, infracționalitatea cibernetică, care la rândul ei a determinat noi abordări de cercetare a fenomenului și un nou corpus de literatură de specialitate. Grabosky (2007) a fost printre primii care au examinat modul în care tehnologiile digitale sunt exploatate de grupurile criminale organizate. Acesta a tratat modul în care tehnologia a transformat activitățile criminale organizate, concentrându-se pe aspectul calitativ și pe cel al eficientizării. Sullivan (2023) a argumentat că ascensiunea *statului-rețea* (concept preluat de Sullivan de la Castells, pentru a denumi statul în societatea informației, unde noile tehnologii facilitează transformarea rețelelor de putere, a economiei oficiale și a celei negre, și contribuie la crearea unor noi tipuri de rețele interactive, care se manifestă prin mișcări sociale, proteste etc.) (*ibidem*, p. 53) a produs noi forme de activitate criminală, facilitate de tehnologiile de comunicare digitală. Di Nicola (2022) a propus un cadru teoretic amplu, bazat pe conceptul de „criminalitate organizată digitală" și o „teorie a spectrului" asociată, care plasează grupurile criminale pe un continuum, de la organizații de criminalitate cibernetică pur online la grupuri tradiționale *offline*, cu o gamă de formațiuni

hibride om-calculator. Acest cadru a fost ulterior operaționalizat de Di Nicola *et al.* (2025), care au aplicat o grilă de 15 elemente constitutive derivate din literatura de specialitate privind definiția crimei organizate la 71 de cazuri judiciare din baza de date SHERLOC a UNODC. În urma acestui studiu au propus un cadrul analitic adaptat pentru activitățile delincvente sistematice, în mediul fizic și în cel digital.

În privința tipologiilor organizațiilor delincvente contemporane, Choo (2008) a propus o clasificare cu trei categorii: în prima categorie se înscriu grupurile criminale organizate tradiționale care utilizează TIC pentru a-și intensifica activitățile *offline*, în cea de-a doua, grupurile care operează exclusiv online și în ultima categorie, grupurile motivate ideologic sau politic ce utilizează instrumentele digitale pentru activități ilegale. Lavorgna (2015) a propus o bază empirică pentru aceste distincții printr-un studiu cu metode mixte care a combinat 31 de interviuri cu experți și 120 de studii de caz judiciare din Italia, Regatul Unit, Statele Unite și Olanda, demonstrând că internetul funcționează, în primul rând, ca un facilitator al infracțiunilor pentru grupurile criminale organizate tradiționale, mai degrabă decât ca bază a unor formațiuni complet noi. Leukfeldt *et al.* (2019) au extins acest demers empiric prin intermediul *Dutch Organised Crime Monitor* și au constat că rețelele de tip mafiot din era digitală presupun un amestec de infractori tradiționali cu experiență infracțională îndelungată și un număr limitat de membri ce dețin competențe tehnice.

Lusthaus (2013) a testat percepțiile privitoare la sofisticarea organizațională a grupurilor de criminalitate cibernetică și a constatat că, deși actorii de pe unele forumuri online cunoscute pentru tranzacții ilegale adoptă terminologia mafiei, ierarhia și nivelul lor de organizare nu este în acord cu definițiile academice.

Specializarea infracțională a făcțiunilor cu activitate ilicită în sfera digitală a fost tratată în diverse lucrări. Whelan *et al.* (2024) au examinat grupurile care lansează operațiuni de *ransomware* prin prisma cadrului de analiză lui von Lampe, care presupune trei dimensiuni: activitățile infracționale, structurile sociale ale infractorilor și controlul teritorial. În studiu se afirmă că anumite grupuri de *ransomware* îndeplinesc criteriile crimei organizate dacă sunt analizate printr-un cadru flexibil, iar aspectele precum violența și controlul teritorial sunt reconceptualizate pentru contextul digital.

Tung (2021) a menționat rolul platformelor de comunicare criptată, Sky ECC, EncroChat și infrastructura *dark web* în facilitarea rețelelor transnaționale și a spălării de bani. Jian *et al.* (2020) au analizat extorcarea cibernetică organizată printr-o metodologie *grounded theory* aplicată la 80 de cazuri judecate, identificând, la baza modului de operare al celor judecați, o rațiune motivațională, activități de organizare, direcții de învățare și implementare, specifice grupurilor infracționale. Folosirea criptomonedelor pentru activități ilicite a fost abordată de Albrecht *et al.* (2019), care au urmărit operațiunile de spălare de bani cu ajutorul criptomonedelor prin secvența clasică plasare, stratificare și integrare, iar Garcia Otero și Mendez Diaz (2025), au studiat, în Columbia, un exemplu al modului în

care criptomonedele sunt integrate în operațiunile ilicite internaționale. Racoveanu (2024) a evidențiat rolul dual al inteligenței artificiale, atât ca instrument de transgresiune a legii, cât și ca instrument de aplicare a acesteia. Constatarea autorului este că prin IA, grupurile criminale reușesc să cloneze voci, să producă *deepfake* și să transforme modelul infracțional, care necesita cunoștințe tehnice ridicate, în „Crime-as-a-Service" menționat de EUROPOL.

METODOLOGIE

Acest articol se bazează pe analiza datelor secundare și pe cercetarea documentară. Sursele documentare se împart în trei categorii: literatura academică, rapoartele instituționale și anchete jurnalistice.

Baza de surse academice cuprinde 31 de articole și capitole de carte care acoperă domenii precum criminologia, criminologia economică, studii privind criminalitatea cibernetică, științele politice și sociologia organizațională, acoperind perioada de la Maltz (1976) până la Di Nicola *et al.* (2025). Acestea au fost selectate de autori pe baza relevanței lor pentru subiectul articolului și acoperă următoarele domenii tematice: evoluția conceptuală a crimei organizate, tipologia organizațiilor criminale, efectele activității criminale organizate (inclusiv ale celei cibernetice) la nivel global, criminalitatea organizată cibernetică și efectele acesteia în spațiul românesc.

Documentele instituționale includ rapoarte ale instituțiilor de forță naționale și internaționale precum DIICOT (2024, 2025), EUROPOL (2025, 2026), FBI (2020, 2025), Serviciul Român de Informații (SRI, 1996), dar și ale unor instituții financiare precum Banca Mondială.

CRIMA ORGANIZATĂ – DEFINIȚII

Pentru a trece peste impasul conceptual, Maltz (1976) definește crima organizată drept un act ilicit comis de doi sau mai mulți asociați și include în această definiție o tipologie bazată pe mijloacele utilizate (violență, furt, corupție, putere economică, înșelăciune, complicitatea victimei) și pe obiectivele urmărite (putere politică sau economică). Acest cadru a reprezentat un progres față de teoriile bazate pe etnie care dominau discursul criminologic american, în special modelul care atribuia crima organizată în primul rând grupurilor de imigranți. Zabyelina (2023) urmărește genealogia acestei dispute definiționale prin prisma criminologiei economice. Aceasta argumentează că studiul structurilor infracționale face parte din criminologia economică și subliniază motivația economică a activităților acestor structuri. În această perspectivă, Convenția Națiunilor Unite împotriva crimei organizate transnaționale (UNTOC, 2000 în Zabyelina, 2023) oferă cea mai larg acceptată definiție, ce susține că un grup delincvent este format din trei sau mai multe persoane care activează pentru o perioadă de timp și

acționează în mod concertat cu scopul de a comite infracțiuni pentru a obține beneficii financiare sau alte beneficii materiale. Astfel, definiția din Codul penal român a grupului criminal organizat (art. 367) reflectă îndeaproape cadrul stabilit de Convenția împotriva crimei organizate.

Rider (1993) a identificat un set de caracteristici care completează aceste definiții. Conform acestuia, sindicatele crimei organizate se disting prin continuitatea lor, mai degrabă decât prin acte ilegale izolate, prin caracterul lor antreprenorial, prin necesitatea de a corupe, corupția servind atât la protejarea întreprinderii, cât și la facilitarea activităților sale, prin izolarea ierarhică a conducerii de expunerea operațională și prin diversificarea deliberată a activităților și jurisdicțiilor în care activează. Rider (1993) a indicat analiza tranzacțiilor și a activelor financiare ca metodă principală de investigare, având în vedere că singura legătură concretă între organizație și activitatea ilicită este, de obicei, fluxul de venituri provenite din activitățile ilegale.

Referitor la evoluția crimei organizate, la nivel global, Singh *et al.* (2025) identifică patru faze istorice: etapa de fondare, începută prin decolonizarea ce s-a desfășurat în anii 1970, o a doua fază de la începutul anilor 1990 marcată de instabilitatea post-Război Rece și de alianțele organizațiilor criminale transfrontaliere, o a treia fază care începe aproximativ din anii 2000, caracterizată de activitatea rețelelor mafiote sofisticate din punct de vedere tehnologic și o a patra etapă, care a început odată cu pandemia de COVID-19. Această ultimă etapă a intensificat activitatea ilegală prin accentuarea sărăciei, a eșecurilor guvernamentale și a vulnerabilizării instituțiilor. Periodizarea propusă de Singh *et al.* (2025) subliniază caracterul dinamic al fenomenului și faptul că este influențat de transformări politice și socio-economice.

Hobbs (1998) critică cadrul globalizării prin argumentul că discursul privind crima organizată transfrontalieră a apărut dintr-o conjunctură politică specifică post-Războiului Rece. Hobbs presupune că acest discurs servea intereselor instituționale ale agențiilor de securitate occidentale, iar dovezile empirice nu susțin existența unor formațiuni cu adevărat noi. Examinând dinamica locală a crimei organizate într-un context urban englez, Hobbs a constatat că ceea ce apare ca activitate ilegală organizată transnațională se realizează, de obicei, prin conectarea rețelelor criminale locale la fluxurile globale de mărfuri ilicite. Acest cadru „glocal", în care actorii locali se conectează la infrastructura criminală globală fără a deveni organizații internaționale, are implicații pentru analiza cazurilor precum România, unde rețelele interlope interne au dobândit o anvergură internațională, păstrându-și în același timp structura de bază locală.

Barnes (2017) a demonstrat că violența manifestată de sindicatele crimei organizate este echivalentă cu violența politică în ceea ce privește efectele sale asupra statului, capacității instituționale și ordinii sociale. Argumentul său, faptul că omorurile intenționate comise de grupări infracționale între 2007 și 2012 au înregistrat o medie anuală de peste cinci ori mai mult decât media deceselor

cauzate de conflicte directe în aceeași perioadă, îl determină să includă studiul acestui tip de violență în aria științelor politice. Tipologia sa privind relațiile dintre crimă și stat (confruntare, aplicare-evaziune, alianță și integrare), oferă un cadru pentru situarea cazurilor naționale specifice în cadrul unei sociologii comparative a crimei organizate.

EFECTELE CRIMEI ORGANIZATE LA NIVEL GLOBAL

Efectele activităților entităților criminale la nivel global se manifestă pe plan economic, politic, social și instituțional, iar interdependențele dintre acestea provoacă un impact cumulativ, destabilizator la nivel societal. Costa (2010) a luat în considerare amploarea macroeconomică a acestor efecte pe baza datelor Oficiul Națiunilor Unite pentru Droguri și Criminalitate. Astfel, crima organizată are efecte directe asupra integrității fizice și libertății personale: s-au înregistrat aproximativ 140 000 de victime ale traficului de persoane în scopul exploatării sexuale numai în Europa (ceea ce costă UE 3 miliarde de dolari anual). Migrația ilegală (2,5 până la 3 milioane de migranți traficați din America Latină către Statele Unite anual) generează pierderi la nivelul UE de 6,6 miliarde de dolari, iar piața europeană a heroinei este evaluată la 20 de miliarde de dolari. Mărfurile contrafăcute la frontierele europene depășesc 10 miliarde de dolari anual, iar furtul de identitate afectează 1,5 milioane de persoane anual, cu un cost de un miliard de dolari. Aceste cifre, susține Costa (2010), reprezintă estimări prudente, având în vedere absența unor instrumente de măsurare mai precise pentru economiile ilicite.

Efectele economice ale grupurilor delicvente sunt atât directe, cât și indirecte, iar distribuția lor este inegală în contextele naționale. Hann (1971) a stabilit fundamentul teoretic pentru înțelegerea crimei organizate ca sursă de „diseconomies" (costuri impuse terților și bunăstării sociale mai largi, care sunt absorbite de victime și de stat). Rider (1993) a studiat modul în care infracțiunile economice devin atractive pentru grupurile delicvente organizate pentru că sunt profitabile și prezintă un risc redus, fiind capabile să finanțeze și astfel să faciliteze tipuri de activități economice legale. Ering (2011) a demonstrat efectul asupra economiilor în curs de dezvoltare, unde criminalitatea transfrontalieră subminează integritatea instituțională, influențează negativ piețele forței de muncă și drenează resurse dinspre activitatea economică legitimă. Mocetti și Rizzica (2024) au analizat date cantitative ale daunelor economice provocate de activitatea mafiei în Italia, și au constatat că provinciile cu o pătrundere mai mare a mafiei au înregistrat, comparativ cu celelalte provincii, o creștere mai mică a ocupării forței de muncă și a valorii adăugate pe o perioadă de 50 de ani.

Efectele politice ale crimei organizate au fost analizate de Felbab-Brown (2017), care a cercetat modul în care economiile ilicite furnizează rețelelor infracționale și politicienilor corupți resursele necesare pentru a infiltra și, în cele

din urmă, a domina procesele democratice. Scandalul columbian al „politicii paralele" este un exemplu în care grupurile criminale și paramilitare au controlat numeroase administrații municipale și au sponsorizat cel puțin o treime din Congresul Național. Corupția sistemelor judiciare este un efect mai degrabă principal decât secundar, iar cazul Mexicului susține acest lucru, întrucât doar 2% din infracțiunile violente au fost efectiv urmărite penal în timpul războiului declarat de autorități împotriva cartelurilor în 2006, război care a durat mai bine de zece ani (Felbab-Brown, 2017). Arias (2018) a adăugat perspectiva microsocială la analiza efectelor politice, printr-o cercetare de teren efectuată în trei orașe. Acesta a demonstrat că grupurile de tip mafiot influențează politica locală prin trei mecanisme distincte, fricțiunea, dezbinarea și medierea. Prima crește costurile implementării politicilor fără a le modifica conținutul, cea de-a doua reprezintă dezbinarea comunităților și subminarea acțiunilor colective, iar prin mediere, grupurile delincvente se poziționează ca intermediari necesari între instituțiile statului și comunități, consolidându-le atât puterea teritorială, cât și legitimitatea politică.

Abilitatea structurilor de crimă organizată de a înlocui funcțiile statului a fost teoretizată prin conceptul de „guvernare paralelă". Cubides-Cardenas *et al.* (2025) identifică modul în care crima organizată transfrontalieră din Occident funcționează ca o formă de guvernare paralelă, îndeplinind funcții sociale, economice și coercitive alocate în mod tradițional statului și adăugă astfel o nouă dimensiune conceptului weberian al statului care deține monopolul asupra violenței legitime. În regiunile cu instituții slabe, rețelele criminale pot căuta în mod activ legitimitate politică prin înlocuirea serviciilor statale absente, o dinamică de natură să complice răspunsurile forțelor de ordine prin faptul că infractorii devin protejați de către comunitate. Schonenberg și Heinrich-Boll-Stiftung (2013) încadrează guvernarea paralelă drept o amenințare directă la adresa procesului decizional democratic la scară globală. Puterea financiară acumulată prin economiile criminale le conferă infractorilor capacitatea de a exercita o influență directă asupra sistemelor politice, a proceselor de reglementare și a rezultatelor electorale.

Activitatea de spălare de bani merită o atenție specială, fiind mecanismul prin care veniturile provenite din activitățile ilicite sunt integrate în economiile legale, amplificând efectele economice și politice menționate mai sus. Schonenberg și Heinrich-Boll-Stiftung (2013) estimează că între 2 și 5 la sută din PIB-ul global, aproximativ 1,3 până la 3 trilioane de dolari anual, este spălat prin sistemul financiar internațional. Acest proces denaturează prețurile activelor, corupe instituțiile financiare și creează avantaje pentru întreprinderile criminale care concurează cu întreprinderile legitime. Rider (1993) a susținut că activitatea de spălare de bani nu este doar o consecință a crimei organizate, ci un element constitutiv al modelului său operațional, permițând reinvestirea, diversificarea și expansiunea geografică caracteristică întreprinderilor criminale mature.

CRIMA ORGANIZATĂ DIGITALĂ – TIPOLOGII ȘI EFECTE GLOBALE

Definită în sens larg, criminalitatea cibernetică include activitatea ilegală și infracțională desfășurată prin intermediul computerului și al tehnologiei informației. Aceasta cuprinde o gamă largă de activități ilegale, precum hărțuirea cibernetică (cyberbullying), terorismul cibernetic, furtul de identitate, urmărirea cibernetică (cyberstalking), pornografia virtuală (prin internet), spionajul cibernetic (obținerea ilegală de date confidențiale), pirateria informatică (hacking), frauda informatică, hărțuirea online, *phishing*-ul, pirateria online, procedeele de șantaj, extorcarea cibernetică, atacurile de tip spam, încălcarea drepturilor de autor, programele de tip virus informatic (instalarea de programe software malițioase, precum virușii de tip cal troian) (Antonescu și Birău, 2015).

Prin folosirea tehnologiei informației, crima organizată se digitalizează și astfel se transformă calitativ și cantitativ. Di Nicola (2022) oferă o analiză amplă a acestei transformări și susține că societatea digitală a permis coexistența diverselor grupuri infracționale, de la organizații de criminalitate cibernetică pur online la grupuri tradiționale *offline* și până la formațiuni hibride, în care oamenii și mașinile colaborează sub forma unor rețele de actori umani și non-umani. Di Nicola (2022) propune trei categorii de activități ale crimei organizate în societatea digitală: infracțiunile dependente de mediul cibernetic, care nu ar putea exista fără tehnologia digitală (*hacking, ransomware, malware*), activitățile ilicite facilitate de mediul cibernetic (care sunt de fapt activități criminale tradiționale, eficientizate cu ajutorul instrumentelor digitale) și transgresiunile influențate de mediul cibernetic, în care tehnologia digitală modelează structura organizațională și relațiile externe ale grupurilor implicate în principal în activități criminale *offline*.

„Teoria spectrului crimelor organizate digitale" propusă de Di Nicola (2022) situează aceste categorii de-a lungul unui continuum, în loc să le trateze ca tipuri distincte. Această teorie încearcă să reflecte cât mai mult realitatea organizațiilor criminale contemporane în care majoritatea asocierilor ilegale ocupă poziții intermediare și hibride. Operaționalizarea acesteia a fost realizată de Di Nicola *et al.* (2025) prin Cadrul de crimă organizată fizică-digitală (Physical–Digital Organized Crime Framework), care aplică o grilă de 15 elemente constitutive asupra cazurilor empirice, printre care: colaborarea în grup, continuitatea, orientarea spre profit, ierarhia, violența, corupția și ambiția pentru monopol asupra piețelor ilegale. Astfel, în urma analizei a 71 de cazuri judiciare din baza de date SHERLOC a UNODC, care combină criminalitatea cibernetică cu participarea la un grup criminal organizat, Di Nicola *et al.* (2025) au constatat că grupurile de criminalitate cibernetică manifestă în mod constant colaborare, continuitate, orientare spre profit, spirit antreprenorial și organizare în rețea. În același timp, aceste grupuri rareori manifestă violență, corupție sau ambiții monopoliste, un profil care contestă definițiile clasice ale crimei organizate și confirmă necesitatea unui cadru teoretic adaptat.

Tipologia lui Choo (2008) distinge trei categorii de grupuri infracționale care exploatează tehnologia informației. Astfel, primul tip ar fi cel din sfera crimei organizate tradiționale, care utilizează tehnologia pentru a-și intensifica activitățile criminale din mediul fizic, cel de-al doilea se referă la grupurile infracționale care operează exclusiv online, iar ultima categorie cuprinde grupurile motivate ideologic sau politic care utilizează TIC pentru facilitarea activităților ilegale.

Lavorgna (2015), după studiul a 120 de cazuri judiciare și a realizării a 31 de interviuri cu experți din patru țări, a constatat că grupurile criminale organizate tradiționale mai degrabă exploatează internetul ca facilitator al activităților pe care le desfășoară deja *offline*, precum traficul internațional, spălarea de bani și operațiunile financiare frauduloase, decât să se transforme în organizații de criminalitate cibernetică propriu-zise. Leukfeldt *et al.* (2019) au confirmat această constatare prin intermediul *Dutch Organised Crime Monitor*. Aceștia au demonstrat că rețelele mafiote din era digitală cuprind de obicei un amestec de infractori tradiționali și un număr limitat de membri cu competențe tehnice. De asemenea, au observat că se păstrează dimensiunea locală a activităților ilegale digitale, vânzătorii olandezi de droguri online deservind în principal piețele naționale și vecine, în ciuda acoperirii globale a infrastructurii lor digitale.

Întrebarea dacă grupurile care comit activități ilegale prin intermediul noilor tehnologii cibernetice sunt organizații criminale în sensul academic a generat o dezbatere susținută. Lusthaus (2013) a încercat să aplice unele criterii de definire grupurilor de pe forumurile online cunoscute pentru tranzacții ilicite și a constatat că, deși unele grupuri adoptă terminologia mafiei (i.e., ranguri precum „Capo", preluate de la Cosa Nostra), aplicarea definițiilor formale ale crimei organizate trebuie făcută cu precauție. Whelan *et al.* (2024) continuă această dezbatere, argumentând că anumite grupuri de *ransomware* îndeplinesc criteriile pentru crima organizată dacă se adoptă un cadru flexibil care reconceptualizează violența pentru domeniile digitale. În contextul digital, violența se manifestă nu ca o coerciție fizică, ci ca o amenințare cu distrugerea datelor, cu perturbarea operațională și cu afectarea reputației, în timp ce controlul teritorial se exercită mai degrabă asupra infrastructurii digitale, decât asupra spațiului geografic.

Tehnologia utilizată de actorii criminalității cibernetice este din ce în ce mai sofisticată. Tung (2021) a observat că diverse platforme de comunicare criptate (Sky ECC și EncroChat) au permis rețelelor criminale transfrontaliere să coordoneze traficul de droguri, spălarea de bani și alte operațiuni. *Dark web*-ul a oferit delincvenților o piață care reduce costurile de tranzacție și barierele geografice pentru comerțul ilicit cu droguri, arme, date financiare furate și *malware* (Tung, 2021; Grabosky, 2007).

Parte a acestei tehnologii sofisticate sunt criptomonedele. Acestea au devenit o arteră financiară a crimei organizate digitale ce permite operațiuni de spălare de bani. Acestea sunt folosite pentru pseudoanonimatul tranzacțiilor *blockchain*, accesibilitatea criptomonedelor care asigură confidențialitatea, precum Monero și

Zcash, și reglementarea internațională ambiguă (Albrecht *et al.,* 2019). Procesul de spălare de bani în contextul criptomonedelor reproduce secvența clasică de plasare, stratificare și integrare, dar cu o expunere redusă în fiecare etapă. Plasarea are loc prin schimburi de criptomonede cu controale KYC (*know your customer*) inadecvate, stratificarea exploatează trecerea de la un lanț la altul între mai multe criptomonede și zone geografice, iar integrarea are loc prin conversia în monedă fiduciară prin intermediul unor burse slab reglementate sau prin cheltuieli directe la comercianții cu amănuntul, care acceptă plăți în criptomonede (Albrecht *et al.,* 2019). Garcia Otero și Mendez Diaz (2025) studiază integrarea criptomonedelor în rețelele columbiene de trafic de droguri prin operațiuni precum „White Tulip", în cadrul căreia o rețea de crimă organizată a spălat veniturile din droguri prin achiziționarea de Bitcoin în Spania și a transferat apoi fondurile către portofelele digitale ale membrilor columbieni. Jian *et al.* (2020) a analizat 80 de cazuri de extorcare cibernetică. În urma acestei analize a identificat un cadru cu patru elemente: motiv, organizare, învățare și dezvoltare, execuție, elemente ce stau la baza activității grupurilor de crimă organizată cibernetică.

Inteligența artificială reprezintă cel mai recent instrument cu eficiență crescută exponențial pentru grupările de crimă organizată digitală. Racoveanu (2024) aduce în prim-plan integrarea rapidă a instrumentelor de IA în operațiunile criminale prin modelul „Crime-as-a-Service" identificat de EUROPOL, care permite grupurilor criminale fără expertiză tehnică să realizeze operațiuni ilegale digitale. Manifestările concrete includ tehnologia de clonare a vocii utilizată pentru a impersona un individ în scopul efectuării de transferuri financiare frauduloase, un caz din 2019 implicând un transfer de 220 000 de euro autorizat pe baza unei voci generate de IA, precum și tehnologia video *deepfake* utilizată pentru fraudă de identitate și șantaj. Racoveanu (2024) susține că această competiție dintre crima organizată și forțele de ordine va fi în avantajul celor din urmă dacă aceștia vor accelera integrarea IA în aplicarea legii. Cu toate acestea, autorul nu aduce în discuție riscurile folosirii IA de către instituțiile de forță, riscuri care pot presupune limitarea libertății individuale prin monitorizare extensivă și intensivă.

Dezvoltarea tehnologiilor digitale este însoțită de creșterea atacurilor și infracțiunilor cibernetice (de la un hobby personal, la furtul de carduri de credit, până la *hacking* coordonat de guverne) precum și de terorism (Ioanid *et. al,* 2017). România este afectată direct, la nivel macro (instituțional și în mediul corporativ) dar și micro, la nivelul vieții private a cetățenilor săi. Ca răspuns la aceste amenințări, Autoritatea pentru Digitalizarea României și Universitatea Tehnică din Cluj-Napoca au elaborat Strategia Națională pentru Inteligență Artificială 2024–2027. Strategia stabilește șase direcții de acțiune, educație/competențe IA, infrastructură și date, cercetare-dezvoltare, transfer tehnologic către piață, adoptare sectorială (sănătate, educație, transport, agricultură, apărare etc.) și guvernanță/reglementare. Concret, propune programe universitare noi în IA, acces la infrastructură de calcul, fonduri de cercetare, un catalog al aplicațiilor IA din administrație, aplicații IA

pilot pe sectoare prioritare, dar și o autoritate națională de reglementare și centre de certificare conform *AI Act* (Autoritatea pentru Digitalizarea României și Universitatea Tehnică din Cluj-Napoca, 2024).

Acest document trasează responsabilitățile pentru implementarea unor proiecte, indică surse de finanțare și stabilește termene de realizare. Cu toate acestea, implementarea unor proiecte este deficitară și într-o anumită măsură afectează încrederea în anumite instituții. În demersul pentru digitalizarea instituțiilor, ANAF a fost printre primele care a adoptat IA în procesele sale, însă rezultatele obținute nu au fost cele urmărite. Soluționarea disputelor fiscale de către ANAF cu ajutorul IA a dus la trimiteri la articole de lege inexistente, hotărâri judecătorești care nu există sau practici juridice inventate (Cicovschi, 2026).

Un alt proiect guvernamental, a cărui acoperire în presă a alimentat o imagine nefavorabilă autorităților, este robotul ION, consilierul onorific bazat pe inteligență artificială al premierului din perioada 2021–2023. Scopul acestui robot era să ofere informații de ordin administrativ cetățenilor, fiind conectat la o aplicație care centraliza serviciile publice. Pentru că nu au existat resurse suficiente, acest proiect a fost sistat (Vasilache și Popa, 2024), iar ceea ce a fost prezentat ca un progres tehnologic a ajuns să fie văzut ca o campanie de marketing politic nereușită.

Paralel cu aceste inițiative, DNSC semnalează, printre vulnerabilitățile instituțiilor românești în fața atacurilor cibernetice, lipsa de conștientizare a angajaților și lipsa personalului de specialitate (DNSC, 2025), ceea ce încetinește ritmul de adoptare a tehnologiilor de apărare în fața atacurilor cibernetice.

În acest timp, grupurile infracționale digitale din România se perfecționează constant, atacă cu succes instituții guvernamentale, instituții publice și companii, lansează campanii *deepfake* de înșelăciune prin folosirea imaginii unor personalități guvernamentale sau din showbiz (reclame pe YouTube cu Mugur Isărescu care promovează o aplicație de *trading*, Robert Turcescu care susținea investiții în anumite active etc.). Mai mult, apelurile telefonice de tip *vishing/spoofing* (*voice phishing* sau fraudă prin telefon) devin din ce în ce mai elaborate, prin prezentarea unor detalii menite să creeze impresia de legitimitate (menționarea unor numere de identificare a agentului constatator, legitimația acestuia transmisă pe WhatsApp, apoi preluarea datelor prin intermediul unui apel video) (Profit.ro, 2025).

Cazul României se încadrează în peisajul mai larg al infracțiunilor din mediul digital la nivel european. În 2024, s-au înregistrat peste 26 000 de elemente unice de conținut ilegal raportate pe 125 de platforme online, demonstrând capacitatea rețelelor criminale de a exploata infrastructura digitală în diferite zone, în moduri care pun la încercare cadrele naționale de aplicare a legii (EUROPOL, 2026a). Aceste activități sunt încurajate de o economie de tip „Crime-as-a-Service", în care platformele de *ransomware*, kiturile de *phishing* și piețele de pe *dark web* sunt accesibile comercial, indiferent de sofisticarea tehnică, datele devenind marfa centrală – colectate, tranzacționate și transformate în arme pe piețele ilicite

interconectate (EUROPOL, 2025a). Inteligența artificială funcționează ca un catalizator în cadrul acestui sistem prin faptul că reduce atât capitalul uman, cât și expertiza tehnică necesare pentru desfășurarea operațiunilor la scară largă. EUROPOL observă că instrumentele bazate pe IA permit rețelelor infracționale să vizeze victimele cu o viteză și o precizie sporite. Aceasta se remarcă în proliferarea materialelor generate de IA cu abuz sexual asupra copiilor și a platformelor de tip *ransomware-as-a-service*, precum LockBit, care, la apogeu, a reprezentat aproximativ 30% din totalul atacurilor de tip *ransomware* la nivel global (EUROPOL, 2025b).

CRIMA ORGANIZATĂ ȘI CRIMINALITATEA CIBERNETICĂ ÎN ROMÂNIA – EVOLUȚIE ȘI DATE

În anul 2015, la nivel internațional, fraudele economice au avut cea mai mare pondere din totalul infracțiunilor. Acestea au fost urmate de infracțiunile în domeniul cibernetic, estimate la 32% din totalul infracțiunilor. Referitor la fraudele economice, cele de mită și corupție au avut o pondere de 24%, deși în țările din Europa Centrală și de Est, inclusiv România, mita și corupția au fost considerate predominante (Goschin, 2016, p. 85).

După prăbușirea socialismului, România a cunoscut o creștere a activității infracționale în general și a infracțiunilor economice în special (*ibidem*, p. 80). Criminalitatea economică a luat diverse forme, de la deturnarea de fonduri, mită, la fraudele în achiziții publice și în contabilitate, iar criminalitatea cibernetică a devenit o categorie în ascensiune rapidă, care a depășit majoritatea tipurilor clasice de infracțiuni economice în ultimii ani (idem).

Organizațiile criminale tradiționale din România au devenit transnaționale, supraspecializate și sofisticate, capabile să exploateze avantajele globalizării. Factorii care au favorizat dezvoltarea grupurilor infracționale din România includ extinderea economiei subterane, sărăcia și slăbirea puterii statului în controlul criminalității, cadrul juridic confuz și corupția (*ibidem*, p. 81).

Traiectoria crimei organizate în România își are rădăcinile într-o evoluție istorică mai amplă, care a început imediat după prăbușirea regimului comunist, în 1989. Provocările majore în acea perioadă au venit de la racheții din fosta URSS, de la grupurile arabe ori chineze care au stabilit afaceri ilicite cu întindere națională și anvergură internațională, dar și de la grupările pe care Pitulescu (1996) le desemnează drept „mafia țigănească", despre care autorul susține că și-au delimitat zone de influență la nivel național. Membrii acestor grupări, în special liderii lor, au creat un sistem de relații clientelare cu persoane din mediul politic, al magistraturii și al poliției. Aceste relații s-au întins până la medici și notari, protejând astfel infractorii de rigorile legii (*ibidem*).

Criminalitatea organizată, observă Stan (2018), s-a dezvoltat în medii favorabile, exploatând sărăcia, lipsa educației și a oportunităților economice, condiții întrunite concomitent în perioada instabilă a tranziției.

Cu toate acestea, clasamentul județelor în funcție de rata criminalității, măsurată ca număr total de infracțiuni la 100 000 de locuitori, relevă că cele mai bogate județe au rata criminalității mai mare. Astfel, Județul Ilfov a înregistrat în mod constant cea mai ridicată rată a criminalității între 1990 și 2002, înainte de a ajunge treptat pe poziții inferioare în perioada 2007–2011. În privința Municipiul București, acesta a avut o prezență mai stabilă pe parcursul majorității perioadei, în timp ce alte unități teritoriale, județe precum Hunedoara, Alba, Gorj și Olt au fost, de asemenea, frecvent reprezentate în clusterul cu infracționalitate ridicată (Goschin, 2016, p. 88). La polul opus, cele mai scăzute rate ale criminalității au fost înregistrate în Teleorman, Vâlcea, Sălaj, Bihor și Neamț. Astfel, modelul teritorial general indică o criminalitate mai ridicată în județele mai dezvoltate din punct de vedere economic, deși există excepții în ambele sensuri (*ibidem,* p. 89).

Faza de tranziție postcomunistă (1990–2000) a fost marcată de noi infracțiuni, precum traficul internațional de persoane, de migranți, arme, vehicule și droguri, permise de deschiderea frontierelor și de slăbiciunea instituțională a unui stat care trecea printr-o transformare politică, economică și juridică (Stan, 2018). Raportul SRI din 1996 a documentat prezența organizațiilor criminale pe teritoriul României în perioada tranziției. În raport sunt menționate implicarea ofensivă a structurilor internaționale în colaborare cu formațiunile interlope autohtone aflate în continuă dezvoltare. Raportul a identificat apariția mai multor clanuri mafiote italiene (Sacra Corona Unita, Cosa Nostra, Camorra, N'Drangheta), a mafiei ruse și ucrainene care își extindeau operațiunile ilegale în România, precum și importarea de către lumea interlopă internă a unor modele organizaționale și proceduri specifice activității de tip mafiot, cu structuri care își împărțeau zonele de influență în mai multe orașe (SRI, 1996). Grupurile de tip mafiot au exercitat o presiune puternică asupra administrației locale, încălcând în același timp drepturile și libertățile cetățenilor (SRI, 1996).

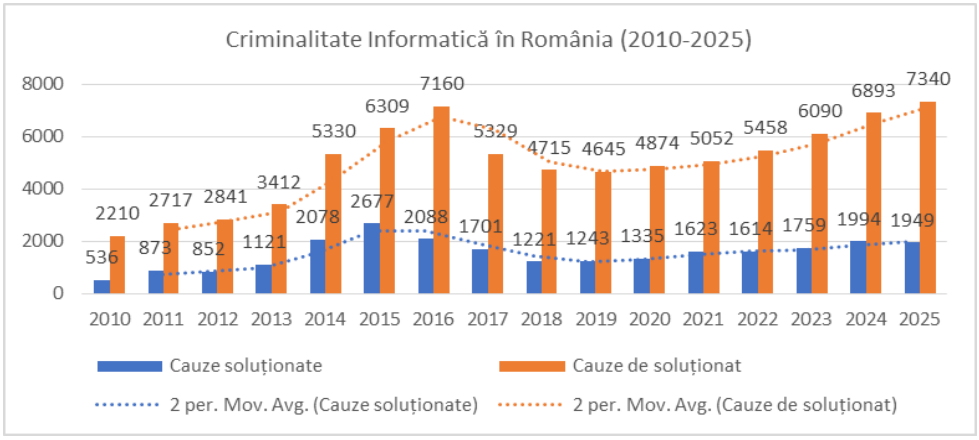
Faza de integrare în UE (2000–2020) a cunoscut o diversificare a rolului României în rețelele criminale internaționale. Țara a rămas o sursă de victime ale traficului de carne vie în Europa de Vest, devenind în același timp o rută de tranzit pentru droguri și imigrație ilegală care se îndreptau spre vest. În aceeași perioadă, România este recunoscută ca un centru pentru frauda online și criminalitatea cibernetică (EUROPOL, 2025; DIICOT, 2025). În prezent, funcția României ca țară de tranzit pentru narcotice a lăsat locul celei de destinație și piață de desfacere pentru consumul de droguri (DIICOT, 2025). Importurile de droguri se efectuează din ce în ce mai mult prin rute comerciale legale, în special prin servicii internaționale de curierat, sau prin intermediari care exploatează mobilitatea ridicată oferită de spațiul Schengen (DIICOT, 2025). DIICOT a raportat confiscări record de droguri în 2025: 3 102 kg în total, o creștere de aproape trei ori față de 1 109 kg în 2024, incluzând 1 090 kg de droguri de mare risc și 2 012 kg de droguri de risc, dintre care 1 969 kg erau canabis (DIICOT, 2025). Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism încadrează aceste tendințe în contextul

reconfigurării pieței europene a drogurilor. Europa de Vest este suprasaturată cu oferta de cocaină, având capturi-record în Belgia și Olanda, în timp ce Europa de Est prezintă o creștere lentă, dar constantă a prevalenței consumului de droguri, tinerii din România, Polonia și Bulgaria fiind din ce în ce mai expuși la substanțe psihoactive (idem). Organizațiile criminale care facilitează consumul de droguri se regăsesc frecvent în zone cu densitate mare a populației, șomaj crescut și nivel de trai scăzut. În aceste regiuni, rețelele familiale se implică în comercializarea substanțelor psihoactive, motivate de lipsa oportunităților socio-economice, ceea ce ilustrează caracterul descentralizat și adaptabil al distribuției narcoticelor (idem).

Referitor la caracteristicile actorilor autohtoni implicați în crima organizată, Neag (2021) identifică specificul grupurilor de infracționalitate românești față de omologii lor regionali. Pe baza unor interviuri cu polițiști și procurori, Neag a constatat că grupurile de crimă organizată din România erau descrise, în general, ca fiind slab organizate, dinamice și relativ ușor de combătut în comparație cu alte formațiuni precum mafiile italiene, bandele albaneze și clanurile rome, care tind să fie organizate pe linii familiale sau comunitare, au relații mai strânse și continuitate îndelungată (*ibidem*, p. 123). Explicația oferită de persoanele intervievate pentru această diferențiere a fost că, datorită trecutului comunist al României și moștenirii poliției secrete represive, forțele de ordine române erau încă foarte puternice, prin aceasta înțelegându-se de obicei autoritare, ceea ce sugerează că grupurilor autohtone de crimă organizată nu li s-a permis să devină ele însele mai puternice (*ibidem*, pp. 123–124).

România este o țară europeană cu rată ridicată a criminalității, iar în contextul integrării europene și al dezvoltării tehnologiilor informației și comunicațiilor, grupările criminale românești s-au extins în noi domenii și s-au alăturat structurilor criminale internaționale (Nicolae, 2017, p. 275). Principala instituție cu mandat legal de a investiga și urmări penal infracțiunile de criminalitate organizată în România este Direcția de Investigare a Criminalității Organizate și a Terorismului (DIICOT), al cărei mandat acoperă, printre altele, traficul de persoane, traficul de droguri, criminalitatea cibernetică, contrafacerea și contrabanda. Statisticile oficiale indică o creștere a urmăririi penale a infracțiunilor cibernetice, numărul dosarelor trimise instanțelor dublându-se în cinci ani, iar numărul total al cazurilor de criminalitate cibernetică înregistrate triplându-se în 2015 (idem).

Peisajul de criminalitate cibernetică din România devine mai clar cu ajutorul datelor DIICOT. Acestea arată o traiectorie ascendentă constantă a numărului de cazuri de infracțiuni cibernetice: de la 536 de cazuri soluționate în 2010, infracțiunile urcă la un vârf de 2 677 în anul 2015 apoi se stabilizează în jurul mediei de 1 650 de cazuri soluționate pe an. În privința cazurilor de soluționat, acestea depășesc 7 000 de dosare în anumiți ani și au o medie anuală, în perioada 2010–2025, de 5 000 de cazuri de soluționat pe an (DIICOT, 2025). Aceste numere plasează criminalitatea cibernetică în mod constant pe locul al doilea ca pondere în categoriile de infracțiuni abordate de DIICOT, după traficul de droguri, care reprezintă 75% din totalul cazurilor în 2024 și 77% în 2025 (idem).



Sursa: DIICOT, 2025

Figura nr. 1. Criminalitatea informatică în România (2010–2025).

Referitor la tipurile de atacuri cibernetice, se remarcă în special o creștere a atacurilor de tip *phishing*, care au vizat practic toate instituțiile bancare din România, cu metode tot mai diverse de colectare a datelor de acces pentru aplicațiile de *internet banking*. Pentru menținerea acestei situații sub control, cooperarea judiciară internațională în domeniul crimei informatice a rămas constantă, cu 297 de cereri în 2024 (181 active și 116 pasive) și 225 de cereri în 2025 (129 active și 96 pasive) (idem).

Domeniul infrastructurii digitale este important pentru înțelegerea atât a expunerii României la crima organizată digitală, cât și a condițiilor care o fac posibilă. Adoptarea tehnologiei digitale în România se numără printre cele mai ridicate din Uniunea Europeană, cu 17,7 milioane de utilizatori de internet, reprezentând 94% din populație, 25,5 milioane de conexiuni mobile, iar viteza medie de internet fix este de 247,12 Mbps, una dintre cele mai ridicate din UE. De asemenea, România ocupă locul 3 în UE pentru conexiuni de peste 1 Gbps (DataReportal, 2026; Comisia Europeană, 2025). Această stabilitate și viteză a infrastructurii creează atât oportunități pentru activități ilicite, cât și provocări de investigare pentru că aceeași conectivitate care permite activitatea economică digitală legitimă oferă și rețelelor criminale o infrastructură operațională cu lățime de bandă mare și latență redusă.

Cele mai recente date indică o creștere a activității de fraudă digitală în România, în concordanță cu tendințele globale indicate de Racoveanu (2024) și EUROPOL (2025). Un raport din 2025 citat de Digi24 a înregistrat o creștere de 180% a fraudei digitale în 2025 comparativ cu 2024, atacurile sofisticate crescând de la 10% la 28% din totalul incidentelor de acest tip. Atacurile de *phishing* au reprezentat 45% din total, fiind urmate de atacurile generate de breșele sistemelor informatice ale companiilor furnizoare de servicii sau produse, care au însumat

36%. Raportul a menționat, de asemenea, apariția documentelor de identitate falsificate cu IA, care reprezintă 2% din totalul actelor false, cu un trend ascendent.

O altă inovație cu potențial infracțional este cea a sistemelor autonome de fraudă, capabile să execute întregul ciclu de fraudă, de la producerea unei identități false, la interacțiunea cu sistemele de verificare și adaptarea comportamentului ca răspuns la măsurile de securitate (Digi24, 2025).

Traficul de droguri, deși nu se desfășoară exclusiv digital, este facilitat de diversele aplicații de comunicare online. DIICOT a identificat Telegram și Signal ca fiind principalele canale de distribuție pentru droguri și substanțe psihoactive noi, cu ambalaje înșelătoare care prezintă produsele ilegale ca fiind aparent legale (DIICOT, 2025).

Schimbul de experiență și preluarea bunelor practici de la colegii din alte țări sunt o prioritate pentru DIICOT și pentru alte instituții avizate, prin aceasta cooperarea internațională a României în domeniul combaterii crimei organizate extinzându-se. DIICOT a menținut 11 parteneriate cu autoritățile judiciare, construite de-a lungul timpului cu omologii din Belgia, Turcia, Țările de Jos, Republica Moldova, Italia, Ucraina, Bulgaria și Albania, cu trei noi acorduri încheiate în 2025 cu Parchetul din Paris, Parchetul Național Antidrog din Spania și PCCOCS din Moldova (idem). În 2025, au fost constituite 27 de echipe comune de anchetă cu autoritățile competente din Germania, Italia, Franța, Spania, Regatul Unit, Belgia, Ungaria, Lituania, Republica Cehă, Elveția, Polonia, Finlanda, Danemarca, Suedia, Ucraina, Slovenia și Republica Moldova (idem). Această dinamică interinstituțională la nivel internațional reflectă importanța poziției geografice a României ca membru cu drepturi depline al spațiului Schengen începând cu 1 ianuarie 2025, cât și expunerea sa la activitatea rețelelor criminale transfrontaliere.

EFECTELE CRIMEI ORGANIZATE ȘI ALE CRIMINALITĂȚII CIBERNETICE ÎN CONTEXTUL ROMÂNESC

Efectele crimei organizate și ale criminalității din sfera digitală, în România, se manifestă pe plan economic, instituțional, social și politic. Economia subterană a României, deși se află pe o traiectorie descendentă, rămâne printre cele mai mari din Uniunea Europeană. Medina și Schneider (2018), precum și Banca Mondială (2010), remarcă un vârf istoric al economiei subterane în 1991, de 36% din PIB. Schneider (2022) extinde această serie, arătând o reducere la 27% în 2019 și o revenire prognozată la aproximativ 29% în 2022, cu mult peste media UE de aproximativ 17% (Schneider, 2022). Principalii factori care determină persistența economiei subterane în România sunt fiscalitatea ridicată, eficiența scăzută a administrației publice, șomajul ridicat, structurile economice bazate pe familie și predominanța tranzacțiilor în numerar (Medina și Schneider, 2018). BTI (2026) confirmă faptul că România are una dintre cele mai scăzute rate de conformare fiscală din Uniunea Europeană, cu o colectare ineficientă a TVA-ului care nu

depășește 30%, și a înregistrat unul dintre cele mai scăzute niveluri de venituri publice din UE în 2024, de doar 34% din PIB, comparativ cu media UE de 46% (BTI, 2026).

Relația de cauzalitate dintre crima organizată și economia subterană din România poate fi privită prin filtrul teoretic propus de Hann (1971). Impozitarea ridicată, aplicarea slabă a legii și neîncrederea instituțională creează stimulente pentru activitatea economică subterană, pe care crima organizată o exploatează și o consolidează.

Efectele instituționale ale activităților grupurilor infracționale în România sunt în mare parte cunoscute, acestea servind drept subiecte intens mediatizate în presă. Cu toate acestea, anchetarea persoanelor politice pentru fapte de corupție, de către Direcția Națională de Anticorupție, a fost limitată din cauza unor încălcări procedurale de către procurorii săi (BTI, 2026). Serviciile de informații sunt suspectate că influențează deciziile politice și judiciare, în timp ce lipsa unei supravegheri eficiente din partea instituțiilor avizate a serviciilor de informații din România slăbește și mai mult separarea puterilor în stat (BTI, 2026). Aceste constatări sunt aliniate cu tipologia relațiilor dintre crimă și stat elaborată de Barnes (2017), unde România prezintă trăsături ale categoriilor „alianță" și „integrare", relații în care organizațiile criminale și reprezentanții statului dezvoltă aranjamente reciproc avantajoase care compromit integritatea instituțională.

În egală măsură, eficiența sistemului judiciar este afectată de instabilitatea legislativă ori legiferarea lacunară, de deficitul cronic de personal al sistemului judiciar și de impredictibilitatea carierei magistraților.

În privința legiferării, din punct de vedere cantitativ, la începutul anului 2025 erau în vigoare un număr de 12 503 de acte normative care fac parte din legislația primară, iar numărul acestora crește cu 500 în fiecare an (Juridice.ro, 2026), fapt ce afectează atât calitatea serviciilor publice, cât și activitatea sistemului judiciar.

Din punct de vedere calitativ, legislația penală a suferit numeroase amendamente impuse prin decizii succesive ale Curții Constituționale a României (CCR) prin care s-au admis excepții de neconstituționale (vezi decizia nr. 51/16.02.2016, nr. 405/15.06.2016, nr. 297/26.04.2018, 358/26.05.2022). Aceste decizii de neconstituționalitate au condus la stingerea acțiunii penale în cauze intens mediatizate și au afectat negativ percepția publică asupra sistemului de justiție (CCR, 2016a; CCR, 2018; CCR, 2022).

Trebuie de asemenea subliniat faptul că la scăderea încrederii în justiție a contribuit și pasivitatea legiuitorului, care nu a pus în acord legislația cu deciziile Curții Constituționale în termenul de 45 de zile prevăzut de art. 28 alin. 3 din Legea 47/1992 privind organizarea și funcționarea Curții Constituționale, fapt ce a generat un vid legislativ în privința unor instituții de drept deosebit de importante (Parlamentul României, 1992).

Or, acest vid legislativ a generat practici neunitare și a întărit percepția publică conform căreia sistemul judiciar nu este independent și imparțial, deciziile

instanțelor fiind influențate de calitatea de persoană publică a anumitor acuzați. La această stare de fapt se adaugă volumul crescut de cazuri atribuite curților de judecată, procurorilor Ministerului Public, DIICOT și instabilitatea din sistemul judecătoresc, care se confruntă cu un val de ieșiri din sistem.

Pătrunderea rețelelor mafiote în structurile politice a fost subiectul unor anchete jurnalistice referitoare la diverse dosare publice. Ancheta în serie a RISE Project a dezvăluit legături între clanul Sportivilor și Primăria Sectorului 4. Jurnaliștii au anchetat modul în care dosarele penale împotriva fondatorilor clanului au fost închise cu decizii de neîncepere a urmăririi penale și modul în care membrii clanului au fost recrutați în forțele de poliție locale după ce s-au înscris oficial într-un partid politic (RISE Project, 2024; Libertatea, 2021). Relația clanului Vasiloi cu autoritățile locale din Sectorul 6 a fost devoalată în urma atribuirii contractelor de remorcare a vehiculelor către firme care aveau legături cu clanul, la schimb cu sprijin electoral pentru politicienii locali (Buletin de București, 2024).

Corupția judiciară a fost consemnată în mass-media prin cazuri concrete, unul dintre acestea fiind cazul judecătorului Dumitru Rebegea, care a primit 20 000 de euro pentru eliberarea lui Sandu Zamfir „Austrianu" (Prompt Media, 2011), ilustrând modul în care puterea financiară a rețelelor criminale erodează independența judiciară. Aceste tipare sunt în concordanță cu afirmația lui Arias (2018) conform căreia organizațiile criminale obțin influență politică prin mediere, poziționându-se ca intermediari necesari între actorii instituționali și comunitățile locale.

Așa cum am menționat anterior, grupurile infracționale din România s-au specializat, folosind tehnologia pentru extinderea activităților criminale în sfera digitală. Poziția paradoxală a României, ca țară cu o infrastructură de internet fix de clasă mondială, cu o viteză medie de 247 Mbps, dar cu implicare deficitară a autorităților, creează condițiile pe care Ering (2011) le-a identificat ca fiind caracteristice economiilor în curs de dezvoltare afectate în mod disproporționat de criminalitatea transfrontalieră. Astfel, infrastructura tehnică modernă se desfășoară fără pârghii eficiente de control instituțional. Folosirea criptomonedelor, menționată de Albrecht *et al.* (2019) și Garcia Otero și Mendez Diaz (2025) în alte contexte naționale, este importantă pentru cazul României, unde combinația dintre conectivitatea digitală ridicată, lacunele de reglementare și infrastructura rețelelor criminale deja consacrate creează condiții optime pentru spălarea de bani prin intermediul acestei tehnologii. Drept urmare, infracțiunile cibernetice adaugă un șoc suplimentar pe lângă vulnerabilitățile deja menționate.

Creșterea fraudei digitale în perioada 2010–2025 (DIICOT 2025, p. 38) a provocat prejudicii economice absorbite de victime, de instituții și de companiile private. Un caz care exemplifică vulnerabilitatea instituțiilor din România și prejudiciile suferite de cetățeni este atacul *ransomware* din anul 2024. Printr-un soft *malware* a fost perturbată activitatea a 26 de spitale de pe tot cuprinsul țării (DNSC, 2024). Surse specializate (Ransomware.live, Hackout.ro) și un birou de presă regional (Sibiu Independent) menționează atacuri cibernetice asupra Poliției

Române în aprilie 2022 și martie 2024, dar aceste știri nu au fost nici confirmate, nici infirmate de instituție ori de cei care monitorizează aceste ingerințe. Evenimentele mai recente (atacul cibernetic asupra ANCPI care a suspendat activitatea instituției pentru mai bine de șapte zile, clonarea website-ului Ghișeul.ro) susțin și mai puternic această imagine de vulnerabilitate a instituțiilor românești.

În mediul privat, Ioanid *et al.* (2017) a constatat că pierderile companiilor mici și medii din România se traduc în ore de muncă suspendate din cauza atacurilor, iar cuantificarea acestor pauze de activitate depinde de momentul în care are loc atacul. Astfel, sumele vehiculate de unii manageri se încadrează în intervalul 1 000 – 10 000 de euro sau depășesc acest interval dacă activitatea este suspendată în perioade aglomerate precum Black Friday, sărbători etc. (*ibidem*, p. 311). Costurile greu de măsurat sunt însă cele provocate reputației companiei, clienții privind cu suspiciune o firmă care a suferit o breșă în securitatea cibernetică, mai ales dacă acea companie lucrează cu date sensibile ale beneficiarului (date personale, bancare) (idem). Un exemplu elocvent pentru această afirmație dar și pentru interconectivitatea efectelor infracțiunilor digitale este cel al Orange România, a cărei bază de date personale a clienților a fost expusă în februarie 2025 (4.5 TB de date au fost compromise, conform atacatorilor). Ca urmare a incidentului, mai multe instituții guvernamentale au fost afectate (primării, școli, spitale, companii de transport etc.) (Moșneag, 2025).

La nivel individual, în afara efectelor suferite în urma blocării accesului la serviciile publice și a breșelor în securizarea datelor personale, infracțiunile digitale, coroborate cu un nivel crescut de educație în domenii tehnice și cu lipsa oportunităților economice, devin perspective de activitate lucrativă. Aceasta datorită câștigurilor financiare mari obținute într-un timp scurt și cu o investiție minimă de capital, câștiguri care pot fi ușor incluse în economia subterană națională și potențial reintroduse în economie legală prin tehnici de spălare de bani (Darius, 2012). Pe acest fir logic, grupurile de criminalitate cibernetică pot fi considerate angajatori pe piața neagră. Recurgerea la astfel de strategii într-un mediu economic slab ofertant provoacă pierderi pentru societate, pentru statul care a investit în educația individului și pentru statutul persoanei care, dintr-un cetățean educat, ajunge în categoria infractorilor.

Un cost potențial, insuficient semnalat, al acestor infracțiuni este scăderea încrederii în tehnologie dar și în instituții, concomitent cu întărirea unor opinii favorabile unui control mai strict prin măsuri autoritare, al căror efect colateral ar fi restrângerea unor libertăți individuale.

Nicolae (2017), Lusthaus și Varese (2017) au studiat unele grupări de crimă organizată cibernetică din România, iar rezultatele acestor cercetări detaliază expansiunea infracțiunilor digitale în România și, în același timp, descriu tipologiile și modurile de operare ale acestor grupări.

Astfel, Nicolae (2017), în urma a 30 de studii de caz (decizii judecătorești definitive) realizate în perioada 2014–2016, care privesc tot atâtea grupuri, identifică tipurile de grupuri infracționale conform taxonomiei lui Choo (2008). Dintre cele 30 de grupuri analizate, două pot fi considerate grupuri tradiționale de criminalitate organizată implicate și în criminalitatea cibernetică, 27 pot fi considerate grupuri de criminalitate cibernetică organizată, iar un caz se referă la un membru al unui grup de hacktiviști (Nicolae, 2017, p. 279). De asemenea, sunt identificate trei tipuri principale de infracțiuni cibernetice și anume furtul de date prin *phishing*, frauda cu carduri prin *skimming* și frauda în domeniul cumpărăturilor online și al licitațiilor (idem). Raportul anual al DNSC identifică *ransomware*-ul drept amenințarea cu cel mai ridicat potențial de impact operațional asupra organizațiilor din România și îl plasează pe primul loc în ierarhia amenințărilor percepute de organizații (DNSC, 2025, pp. 10–11). Cu o incidență între 1% și 7%, acest tip de operațiune are un grad înalt de periculozitate în toate sectoarele instituționale, economice și publice, la nivel global, dar mai ales în România – unde există procese de *backup* inadecvate, o adoptare scăzută a modului de autentificare în doi pași, și un deficit de personal specializat (idem).

Raportat la totalul amenințărilor, ingineria socială sub formă de *phishing* a fost cel mai des raportată (36%) urmată de frauda și tentativa de fraudă (29%) (*ibidem*, p. 7), iar în privința sectoarelor de activitate, atacurile sunt concentrate în sectorul bancar (71%), dar ponderea mare a acestor atacuri se explică și prin maturitatea sistemelor de protecție a instituțiilor financiare, ce le permite să raporteze mai precis ingerințele (*ibidem,* p. 9).

În privința naționalității autorilor, Nicolae (2017) identifică grupuri locale formate exclusiv din români, grupuri străine, formate din persoane de alte naționalități și grupuri mixte. Echipele locale se împart în două subcategorii, cele cu legături locale și mobilitate redusă în lumea reală și grupurile extrem de mobile care acționează în principal în străinătate (*ibidem,* p. 280).

În privința costurilor provocate de aceste grupări, Nicolae (2017) menționează un grup înființat în 2005 la București care a înșelat peste 600 de victime din SUA, Canada, Australia și Europa de Vest, provocând daune dovedite care depășesc 750 000 de dolari, cu operațiuni structurate în jurul unor persoane ce comandă *online* și un nivel de implementare *offline* compus din membri susținuți de angajații mituiți ai Western Union.

Majoritatea grupurilor au structuri interne stabile, cu un nivel de comandă și agenți de nivel inferior mai flexibili, liderii folosind tineri cu competențe în domeniul TIC, majoritatea infractorilor condamnați având vârste cuprinse între 20 și 30 de ani (*ibidem,* p. 288). Conform unui raport EUROPOL (EUROPOL, 2012, p. 3), doar frauda cu plăți prin card generează aproximativ 1,5 miliarde de euro venit anual pentru grupurile de crimă organizată din Uniunea Europeană, iar autoritățile deseori nu reușesc să identifice toate prejudiciile, lăsând o parte din

profituri în mâinile infractorilor chiar și după condamnare, ceea ce constituie un stimulent pentru continuarea activității infracționale după eliberare.

Lusthaus și Varese (2017), în urma unui studiu etnografic în Râmnicu Vâlcea, identifică trei factori care explică rata ridicată a infracțiunilor digitale provocate din acea zonă. Astfel, primul factor ar fi investițiile regimului Ceaușescu în educația de profil real, matematică-informatică, ceea ce a permis românilor să dezvolte competențe solide în domeniul IT. Al doilea factor este de natură economică, România fiind una dintre cele mai sărace țări din Europa, ceea ce încurajează angajarea în activități ilegale. Al treilea factor, complementar acestora, este, conform autorilor, corupția.

Cazul Râmnicu Vâlcea, oraș în care dezindustrializarea a afectat puternic economia locală, prin închiderea angajatorului principal, Oltchim, ilustrează modul în care criminalitatea cibernetică poate deveni un mod de adaptare economică a unei părți din comunitatea locală. Orașul supranumit „Hackerville" a devenit sinonim la nivel internațional cu frauda online, specialitatea sa locală fiind mai degrabă frauda prin licitații decât *hackingul* (*ibidem,* p. 4).

Modul de operare al fraudei este organizat în jurul a două componente interdependente. Aceastea includ gestionarea escrocheriilor online prin intermediul unor echipe care promovează produse fictive și comunică cu victimele, precum și repatrierea fondurilor prin intermediari din străinătate (idem). Activitatea are și o dimensiune *offline*, concentrată geografic, iar corupția a constituit un factor ce a permis continuitatea acestor acte ilicite. Cazul adjunctului șefului poliției locale arestat în decembrie 2014 pentru divulgarea de informații confidențiale către infractori, urmat de un al doilea ofițer arestat sub acuzații similare, sprijină această afirmație. Lusthaus și Varese (2017) susțineau la vremea respectivă că, pe măsură ce criminalitatea cibernetică devine tot mai înrădăcinată la nivel local, potențialul de violență va crește, prin convergența expertizei tehnice și a violenței criminale organizate.

Previziunile cercetătorilor menționați anterior s-au adeverit în mare parte. Infractorii cibernetici au ajuns în punctul în care beneficiază de scalarea industrială a infracțiunilor digitale cu ajutorul tehnologiei care permite transgresiunea legii în spațiul *online* și pentru persoane non-tehnice (DNSC, 2025). Riscurile și costurile devin fără precedent la nivel global, în fața activităților digitale ilegale susținute de anumite state și a compromiterii identității persoanelor. Pagubele provocate de criminalitatea cibernetică ating 10,5 trilioane de dolari, o sumă apropiată de PIB-ul țărilor cele mai dezvoltate economic. La această evoluție contribuie direct utilizarea „inteligenței artificiale ca armă" și indirect factori de ordin economic, care blochează angajarea mai multor specialiști în domeniul securității cibernetice.

La nivel local, anul 2025 a marcat un moment de cotitură pentru securitatea cibernetică din România. Conform DNSC (2025), spațiul cibernetic național s-a confruntat concomitent cu amenințări care continuă să producă efecte la scară largă și cu riscuri emergente ce reduc timpul de reacție al organizațiilor. Deși toate

cele zece sectoare evaluate de DNSC au fost incluse în categoria de nivel de risc mediu, această evaluare statistică maschează diferențe pe un spectru larg, de la sectoare cu apărare solidă în domeniul cibernetic la organizații cu deficite de bază, generalizate.

Impactul cel mai sever îl au, la momentul actual, pe plan internațional dar și local, operațiunile simple, nu cele sofisticate. Ingineria socială, *phishing*-ul, *ransomware*-ul, fraudele cibernetice și compromiterea conturilor reușesc nu prin ingeniozitate, ci prin exploatarea a unor vulnerabilități interne pe care organizațiile nu le-au remediat (idem).

CONCLUZII ȘI RECOMANDĂRI

În acest articol am tratat aspecte de natură conceptuală ale crimei organizate și formele sale de manifestare, de la nivel global cât și local, în special aspectele infracțiunilor cibernetice, având România ca teren de interpretare a conceptelor teoretice. În urma acestui articol se desprind câteva concluzii care stau la baza unor recomandări concrete.

Pe plan teoretic, datele analizate confirmă argumentul central al lui Di Nicola (2022) conform căruia criminalitatea organizată cibernetică constituie un subiect nou al cercetării criminologice, care nu poate fi redus la cadrele tradiționale ale criminalității organizate. Spectrul fizic-digital propus de Di Nicola *et al.* (2025) oferă un cadru analitic adaptat diversității de formațiuni infracționale, de la grupuri de *ransomware* pur online la organizații tradiționale eficientizate digital, fără a impune granițe categoriale artificiale. Reconceptualizarea violenței și a controlului teritorial pentru domeniile digitale, propusă de Whelan *et al.* (2024), aduce o completare necesară a acestui cadru, având în vedere că definițiile clasice ale crimei organizate, ancorate în coerciția fizică și controlul teritorial, omit sofisticarea organizațională a grupurilor de crimă cibernetică.

Efectele crimei organizate sunt mai degrabă sistemice decât episodice și afectează simultan planul economic, politic, instituțional și social. În privința criminalității cibernetice, Anderson *et al.* (2019) enumeră costurile acesteia, dar în același timp subliniază efectele mai greu de cuantificat. Astfel, în Statele Unite și Marea Britanie, infracțiunile cibernetice care provoacă cele mai mari pagube cetățenilor și instituțiilor sunt fraudele prin telefon (7 miliarde $), atacuri de tip *denial-of-service* (1–2 miliarde $), urmate de vânzarea frauduloasă de bilete de avion (un miliard de dolari) și de fraudele online cu carduri de credit (940 milioane $). Pe lângă aceste pagube materiale imense, infracțiunile cibernetice adâncesc neîncrederea în anumite servicii și operațiuni online, provoacă suferință psihologică (în *romance scams* unele pagube materiale sunt mici comparativ cu alte tipuri de fraude cibernetice, dar daunele emoționale sunt disproporționate) frustrări și timp pierdut (*ibidem*, pp. 5, 18, 22). Mai mult, faptul că în unele cazuri poliția nu reușește să prindă infractorii poate contribui la o percepție nefavorabilă asupra

forțelor de ordine și la încurajarea infractorilor care devin din ce în ce mai îndrăzneți (*ibidem,* p. 26).

Activitatea de spălare de bani, mediată în prezent prin piața crypto, reprezintă o nouă vulnerabilitate. Așa cum demonstrează Albrecht *et al.* (2019), caracteristicile criptomonedelor (pseudoanonimatul, transferabilitatea în afara granițelor, fragmentarea reglementării) creează oportunități pentru fluxurile financiare ilegale pe care instituțiile de forță nu sunt momentan pregătite să le gestioneze.

Referitor la vulnerabilitatea României în fața atacurilor cibernetice și la efectele acestora, situațiile recente sunt elocvente. Răspunsul autorităților dar și atitudinea managementului organizațiilor față de infracțiunile cibernetice evidențiază starea de vulnerabilitatea menționată: personalul instituțiilor nu conștientizează gravitatea unor atacuri online, prioritizarea fondurilor este chestionabilă, iar specialiștii în securitate cibernetică sunt subreprezentați în organigrama instituțiilor. Cazul furtului de date de la ANCPI poate servi drept exemplu pentru lipsa de conștientizare din partea personalului instituțiilor a pericolului unui atac cibernetic și a seriozității efectelor acestuia. Managementul financiar al instituției menționate, prin care s-au alocat fonduri în proporție de 0,2% pentru securitate cibernetică, sugerează că „apărarea cibernetică este tratată ca o anexă" (Seceleanu, 2026).

Având la dispoziție toate aceste informații, recomandările pentru o mai bună securizare informatică a cetățenilor și instituțiilor din România țin cont de rolul important pe care țara îl ocupă în contextul geopolitic actual și de perspectivele evoluției tehnologiei digitale, care va fi tot mai prezentă în majoritatea domeniilor vieții sociale și private.

O primă recomandare pentru consolidarea sistemului de apărare împotriva grupărilor de crimă organizată se referă la extinderea cooperării judiciare internaționale a României, cooperare care în prezent este un punct forte, dar care trebuie accentuată mai ales în contextul conflictului din Ucraina și al perspectivelor post război, dar și în cazul aderării la spațiul Schengen, eveniment care aduce noi provocări.

O altă recomandare este dezvoltarea de instrumente bazate pe inteligența artificială pentru combaterea infracțiunii cibernetice, inclusiv detectarea automată a clonării vocii și a fraudei bazate pe *deepfake*, înainte ca decalajul tehnologic dintre actorii criminali și cei instituționali să se adâncească și mai mult.

În ceea ce privește criptomonedele, reglementarea ar trebui armonizată la nivelul UE cu cerințe privind tehnologia de identificare și monitorizarea tranzacțiilor pentru toate platformele de schimb care operează în jurisdicțiile statelor membre, ceea ce ar elimina lacunele exploatate în prezent de rețelele de spălare de bani.

O altă recomandare se referă la includerea în studiul TIC (gimnaziu și liceu) a tipurilor de infracțiuni cibernetice și a modurilor de prevenire a acestora. O astfel de abordare va pregăti tinerii să fie mai abili în fața provocărilor viitorului mai ales pentru că noile tehnologii IoT (Internet of Things) vor fi pseudo-ubicue, ceea ce presupune un risc generalizat de intervenții malițioase.

În cele din urmă, în concordanță cu avertismentul lui Felbab-Brown (2017) împotriva strategiilor de suprimare contraproductive, politicile din România ar trebui să completeze aplicarea legii cu intervenții care să se adreseze vulnerabilităților socio-economice precum șomajul, neîncrederea instituțională și deficitele instituționale, acestea reprezentând o parte din factorii care creează condițiile propice pentru asocierea în activități infracționale.

BIBLIOGRAFIE

1. Albrecht, C., Albrecht, C., Duffin, M., și Hawkins, S. (2019). *The use of cryptocurrencies in the money laundering process*. The Journal of Money Laundering Control, 22(2), 210–216.
2. Anderson, R., Barton, C., Bohme, R., Clayton, R., Ganan, C., Grasso, T., Levi, M., Moore, T., și Vasek, M. (2019). *Measuring the changing cost of cybercrime*. WEIS 2019. *https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_25.pdf*.
3. Antonescu, M., și Birău, R. (2015). *Financial and non-financial implications of cybercrimes in emerging countries*. Procedia Economics and Finance, 32, 618–621.
4. Arias, E.D. (2018). *Criminal organizations and the policymaking process. Global Crime*, 19(3–4), 339–361. *https://doi.org/10.1080/17440572.2018.1471990*.
5. Autoritatea pentru Digitalizarea României și Universitatea Tehnică din Cluj-Napoca. (2024). *Strategia națională în domeniul inteligenței artificiale 2024–2027*. Secretariatul General al Guvernului. *https://sgg.gov.ro/1/wp-content/uploads/2024/07/ANEXA-1-10.pdf*.
6. Banca Mondială. (2010). *Shadow economies all over the world: New estimates for 162 countries from 1999 to 2007* (Policy Research Working Paper 5356). h*ttps://documents1.worldbank.org/curated/en/311991468037132740/pdf/WPS5356.pdf*.
7. Barnes, N. (2017). *Criminal politics: An integrated approach to the study of organized crime, politics, și violence*. Perspectives on Politics, 15(4), 967–987. https://doi.org/10.1017/S1537592717002110
8. Bertelsmann Transformation Index. (2026). *BTI 2026 Romania Country Report*. *https://bti-project.org/en/reports/country-report/ROU*.
9. Buletin de București. (2024). *Percheziții DNA la un dezvoltator imobiliar din clanul Vasiloi din București*. *https://buletin.de/bucuresti/perchezitii-dna-la-un-dezvoltator-imobiliar-din-clanul-vasiloi-din-bucuresti/*.
10. Choo, K.-K.R. (2008). *Organised crime groups in cyberspace: A typology*. Trends in Organized Crime, 11(3), 270–295.
11. Cicovschi, A. (2026). *„Halucinațiile" AI la ANAF. Fiscul motivează respingerea contestațiilor cu articole de lege inexistente, generate de Inteligența Artificială*. Adevărul.
12. Comisia Europeană. (2025). *Digital Decade Romania 2025*. *https://digital-strategy.ec.europa.eu/ro/factpages/romania-2025-digital-decade-country-report*.
13. Costa, A.M. (2010). *The economics of crime: A discipline to be invented and a Nobel Prize to be awarded*. Journal of Policy Modeling, 32, 648–660.
14. Cubides-Cardenas, J., Hernández-Alvarado, C.E., Jimenez-Reina, J., și Roncancio-Bedoya, A.F. (2025). *Regional cooperation against transnational organized crime: Challenges and opportunities in the Western Hemisphere*. Frontiers in Political Science, 7, 1657969.
15. Curtea Constituțională a României. (2016a). *Decizia nr. 51 din 16 februarie 2016*. *https://www.ccr.ro/wp-content/uploads/2020/07/Decizie_51_2016.pdf*.
16. Curtea Constituțională a României. (2018). *Decizia nr. 297 din 2018*. *https://www.ccr.ro/wp-content/uploads/2020/07/Decizie_297_2018.pdf*.
17. Curtea Constituțională a României. (2022). *Decizia nr. 358 din 2022*. *https://www.ccr.ro/wp-content/uploads/2022/06/Decizie_358_2022.pdf*.

18. Darius, I. (2012). *Cybercrime – Part of the underground economy in Romania*. Ovidius University Annals, Economic Sciences Series, XII(1), 532–536.
19. DataReportal. (2026). *Digital 2025: Romania*. *https://datareportal.com/reports/digital-2025-romania*.
20. Di Nicola, A. (2022). *Towards digital organized crime and digital sociology of organized crime*. Trends in Organized Crime, 25, 1–20.
21. Di Nicola, A., Baratto, G., și Martini, E. (2025). *Defining digital organized crime: Applying criminological definitions to cybercrime groups*. Trends in Organized Crime.
22. Digi24. (2020). *Harta clanurilor interlope din București*. *https://www.digi24.ro/stiri/actualitate/evenimente/harta-clanurilor-interlope-din-bucuresti-cine-controleaza-lumea-subterana-din-bucuresti-si-cum-sunt-impartite-teritoriile-1349470*.
23. Digi24. (2025). *Explozie de fraude digitale în 2025*. *https://www.digi24.ro/digieconomic/digital/explozie-de-fraude-digitale-in-2025-atacurile-avansate-cresc-cu-180-pe-fondul-utilizarii-ai-76733*.
24. DIICOT. (2026). *Raport de activitate 2025*.
25. Directoratul Național de Securitate Cibernetică. (2025). *Raport anual de activitate 2024*.
26. DNSC. (2024). *Alertă: Backmydata ransomware – indicatori de compromitere (IOCs)*. https://www.dnsc.ro/citeste/alert-backmydata-ransomware-spitale-romania
27. DNSC. (2025). *Buletin de indicatori, statistici și tendințe de securitate cibernetică – Semestrul 1*.
28. DNSC. (2025). *Raport anual privind evaluarea riscurilor cibernetice ale spațiului cibernetic național civil*.
29. Ering, S.O. (2011). *Trans-border crime and its socio-economic impact on developing economies*. Journal of Sociology and Social Anthropology, 2(2), 73–80.
30. Europa FM. (2025). *Peste trei tone de droguri capturate în 2025*. *https://www.europafm.ro/peste-trei-tone-de-droguri-au-fost-capturate-in-2025-de-diicot-stupefiantele-provin-mai-ales-din-europa-de-vest/*.
31. EUROPOL. (2012). *Situation report: Payment card fraud in the European Union*. https://www.europol.europa.eu/publications-events/publications/situation-report-payment-card-fraud-in-european-union
32. EUROPOL. (2025). *Organised crime online: How EUROPOL disrupts cybercrime*. Publications Office of the European Union. *https://doi.org/10.2813/1796618*.
33. EUROPOL. (2025b). *How crime is accelerated by AI* (Podcast transcript). https://www.europol.europa.eu/podcast
34. EUROPOL. (2026a). *2024 EU Internet Referral Unit transparency report*. *https://doi.org/10.2813/9178956*.
35. Federal Bureau of Investigation. (2020). *Romanian hackers sentenced: Members of Bayrob criminal enterprise infected thousands of computers with malware, stole millions of dollars*. *https://www.fbi.gov/news/stories/members-of-bayrob-romanian-hacking-group-sentenced-022020*.
36. Felbab-Brown, V. (2017). *Organized crime, illicit economies, civil violence și international order: More complex than you think*. Dædalus, 146(4), 98–111.
37. García Otero, R., și Méndez Díaz, R. (2025). *Crypto crime: Approaches from transnational crime and money laundering in Colombia*. Procedia Computer Science, 257, 1166–1171.
38. Goschin, Z. (2016). *Mapping global and economic crime in Romania: Regional trends and patterns*. Romanian Journal of Sociology, 2, 80–96.
39. Grabosky, P. (2007). *The internet, technology, and organized crime*. Asian Criminology, 2, 145–161.
40. Hann, R.G. (1971). *Crime and the cost of crime: An economic approach*. Centre of Criminology, University of Toronto.
41. Hobbs, D. (1998). *Going down the glocal: The local context of organised crime*. The Howard Journal of Criminal Justice, 37(4), 407–422.
42. Ioanid, A., Scarlat, C., și Militaru, G. (2017). *The effect of cybercrime on Romanian SMEs in the context of Wannacry ransomware attacks*. Academic Conferences International.

43. Jian, J., Chen, S., Luo, X., Lee, T., și Yu, X. (2020). *Organized cyber-racketeering: Exploring the role of internet technology in organized cybercrime syndicates*. IEEE Transactions on Engineering Management. *https://doi.org/10.1109/TEM.2020.3003838*.
44. Juridice.ro. (2025). *Raport privind activitatea DIICOT în anul 2025*. *https://www.juridice.ro/816469/raport-privind-activitatea-diicot-in-anul-2025.html*.
45. Lavorgna, A. (2015). *Organised crime goes online: Realities and challenges*. Journal of Money Laundering Control, 18(2), 153–168.
46. Leukfeldt, E.R., Kleemans, E.R., Kruisbergen, E.W., și Roks, R.A. (2019). *Criminal networks in a digitised world: On the nexus of borderless opportunities and local embeddedness*. Trends in Organized Crime, 22, 324–345.
47. Libertatea. (2021). *Interlopii care controlează Sectorul 4 au devenit polițiști locali după ce s-au înscris în PSD*. *https://ziaristii.com/marea-fuziune-interlopii-care-controleaza-sectorul-4-au-devenit-politisti-locali-dupa-ce-s-au-inscris-psd-si-au-jurat-credinta-partidului/*.
48. Lusthaus, J. (2013). *How organised is organised cybercrime?* Global Crime, 14(1), 52–60.
49. Maltz, M.D. (1976). *On defining "organized crime": The development of a definition and a typology*. Crime & Delinquency, 338–346.
50. Medina, L. și Schneider, F. (2018). *Shadow economies around the world* (IMF Working Paper WP/18/17). *https://www.imf.org/-/media/files/publications/wp/2018/wp1817.pdf*.
51. Mocetti, S. și Rizzica, L. (2024). *Organized crime in Italy: An economic analysis*. Italian Economic Journal, 10, 1339–1360.
52. Moșneag, I. (2025). *Orange România, ținta unui nou atac cibernetic? Hackerii susțin că au informații „foarte detaliate" și amenință că vor publica 1TB date*. Mediafax.
53. Neag, A. (2021). *The socio-legal construction of organised crime in Romania* (Teză de doctorat). University of Essex.
54. Nicolae, R. (2017). *Organised crime and cybercrime in Romania*. In Van Duyne *et al.* (Eds.), *The many faces of crime for profit and ways of tackling it* (pp. 274–290). Wolf Legal Publishers.
55. Parlamentul României. (1992). *Legea nr. 47/1992 privind organizarea și funcționarea Curții Constituționale*. https://www.ccr.ro/baza-legala/legea-nr-47-1992/
56. Pitulescu, I. (1996). *Al 3-lea Război Mondial. Crima organizată*. Editura Național.
57. Popescu, G. H., Davidescu, A. A., și Huidumac, C. (2018). *Researching the main causes of the Romanian shadow economy at the micro and macro levels: Implications for sustainable development*. Sustainability, 10(10). *https://www.mdpi.com/2071-1050/10/10/3518*.
58. Prompt Media. (2011). *Clanurile interlope, de la influență locală la fenomen care atentează la siguranța națională*. *https://www.promptmedia.ro/2011/10/clanurile-interlope-de-la-influenta-locala-la-fenomen-care-atenteaza-la-siguranta-nationala/*.
59. Profit.ro. (2025). *Fraudele spoofing în România – Cum arată o conversație în care se încearcă să ni se ia banii*.
60. Racoveanu, C. (2024). *Artificial intelligence – a double-edged sword: Organized crime's AI vs law enforcement's AI*. Sciendo, 507–517. *https://doi.org/10.2478/picbe-2024-0044*.
61. Realitatea de Tulcea. (2022). *Lupta clanurilor interlope pentru administrația locală din Sectorul 6*. *https://realitateadetulcea.net/lupta-clanurilor-interlope-prietene-cu-hubert-thuma-pentru-administratia-locala-ce-jocuri-fac-in-sectorul-6/*.
62. Revista Juridice. (2026, mai 23). *Inflație legislativă: 12.500 acte normative în vigoare*. *https://www.juridice.ro/766938/inflatie-legislativa-12-500-acte-normative-in-vigoare.html*.
63. Rider, B.A.K. (1993). *The financial world at risk: The dangers of organized crime, money laundering and corruption*. Managerial Auditing Journal, 8(7), 3–14.
64. Rise Project. (2024). *Clanul din Sectorul 4*. *https://www.riseproject.ro/projects/clanul-din-sectorul-4/*.
65. Rise Project și Radio Europa Liberă. (2021). *Biblia interlopilor*. *https://romania.europalibera.org/a/regulile-clanurilor-mafiote/31506950.html*.

66. Schneider, F. (2022). *New COVID-related results for estimating the shadow economy in the global economy in 2021 and 2022*. International Economics and Economic Policy, 19, 299–313.
67. Schönenberg, R. și Heinrich-Böll-Stiftung (Eds.). (2013). *Transnational organized crime: Analyses of a global challenge to democracy*. Transcript Verlag.
68. Singh, S.B., Jagganath, G., și Ojolo, T. (2025). *The economics of transnational organised crime: A conceptual analysis of issues and challenges in the 21st century*. In A. Adeniran et al. (Eds.), *The Palgrave handbook of (in)security and transnational crime in Africa* (pp. 1–17). Palgrave Macmillan.
69. Sibiu Independent. (2025, februarie 13). *Dovadă: Atac cibernetic Poliția Română, mii de documente furate*. *https://sibiuindependent.ro/2025/02/13/exclusiv-a-aparut-de-vanzare-baza-de-date-a-politiei-romane-pe-dark-web/*.
70. SRI. (1996). *Raport de activitate 1996*. https://www.sri.ro/assets/files/rapoarte/1996/raport%20activitate%201996.pdf
71. Stan, C. (2018). *Reprezentările criminalității organizate la nivelul comunităților rurale ieșene* (Teză de doctorat). Universitatea „Alexandru Ioan Cuza", Iași.
72. Sullivan, J.P. (2023). *The information age: Transnational organized crime, networks, și illicit markets*. Journal of Strategic Security, 16(1), 51–70.
73. Tung, G. (2021). *Technology as a tool for transnational organized crime: Networking și money laundering*. The Journal of Intelligence, Conflict, and Warfare, 4(1), 118–127.
74. Vasilache, A. și Popa, D. (2024). *Inteligența artificială „ION" a plecat odată cu Ciucă de la Guvern, dar se lucrează la versiunea 2.0: „Va opera ca un funcționar public virtual"*. Hotnews.
75. Whelan, C., Bright, D. și Martin, J. (2024). *Reconceptualising organised (cyber)crime: The case of ransomware*. Journal of Criminology, 57(1), 45–61.
76. Zabyelina, Y. (2023). *Revisiting the concept of organized crime through the disciplinary lens of economic criminology*. Journal of Economic Criminology, 1.
77. Ziare.com. (2011). *Clanurile interlope care și-au împărțit România*. *https://ziare.com/stiri/crima/clanurile-interlope-care-si-au-impart* (ziare.com in Bing)