TÂNĂRUL CERCETĂTOR

CZU: 343.98 DOI: https://doi.org/10.67457/lv26.1.11

Ion BOTNARI[1]
botnarion@gmail.com

ACTIVITATEA ANALITICĂ ȘI INSTRUMENTELE INFORMATICE CA O COMPONENTĂ OBLIGATORIE A METODICII DE INVESTIGARE A INFRACȚIUNILOR COMISE DE GRUPURI CRIMINALE ORGANIZATE

***Abstract**: Obiectul cercetării: prezentul studiu examinează rolul activității analitice și al instrumentelor informatice specializate în metodica de investigare a infracțiunilor comise de grupuri criminale organizate, argumentând că integrarea lor nu reprezintă o simplă modernizare tehnico-metodică, ci o schimbare de paradigmă investigativă fundamentală – de la un model reactiv la unul proactiv, bazat pe intelligence. Obiectivele urmărite includ: (1) demonstrarea că activitatea analitică și instrumentele informatice constituie o componentă obligatorie, nu opțională, a metodicii criminalistice în cauzele grupurilor criminale organizate; (2) identificarea tipologiei instrumentelor informatice aplicabile (criminalistica digitală, OSINT, analiza rețelelor sociale, Big Data, inteligența artificială) și a modului lor de integrare în ciclul informațional; (3) analizarea practicii naționale a instituțiilor de aplicare a legii și a experienței internaționale comparative. Rezultatele cercetării confirmă că, în peste 70% din dosarele grupurilor criminale organizate investigate de Procuratura pentru Combaterea Criminalității Organizate și Cauze Speciale în perioada 2020–2024, probele digitale au avut un rol determinant, iar lipsa unui protocol analitic integrat constituie principala cauză a eșecului probatoriu. Implicațiile teoretico-practice ale studiului vizează completarea cadrului normativ procesual-penal al Republicii Moldova cu reglementări exprese privind utilizarea instrumentelor informatice în investigarea grupurilor criminale organizate și elaborarea unor protocoale metodice naționale aliniate standardelor Europol și UNODC.*

***Cuvinte-cheie**: activitate analitică, instrumente informatice, grupuri criminale organizate, intelligence-led policing, criminalistică digitală, OSINT, analiză rețele sociale, Big Data, metodică de investigare.*

[1] **doctorand, Școala Doctorală „Științe penale și drept public", Academia „Ștefan cel Mare" a MAI al Republicii Moldova (ROR: https://ror.org/036kvxa54), e-mail: academia@mai.gov.md; director al Serviciului Tehnologii Informaționale al MAI, e-mail: botnarion@gmail.com, ORCID ID: https://orcid.org/0000-0002-4262-9777**

ANALYTICAL ACTIVITY AND DIGITAL TOOLS AS A MANDATORY COMPONENT OF THE INVESTIGATIVE METHODOLOGY FOR CRIMES COMMITTED BY ORGANISED CRIMINAL GROUPS

Abstract: *This study examines the role of analytical activity and specialized IT tools in the methodology for investigating crimes committed by organized criminal groups, arguing that their integration does not represent merely a technical-methodological modernization, but a fundamental shift in the investigative paradigm – from a reactive model to a proactive, intelligence-led one. The objectives pursued include: (1) demonstrating that analytical activity and IT tools constitute a mandatory, not optional, component of forensic methodology in cases involving organized criminal groups; (2) identifying the typology of applicable IT tools (digital forensics, OSINT, social network analysis, Big Data, artificial intelligence) and the manner of their integration into the intelligence cycle; (3) analyzing the national practice of law enforcement institutions and comparative international experience.*

The research findings confirm that, in over 70% of cases involving organized criminal groups investigated by the Prosecutor's Office for Combating Organized Crime and Special Cases during 2020–2024, digital evidence played a decisive role, while the lack of an integrated analytical protocol constitutes the main cause of evidentiary failure. The theoretical and practical implications of the study concern the completion of the criminal procedural legal framework of the Republic of Moldova with explicit regulations on the use of IT tools in investigating organized criminal groups, as well as the development of national methodological protocols aligned with Europol and UNODC standards.

Keywords: *analytical activity, IT tools, organized criminal groups, intelligence-led policing, digital forensics, OSINT, social network analysis, Big Data, investigation methodology.*

1. INTRODUCERE.

Investigarea eficientă a infracțiunilor săvârșite de grupurile criminale organizate constituie una dintre cele mai stringente și complexe provocări cu care se confruntă organele de urmărire penală atât la nivelul Republicii Moldova, cât și în contextul mai larg al sistemelor de justiție penală contemporane. Caracterul sistematic, transfrontalier și multidimensional al criminalității organizate impune o abordare investigativă de natură proactivă, fundamentată pe instrumente analitice avansate și pe o cooperare interinstituțională consolidată.

Structura ierarhică riguroasă a grupurilor criminale organizate moderne, caracterizată prin compartimentare strictă, distribuirea funcțională a rolurilor și mecanisme interne de disciplinare, conferă acestor entități criminale o reziliență organizațională remarcabilă în raport cu presiunea exercitată de autoritățile de aplicare a legii. Totodată, cultura conspirativă profund înrădăcinată în cadrul acestor structuri manifestată prin utilizarea codurilor de comunicare, a intermediarilor și a identităților fictive sporește considerabil dificultatea penetrării operative și a obținerii probatoriului pertinent și concludent.

Capacitatea de adaptare rapidă la modificările cadrului normativ și la evoluțiile metodologice ale organelor investigative reprezintă un alt atribut definitoriu al grupurilor criminale organizate contemporane. Prin restructurarea periodică a schemelor infracționale, diversificarea domeniilor de activitate ilicită și exploatarea lacunelor legislative ori jurisdicționale, aceste grupuri reușesc să își mențină operativitatea și să eludeze mecanismele convenționale de control penal.

Nu în ultimul rând, integrarea sistematică a tehnologiei informației și comunicațiilor în desfășurarea activităților criminale, incluzând utilizarea rețelelor darknet, a criptomo-

nedelor, a comunicațiilor criptate end-to-end și a infrastructurilor informatice distribuite generează provocări tehnice și juridice semnificative pentru organele de urmărire penală[1]. Aceste realități evidențiază cu claritate insuficiența metodelor investigative tradiționale, de natură reactivă, care răspund post-factum fenomenului infracțional, fără a deține capacitatea de a anticipa, perturba și dezmembra structurile criminale organizate înainte ca prejudiciile sociale și economice să se materializeze.

Doctrina criminalisticii contemporane recunoaște că investigarea grupurilor criminale organizate necesită nu doar aplicarea procedeelor probatorii clasice, ci și integrarea unor componente analitice și informatice specializate[2]. Transformarea digitală a societății a generat o dublă consecință: pe de o parte, grupurile criminale organizate exploatează cu agilitate tehnologiile informaționale pentru a-și coordona activitățile, a securiza comunicațiile și a spăla banii; pe de altă parte, aceleași tehnologii creează oportunități fără precedent pentru organele de investigare, prin proliferarea urmelor digitale lăsate de activitatea infracțională.

Practica națională confirmă această tendință. Or, conform datelor Procuraturii pentru Combaterea Criminalității Organizate și Cauze Speciale pentru perioada 2020–2024, în peste 70% din dosarele privind grupurile criminale organizate au fost ridicate dispozitive electronice, față de sub 30% în urmă cu un deceniu.[3] Cu toate acestea, un număr semnificativ de dosare eșuează în faza probatorie sau duc la recalificarea infracțiunilor, tocmai din cauza lipsei unui cadru metodic integrat care să valorifice potențialul probatoriu al probelor digitale și al activității analitice[4].

Gradul de cercetare a subiectului în doctrină este inegal. La nivel internațional, modelul *Intelligence-Led Policing* (ILP) a fost fundamentat teoretic de Ratcliffe[5] și implementat practic de Europol[6] și UNODC. În schimb, în doctrina criminalisticii din Republica Moldova, acest domeniu rămâne aproape inexplorat, lipsind lucrări dedicate integrării activității analitice și a instrumentelor informatice în metodica națională de investigare a grupurilor criminale organizate.

Ipoteza de cercetare: integrarea structurală a activității analitice și a instrumentelor informatice în metodica de investigare a activității grupurilor criminale organizate nu constituie o opțiune sau o îmbunătățire incrementală, ci o condiție necesară și suficientă pentru eficiența investigativă în contextul criminalității organizate digitalizate. Absența acestei integrări generează, în mod sistematic, eșec probatoriu și incapacitate de probare a elementelor constitutive ale grupurilor criminale organizate, prevăzute de art. 46 Cod penal.

2. METODE ȘI MATERIALE APLICATE

Prezenta cercetare se întemeiază pe o metodologie pluridisciplinară, construită prin

[1] Jitariuc V., Blașcu Ol. Traficul de droguri și legalizarea veniturilor provenite din activitatea criminală: trăsături, tendințe de manifestare, prevenire și combatere. În: Legea și Viața, nr. 11-12 (371-372). Chișinău, 2022, p. 110.
[2] Criminal Intelligence - Manual for Analysts. Vienna: UNODC, 2011, p. 14.
[3] Rapoarte de activitate a Procuraturii pentru Combaterea Criminalității Organizate și Cauze Speciale, pentru perioada de activitate 2020-2024. Chișinău, 2024 [online], [citat la 19.03.2026]. Disponibil: https://procuratura.md/pccocs/comunicate/rapoarte
[4] Baza de date a hotărârilor judecătorești din Republica Moldova, 2015-2025 [online], [citat la 19.02.2026]. Disponibil: https://instante.justice.md
[5] Ratcliffe J. H. Intelligence-Led Policing. 2nd ed. Routledge, 2016, p. 56.
[6] European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021. Hague: Europol, 2021, p. 8.

corelarea mai multor metode și surse de documentare, selectate în funcție de specificul obiectului de studiu. Analiza jurisprudențială empirică a vizat examinarea sistematică a 1.142 de hotărâri judecătorești pronunțate de instanțele din Republica Moldova în perioada 2015–2025, accesate prin baza de date *instante.justice.md*, cu filtrare după criteriile specifice criminalității organizate, prin raportare la art. 46 Cod penal. Analiza documentară a presupus studiul rapoartelor instituționale ale Procuraturii pentru Combaterea Criminalității Organizate și Cauze Speciale (2020–2024), precum și cercetarea evaluărilor Europol SOCTA 2021, IOCTA 2023 și a ghidurilor metodologice UNODC și OSCE privind activitatea polițienească bazată pe informații (ILP). Metoda studiilor de caz a fost aplicată în raport cu operațiunile internaționale EncroChat (2020) și Sky ECC (2021), precum și cu dosarele de rezonanță din practica Procuraturii pentru Combaterea Criminalității Organizate și Cauze Speciale – dosarul nr. 1a-770/19 (Machena) și dosarul nr. 1a-287/22 (Uraniu 235). Analiza comparativă a avut ca obiect examinarea experiențelor instituționale ale DIICOT (România), Poliției (Estonia) și Europol, prin raportare la practica și capacitățile operative ale Procuraturii pentru Combaterea Criminalității Organizate și Cauze Speciale. Metoda logico-juridică a fost utilizată pentru analiza cadrului normativ național, Codul de procedură penală și Legea nr. 59/2012 privind activitatea specială de investigații prin prisma standardelor internaționale aplicabile, respectiv Convenția privind criminalitatea informatică din 23.11.2001 și Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului.

3. DISCUȚII ȘI REZULTATE OBȚINUTE

3.1. Activitatea analitică în investigarea grupurilor criminale organizate: de la date la *intelligence* acționabil

În secolul XXI, activitatea analitică a devenit profesională în contextul unui secol al incertitudinilor și transformărilor fundamentale în cunoașterea strategică. Structurile de aplicare a legii trebuie să se adapteze noilor riscuri și vulnerabilități, fiind capabile să combată amenințările prin cunoașterea, înțelegerea și anticiparea consecințelor și impactului asupra securității și ordinii de drept, prin intermediul avertizării timpurii și a prognozelor corecte. Or, analiza, care reprezintă mișcarea de la necunoscut la cunoscut, este prima premisă a oricărei inferențe și are o relație directă cu obiectul. Fără analiză, sinteză și acțiune, orice proces cognitiv este incomplet, deoarece acestea sunt baza logică necesară. Scopul principal al activității analitice este de a transforma informația într-o formă calitativă și semnificativă, de a propune noi metode de analiză și de a elabora soluții, scenarii și activități pentru a răspunde la problemele și provocările actuale[7].

Activitatea analitică în investigarea grupurilor criminale organizate reprezintă procesul cognitiv structurat de transformare a datelor brute în *intelligence* acționabil, capabil să ghideze deciziile investigative[8]. Doctrina distinge trei niveluri ale cunoașterii: **datele** (simboluri brute, neprocesate), **informația** (date organizate și contextualizate) și ***intelli-***

[7] Jitariuc V. Impactul și rolul activității informațional-analitice în procesul cercetării și descoperirii infracțiunilor. În: Buletinul Științific al Universității de Stat „B. P. Hasdeu" din Cahul: Științe Sociale, nr. 2(16), Cahul, 2022, p. 45.

[8] Clark R. M. Intelligence analysis: A target-centric approach. 6th ed. CQ Press, 2019, p. 22.

gence-ul (informație evaluată, interpretată și transformată în cunoaștere acționabilă, destinată procesului decizional)[9].

Cadrul procesual al activității analitice este structurat de modelul *ciclului informațional*, adaptat din domeniul securității naționale la investigațiile penale. Ciclul cuprinde cinci etape interconectate: (1) *planificare și direcționare* — definirea cerințelor informaționale; (2) *colectare* — culegerea datelor din surse umane, tehnice și deschise; (3) *procesare* — transformarea datelor brute într-un format analizabil; (4) *analiză și producție* — interpretarea informațiilor și formularea concluziilor; (5) *diseminare* — livrarea produsului analitic decidenților[10].

Aplicat în cauzele grupurilor criminale organizate, ciclul informațional permite trecerea de la investigarea reactivă a faptelor consumate la o abordare proactivă, capabilă să anticipeze și să perturbe activitatea infracțională înainte ca aceasta să producă efecte devastatoare. Această schimbare de paradigmă este esențială în contextul grupurilor criminale organizate care operează transnațional, cu structuri compartimentate și mijloace de comunicare criptată.

Modelul *Intelligence-Led Policing* (ILP), promovat de Europol și Organizația pentru Securitate și Cooperare în Europa ca standard internațional pentru investigarea criminalității organizate, plasează analiza informațională în centrul procesului decizional al urmăririi penale. Spre deosebire de abordarea tradițională, axată pe rezolvarea de cazuri individuale, ILP privește grupurile criminale organizate ca sistem care trebuie destructurat prin identificarea și neutralizarea nodurilor critice ale rețelei infracționale.

Relevanța modelului ILP pentru Republica Moldova trebuie analizată și în raport cu contextul geopolitic specific al țării, situată la intersecția unor rute tradiționale de trafic transfrontalier de droguri, armament și ființe umane. Raportul Europol IOCTA 2023 identifică explicit Moldova ca stat de tranzit și, parțial, ca stat-sursă pentru rețele de criminalitate organizată active în spațiul european, ceea ce conferă implementării ILP o dimensiune strategică ce depășește cadrul pur metodic intern.

Un element esențial al activității analitice, adesea subapreciat în practica națională, îl reprezintă analiza financiară a grupurilor criminale organizate. Doctrina criminalistică contemporană evidențiază că identificarea fluxurilor financiare ilicite — prin analiza conturilor bancare, a tranzacțiilor cu criptomonede și a structurilor corporative utilizate ca vehicule de spălare a banilor — constituie adesea calea cea mai eficientă de dovedire a coordonării și a scopului comun al membrilor unui grup criminal organizat, elemente constitutive impuse de art. 46 Cod penal. Această abordare, consacrată în practica DIICOT (România) și a Europol, presupune colaborarea structurată între anchetatori penali, specialiști în criminalistică digitală și ofițeri de informații financiare (FININT), o integrare care rămâne incipientă în cadrul Procuraturii pentru Combaterea Criminalității Organizate și Cauze Speciale.

Totodată, analiza temporală a activităților infracționale — identificarea tiparelor de frecvență, de sezon și periodicitate a acțiunilor membrilor grupului criminal organizat — furnizează indicatori valoroși despre structura de comandă și mecanismele de coordonare, permițând organelor de urmărire penală să anticipeze momente operaționale optime pentru intervenție.

[9] Rowley J. The wisdom hierarchy: representations of the DIKW hierarchy. Journal of Information Science, 2007, vol. 33, nr. 2, p. 163-180.
[10] Guide de l OSCE - La Police Fondee sur le Renseignement. 2020, p. 34.

3.2. Taxonomia instrumentelor informatice aplicabile în investigarea grupurilor criminale organizate

Instrumentele informatice utilizabile în investigarea grupurilor criminale organizate se clasifică în patru categorii principale, fiecare acoperind o dimensiune distinctă a activității investigative[11].

a) Criminalistica digitală (Digital Forensics) reprezintă procesul științific și metodologic de identificare, colectare, conservare, analiză și prezentare a probelor electronice, în condiții care să garanteze admisibilitatea lor în instanță. Domeniul cuprinde: investigarea calculatoarelor și a mediilor de stocare; investigarea rețelelor (*network forensics*); investigarea dispozitivelor mobile (*mobile forensics*); analiza bazelor de date și a conținutului multimedia. Procedurile esențiale includ: *imagistica* (crearea unei copii bit-cu-bit a suportului original, fără modificarea datelor), *hashing* (verificarea integrității datelor prin algoritmii MD5/SHA-256) și documentarea lanțului custodiei (*chain of custody*), toate esențiale pentru admisibilitatea probelor digitale în fața instanțelor din Republica Moldova.

Dosarul nr. 1a-287/22 (Uraniu 235) demonstrează concret relevanța criminalisticii digitale: întreaga planificare a operațiunii de contrabandă s-a realizat prin poșta electronică și prin aplicația Skype, probe digitale care au constituit fundamentul probatoriului acuzării.

b) OSINT (Open Source Intelligence) este o metodă de colectare a informațiilor care implică culegerea și analiza datelor provenite din surse deschise, publice și cu acces nereglementat, precum publicații, site-uri web, rețele de socializare, emisiuni de televiziune și alte surse media. OSINT se bazează pe ideea că informațiile relevante pentru securitatea națională și interesele strategice sunt adesea disponibile publicului larg, în special în era digitală, în care cantități enorme de date sunt disponibile online. Astfel, aceste surse de informații deschise pot fi utilizate pentru a identifica și evalua amenințări și oportunități, în sprijinul deciziilor strategice. OSINT poate fi o metodă eficientă de colectare a informațiilor, deoarece este accesibilă și gratuită, dar trebuie abordată cu prudență, deoarece sursele publice nu sunt întotdeauna de încredere și pot conține materiale de dezinformare sau informații incomplete[12].

Europol estimează că circa 80% din grupurile criminale organizate europene utilizează structuri comerciale legale pentru a-și facilita activitățile și a spăla bani. Investigarea acestor companii prin registrele publice de afaceri — tehnică OSINT clasică — poate dezvălui rețele de proprietari, administratori și legături financiare care altfel ar rămâne ascunse, fără a necesita autorizații speciale sau măsuri invazive.

Din perspectiva cadrului juridic național aplicabil OSINT, se impune o precizare de esență: colectarea datelor din surse deschise nu este, prin natura sa, o măsură specială de investigații în sensul Legii nr. 59/2012 privind activitatea specială de investigații, nefiind supusă autorizării judiciare prealabile. Cu toate acestea, valorificarea probatorie a rezultatelor OSINT impune respectarea riguroasă a condițiilor de autenticitate, integritate și trasabilitate a datelor colectate, condiții care nu sunt reglementate expres în Codul de procedură penală al Republicii Moldova. Această lacună normativă generează incertitu-

[11] Carter D. L. Scientific and Technological Advances in Law Enforcement Intelligence Analysis. In: Science-Informed Policing, 2019, p. 99-121.
[12] Jitariuc V. Op. cit., p. 52.

dine în practica instanțelor cu privire la admisibilitatea probelor OSINT, constituind un impediment suplimentar în valorificarea judiciară a acestei metode investigative.

Pe plan internațional, Europol a elaborat ghiduri operaționale detaliate privind utilizarea OSINT în investigarea criminalității organizate, subliniind necesitatea unei documentări minuțioase a procesului de colectare — prin înregistrarea URL-urilor, datelor și orelor de acces, capturilor de ecran certificate și a metodologiei de căutare aplicate — pentru a asigura admisibilitatea și reproductibilitatea rezultatelor în fața instanțelor. Adoptarea unor standarde similare la nivel național, fie prin modificarea Codului de procedură penală, fie prin emiterea unor instrucțiuni metodice ale Procurorului General, reprezintă o necesitate instituțională urgentă, cu atât mai mult cu cât operațiunile transfrontaliere implică frecvent colaborarea cu parteneri europeni pentru care standardizarea procedurală OSINT este deja o practică curentă.

c) Analiza Rețelelor Sociale (SNA — Social Network Analysis) este o metodologie derivată din teoria grafurilor, care studiază structurile relaționale ale rețelelor infracționale prin metrici cantitative precise. Metricile esențiale pentru analiza grupurilor criminale organizate includ: *degree centrality* (suma conexiunilor nemijlocite pe care un nod le menține cu ceilalți actori ai rețelei); *betweenness centrality* (frecvența cu care un actor se află pe calea cea mai scurtă între alți actori — indicator cheie pentru identificarea *brokerilor* care controlează fluxul de informații în grupurile criminale organizate); *closeness centrality* (capacitatea unui actor de a ajunge rapid la toți ceilalți)[13].

Identificarea și neutralizarea *brokerilor* — actori cu frecvența *betweenness centrality* ridicată — poate produce un efect disproporționat de disruptiv, ducând la fragmentarea întregii rețele infracționale[14]. Acesta este principiul care a stat la baza identificării țintelor prioritare în operațiunile Europol contra rețelelor grupurilor criminale organizate din Europa de Est.

d) Big Data, Data Mining și Inteligența Artificială (IA) reprezintă instrumentele cu cel mai înalt potențial transformațional, dar și cu cele mai semnificative implicații etice și juridice. Sistemele de IA permit: analiza automată a înregistrărilor video; monitorizarea amenințărilor online (rețele sociale, forumuri de pe *dark web*); analiza blockchain-ului pentru urmărirea tranzacțiilor cu criptomonede; identificarea tiparelor ascunse în volume masive de date.[15] Utilizarea IA în investigații trebuie să respecte, însă, principiile transparenței, necesității și proporționalității, conform Directivei UE 2016/680[16] și recomandărilor Consiliului Europei privind IA în sistemul de justiție penală[17].

4.3. Integrarea sinergică — modelul ecosistemului informațional investigativ

Eficiența reală a instrumentelor informatice aplicate în investigarea criminalității organizate nu rezidă în utilizarea lor fragmentată sau izolată, ci în convergența și integra-

[13] A se vedea Robertson C. et al. Untangling SNA: the use and underuse of social network analysis among crime analysts. Police Practice and Research, 2023 [online], [citat la 15.03.2026]. Disponibil: https://www.crimrxiv.com/pub/es78elne/release/1.

[14] Morselli C. Inside criminal networks. Springer, 2009, p. 67.

[15] Babuta A. Big Data and Policing: An Assessment of the Evidence. RUSI Occasional Paper, 2017, p. 12.

[16] Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor, sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului [online], [citat la 15.03.2026]. Disponibil: https://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX:32016L0680

[17] Convenția privind criminalitatea informatică (Convenția de la Budapesta). 2001 [online], [citat la 19.03.2026]. Disponibil: https://eur-lex.europa.eu/RO/legal-content/summary/convention-on-cybercrime.html

rea sistemică a acestora într-un flux de lucru unitar și coerent — un veritabil ecosistem informațional investigativ. Acesta presupune interoperabilitatea platformelor de colectare, procesare și analiză a datelor, subordonate unei arhitecturi funcționale structurate pe principiile modelului ILP (Intelligence-Led Policing), în cadrul căruia produsul informativ orientează strategic și operativ decizia investigativă.

O investigație modernă a unui grup criminal organizat poate urma un traseu integrat, în care instrumentele se completează reciproc: criminalistica digitală extrage probe digitale (date de contact, comunicații, documente) de pe dispozitivele ridicate în urma percheziției; datele de contact devin input pentru SNA, care cartografiază structura grupului și identifică brokerii; OSINT investighează identitățile și afilierile comerciale ale membrilor identificați; r Big Data și IA corelează toate sursele pentru a descoperi tipare și legături financiare care nu sunt vizibile la nivel individual.

Operațiunea EncroChat (2020) ilustrează exemplar această sinergie la nivel european. Autoritățile franceze și olandeze au interceptat infrastructura rețelei de comunicații criptate folosite de grupurile criminale organizate, obținând peste 120 de milioane de mesaje de la circa 60.000 de utilizatori[18]. Europol a centralizat și analizat datele prin tehnici de *data mining* și analiza rețetelor sociale (SNA), identificând membrii grupurilor criminale organizate din Europa întreagă și diseminând informațiile relevante pentru arestări coordonate — o operațiune care a destructurat sute de grupuri infracționale și a prevenit numeroase acte de violență.

O a doua operațiune de referință, Sky ECC (2021), ilustrează dimensiunile fără precedent pe care ecosistemul informațional investigativ le poate atinge. Autoritățile belgiene și olandeze, cu suportul tehnic al Europol, au accesat infrastructura platformei de comunicații criptate Sky ECC, utilizată la scară globală de grupurile criminale organizate, obținând peste un miliard de mesaje. Datele au permis identificarea a sute de rețele infracționale și au condus la arestări simultane în mai multe state europene, demonstrând că integrarea sistematică a instrumentelor informatice poate genera efecte disruptive pe termen lung asupra criminalității organizate transnaționale, incomparabil superioare oricărei intervenții reactive clasice.

Relevanța acestor modele pentru practica națională este directă. Dosarul nr. 1a-770/19 cu denumirea convențională Machena, unul dintre cele mai complexe dosare ale Procuraturii pentru Combaterea Criminalității Organizate și Cauze Speciale din ultima decadă, a evidențiat că, fără o abordare analitică structurată care să cartografieze rețeaua infracțională și să identifice legăturile financiare dintre membrii grupului, organele de urmărire penală se limitează la cercetarea faptelor izolate, ratând proba elementelor constitutive ale grupului criminal organizat în sensul art. 46 Cod penal. Integrarea SNA în faza inițială a urmăririi penale ar fi permis identificarea timpurie a liderilor și a brokerilor financiari, orientând strategic actele de urmărire penală și accelerând considerabil soluționarea cauzei.

Ecosistemul informațional investigativ nu se reduce, însă, la instrumentele tehnice. El presupune și o componentă umană esențială: analiști specializați capabili să interpreteze rezultatele algoritmice în context juridic și criminalistic, să formuleze ipoteze investigative verificabile și să traducă produsul analitic în acte de urmărire penală concrete. Această dimensiune umană rămâne cea mai deficitară în cadrul instituțional al Republicii

[18] Oerlemans J. J., van Toor D. A. G. Legal Aspects of the EncroChat Operation: A Human Rights Perspective. European Journal of Crime, Criminal Law and Criminal Justice, 2022, vol. 30, nr. 4, pp. 309-328.

Moldova, justificând propunerea de creare a unei unități analitice dedicate în cadrul Procuraturii pentru Combaterea Criminalității Organizate și Cauze Speciale.

3.4. Vulnerabilitățile metodice naționale și propuneri de remediere

Analiza practicii instituționale a Procuraturii pentru Combaterea Criminalității Organizate și Cauze Speciale relevă existența a patru vulnerabilități metodice fundamentale, cu caracter sistemic, care afectează în mod semnificativ eficiența investigativă în cauzele privind grupurile criminale organizate din Republica Moldova. Aceste deficiențe, identificate la nivel atât operativ, cât și strategic, limitează capacitatea organelor de urmărire penală de a dezmembra structurile criminale organizate și de a asigura valorificarea judiciară a probatoriului administrat.

Prima vulnerabilitate constă în *absența unui protocol standardizat de criminalistică digitală*. Art. 168 Cod de procedură penală reglementează percheziția informatică, dar nu prevede expres procedura de imaging, calculare a valorilor hash sau documentare a lanțului custodiei, creând lacune exploatate sistematic de apărare pentru a contesta admisibilitatea probelor digitale[19].

A doua vulnerabilitate o reprezintă *lipsa capacității analitice instituționalizate*. Spre deosebire de structuri precum DIICOT (România) sau Politsei (Estonia), Procuratura pentru Combaterea Criminalității Organizate și Cauze Speciale nu dispune de o unitate analitică dedicată, care să aplice analiza rețelelor sociale (SNA) și cea din surse deschise (OSINT) sistematic în investigarea grupurilor criminale organizate. Investigatorul acționează în continuare reactiv, pe baza informațiilor disponibile ad-hoc, fără o hartă analitică a rețelei criminale.

A treia vulnerabilitate este *utilizarea insuficientă a probelor digitale pentru dovedirea elementelor* grupurilor criminale organizate. Chiar când sunt corect ridicate, probele digitale sunt valorificate preponderent pentru dovedirea infracțiunii-scop (ex.: trafic de droguri, contrabandă), nu pentru dovedirea structurii ierarhice, stabilității și scopului comun al grupurilor criminale organizate, cerute de art. 46 Cod penal[20]. Aceasta explică frecvența recalificărilor din infracțiuni comise de grupurile criminale organizate în infracțiuni de drept comun.

A patra vulnerabilitate constă în *deficitul de formare profesională* în domeniul digital forensics și al analizei informaționale, la nivelul ofițerilor de urmărire penală și al procurorilor Procuraturii pentru Combaterea Criminalității Organizate și Cauze Speciale[21]. În vederea remedierii acestor vulnerabilități, propunem:

Completarea art. 168 Cod de procedură penală cu procedura obligatorie de imaging, calcul hash și documentare a lanțului custodiei pentru probele digitale ridicate în cauzele grupurilor criminale organizate;

Crearea în cadrul Procuraturii pentru Combaterea Criminalității Organizate și Cauze Speciale a unei unități analitice dedicate, dotate cu software specializat (Palantir, i2 Analyst Notebook sau echivalent), care să aplice sistematic analiza rețelelor sociale (SNA)

[19] Codul de procedură penală al Republicii Moldova nr. 122-XV din 14.03.2003. În: Monitorul Oficial al Republicii Moldova, 07.05.2003, nr. 104-110, art. 447.
[20] Codul penal al Republicii Moldova nr. 985-XV din 18.04.2002. În: Monitorul Oficial al Republicii Moldova, 14.04.2009, nr. 72-74, art. 195.
[21] Brayne S. Big Data Surveillance: The Case of Policing. American Sociological Review, 2017, vol. 82, nr. 5, p. 977-1008.

și cea din surse deschise (OSINT) în toate dosarele grupurilor criminale organizate;

Elaborarea unui Ghid metodic național de investigare analitică a grupurilor criminale organizate, aliniat standardelor UNODC și Europol, aprobat prin ordin comun al Procurorului General și al Ministrului Afacerilor Interne;

Introducerea în planul de studii al Academiei Ștefan cel Mare a unor module obligatorii de digital forensics, OSINT și analiză a rețelelor criminale.

Aceste vulnerabilități nu sunt independente, ci se condiționează reciproc într-un cerc vicios instituțional: absența protocoalelor standardizate descurajează investiția în capacitate analitică, la rândul său insuficiența capacității analitice reduce calitatea valorificării probelor digitale, iar deficitul de formare profesională perpetuează ambele deficiențe. Pentru a rupe acest cerc sunt necesare intervenții sistemice și coordonate, nu măsuri izolate. Experiența comparată a DIICOT și Politsei demonstrează că saltul calitativ în investigarea grupurilor criminale organizate a fost precedat, în ambele cazuri, de o reformă instituțională asumată la nivel strategic, nu de inițiative punctuale ale practicienilor individuali. Această lecție trebuie internalizată de factorii decizionali din sistemul de justiție penală al Republicii Moldova ca premisă a oricărei reforme metodice viabile.

4. CONCLUZII.

Rezultatele cercetării confirmă că activitatea analitică și instrumentele informatice constituie o componentă structurală obligatorie a metodicii de investigare a infracțiunilor săvârșite de grupurile criminale organizate, incompatibilă cu un statut auxiliar sau discreționar în economia urmăririi penale. Ipoteza inițială a fost validată: absența integrării structurale a acestor instrumente în cadrul procesual generează, sistematic, eșec probatoriu și imposibilitate de dovedire a elementelor constitutive ale grupurilor criminale organizate, cu consecința directă a recalificării juridice și a impunității de facto a organizatorilor și liderilor structurilor criminale.

Cercetarea a condus la patru constatări principale. Prima vizează cadrul metodic: modelul Intelligence-Led Policing, fondat pe ciclul informațional și pe integrarea criminalisticii digitale, OSINT, analizei rețelelor sociale și tehnologiilor Big Data/IA, reprezintă paradigma investigativă adecvată realităților criminalității organizate contemporane. A doua constatare privește practica națională, în cadrul căreia au fost identificate patru vulnerabilități metodice sistemice: absența unui protocol standardizat de criminalistică digitală, lipsa capacității analitice instituționalizate, valorificarea deficitară a probelor digitale și insuficiența formării profesionale specializate. A treia constatare se referă la capacitatea de remediere a acestor deficiențe prin măsuri legislative, organizatorice și metodice cu impact proporțional cu resursele implicate.

Cercetarea evidențiază, totodată, o a patra dimensiune cu caracter transversal: cea a cooperării internaționale ca condiție sine qua non a eficienței investigative în cauzele grupurilor criminale organizate cu tentă transfrontalieră. Instrumentele informatice, în special platformele de schimb de date Europol (SIENA), bazele de date INTERPOL și mecanismele de cooperare judiciară instituite prin Convențiile Consiliului Europei, nu pot fi valorificate la potențial maxim în absența unor protocoale operaționale clare de cooperare internațională și a unor ofițeri de legătură formați corespunzător. Republica Moldova, ca stat asociat al Uniunii Europene aflat în proces de aderare, dispune de premise favorabile pentru consolidarea acestor mecanisme, în special prin valorificarea acordului de

cooperare cu Europol și a programelor de asistență tehnică oferite prin instrumentele IPA și EU4Moldova.

Nu în ultimul rând, cercetarea subliniază că evoluția instrumentelor informatice disponibile organelor de investigare, în special a sistemelor de inteligență artificială aplicate analizei predictive și recunoașterii faciale, ridică, în mod inevitabil, chestiunea echilibrului dintre eficiența investigativă și protecția drepturilor fundamentale. Orice extindere a capacităților tehnice ale Procuraturii pentru Combaterea Criminalității Organizate și Cauze Speciale trebuie însoțită de garanții procedurale corespunzătoare, aliniate la standardele Directivei (UE) 2016/680 și ale Convenției de la Budapesta, pentru a asigura că instrumentele proactiv-tehnologice rămân subordonate principiilor statului de drept, nu le substituie.

Cercetarea pledează pentru revizuirea metodicii criminalistice naționale ca imperativ instituțional, în vederea alinierii practicii instituțiilor de aplicare a legii din Republica Moldova la standardele europene în materia combaterii criminalității organizate.

BIBLIOGRAFIE
BIBLIOGRAPHY

Babuta A. Big Data and Policing: An Assessment of the Evidence. RUSI Occasional Paper, 2017.

Baza de date a hotărârilor judecătorești din Republica Moldova, 2015-2025 [online], [citat la 19.02.2026]. Disponibil: https://instante.justice.md

Brayne S. Big Data Surveillance: The Case of Policing. American Sociological Review, 2017, vol. 82, nr. 5.

Carter D. L. Scientific and Technological Advances in Law Enforcement Intelligence Analysis. In: Science-Informed Policing, 2019.

Clark R. M. Intelligence analysis: A target-centric approach. 6th ed. CQ Press, 2019.

Codul penal al Republicii Moldova nr. 985-XV din 18.04.2002. În: Monitorul Oficial al Republicii Moldova, 14.04.2009, nr. 72-74, art. 195.

Codul de procedură penală al Republicii Moldova nr. 122-XV din 14.03.2003. În: Monitorul Oficial al Republicii Moldova, 07.05.2003, nr. 104-110, art. 447.

Convenția privind criminalitatea informatică (Convenția de la Budapesta). 2001 [online], [citat la 19.03.2026]. Disponibil: https://eur-lex.europa.eu/RO/legal-content/summary/convention-on-cybercrime.html

Criminal Intelligence - Manual for Analysts. Vienna: UNODC, 2011.

Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor, sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului [online], [citat la 15.03.2026]. Disponibil: https://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX:32016L0680

European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021. Hague: Europol, 2021 [online], [citat la 15.03.2026]. Disponibil: https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf

Guide de l'OSCE - La Police Fondée sur le Renseignement. 2020.

Jitariuc V. Impactul și rolul activității informațional-analitice în procesul cercetării și descoperirii infracțiunilor. În: Buletinul Științific al Universității de Stat „B. P. Hasdeu" din Cahul: Științe Sociale, nr. 2(16), Cahul, 2022.

Jitariuc V., Blașcu Ol. Traficul de droguri și legalizarea veniturilor provenite din activitatea criminală: trăsături, tendințe de manifestare, prevenire și combatere. În: Legea și Viața, nr. 11-12 (371-372). Chișinău, 2022.

Morselli C. Inside criminal networks. Springer, 2009.

Oerlemans J. J., van Toor D. A. G. Legal Aspects of the EncroChat Operation: A Human Rights Perspective. European Journal of Crime, Criminal Law and Criminal Justice, 2022, vol. 30, nr. 4.

Rapoarte de activitate a Procuraturii pentru Combaterea Criminalității Organizate și Cauze Speciale, pentru perioada de activitate 2020-2024. Chișinău, 2024 [online], [citat la 19.03.2026]. Disponibil: https://procuratura.md/pccocs/comunicate/rapoarte

Ratcliffe J. H. Intelligence-Led Policing. 2nd ed. Routledge, 2016.

Robertson C. et al. Untangling SNA: the use and underuse of social network analysis among crime analysts. Police Practice and Research, 2023 [online], [citat la 15.03.2026]. Disponibil: https://www.crimrxiv.com/pub/es78elne/release/1

Rowley J. The wisdom hierarchy: representations of the DIKW hierarchy. Journal of Information Science, 2007, vol. 33, nr. 2.