CZU 343.98 **DOI: https://doi.org/10.5281/zenodo.20809368**

THE INTERFERENCE BETWEEN PERSONAL DATA PROTECTION AND THE REQUIREMENTS OF FORENSIC INVESTIGATION IN IDENTITY THEFT CASES INVOLVING ORGANISED CRIMINAL GROUPS

Ion BOTNARI,
PhD Student,
"Ştefan cel Mare" Academy of the Ministry of Internal Affairs,
Republic of Moldova
ORCID: 0000-0002-4262-9777

Evghenia GUGULAN,
PhD, Associate Professor,
Head of Private Law Department,
"Ştefan cel Mare" Academy of the Ministry of Internal Affairs,
Republic of Moldova
ORCID: 0000-0002-5960-1164

Abstract

In the architecture of contemporary digital society, identity theft committed by organized criminal groups takes on the characteristics of sophisticated criminality, placed at the intersection of legal regimes with apparently divergent purposes: personal data protection and the efficiency of forensic investigation.

The present scientific endeavor seeks to explore this area of normative convergence, highlighting the complexity arising from the need to balance fundamental guarantees of private life with the specific demands of criminal investigation and the administration of evidence in criminal proceedings. The analysis is grounded in an integrative approach that coherently combines doctrinal, normative, and jurisprudential benchmarks at both national and European levels, with a view to delineating an applicable legal framework capable of responding to these dynamics.

Particular attention is devoted to the mechanisms of storage, processing, and preservation of personal data within criminalistic activities, as well as to the evidentiary vulnerabilities generated both by the inherently digital nature of such data and by the organized structure of criminal conduct. From a critical perspective, the research underscores the risk of excessive oscillation between the imperatives of data protection and the demands of effective criminal enforcement, while emphasizing the need to articulate a balanced normative and operational model capable of ensuring coherence and proportionality in legal intervention.

Finally, conceptual benchmarks and directions of reflection are advanced, intended to contribute to the configuration of coherent legal and forensic mechanisms capable of simultaneously meeting the requirements of the rule of law and the emerging challenges of organized cybercrime.

Keywords: identity theft, organized criminal groups, forensic investigation, personal data protection, electronic traces, digital evidence.

INTERFERENȚA DINTRE PROTECȚIA DATELOR CU CARACTER PERSONAL ȘI EXIGENȚELE INVESTIGAȚIEI CRIMINALISTICE ÎN CAUZELE DE FURT DE IDENTITATE COMIS DE GRUPURI CRIMINALE ORGANIZATE

Abstract

În arhitectura societății digitale contemporane, furtul de identitate comis de grupuri criminale orga-

nizate dobândește valențele unei infracționalități sofisticate, plasate la intersecția unor regimuri juridice cu finalități aparent divergente: protecția datelor cu caracter personal și eficiența investigației criminalistice.

Prezentul demers științific vizează explorarea acestei zone de convergență normativă, evidențiind complexitatea generată de necesitatea echilibrării garanțiilor fundamentale ale vieții private cu exigențele specifice investigației criminalistice și ale administrării probelor în procesul penal. Analiza se fundamentează pe o abordare integrativă, care îmbină în mod coerent repere doctrinare, normative și jurisprudențiale, atât la nivel național, cât și european, în vederea conturării unui cadru juridic aplicabil, capabil să răspundă acestor dinamici.

O atenție particulară este acordată mecanismelor de stocare, prelucrare și conservare a datelor cu caracter personal în cadrul activității criminalistice, precum și vulnerabilităților de ordin probatoriu generate atât de natura intrinsec digitală a acestor date, cât și de caracterul organizat al activității infracționale. Dintr-o perspectivă critică, cercetarea evidențiază riscul unei oscilații excesive între imperativele protecției datelor și exigențele eficientizării represiunii penale, subliniind, totodată, necesitatea configurării unui model de echilibru normativ și operațional, apt să asigure coerența și proporționalitatea intervenției juridice.

În acest sens, sunt avansate repere conceptuale și direcții de reflecție menite să contribuie la configurarea unor mecanisme juridice și criminalistice coerente, capabile să răspundă simultan exigențelor statului de drept și provocărilor emergente ale criminalității informatice organizate.

Cuvinte-cheie: furt de identitate, grupuri criminale organizate, investigație criminalistică, protecția datelor cu caracter personal, urme electronice, probe digitale.

Introduction. The accelerated digitalization of society, manifested within the sphere of social relations, has necessitated the establishment of an adapted normative framework, materialized through regulations designed to address specific legal and societal exigencies [18, p.35-36]. The alignment of national legislation with the European acquis communautaire [7] led to the adoption of Law No.133 of 8 July 2011 on the Protection of Personal Data [10]. Subsequently, the adaptation of the regulatory framework to the provisions of a European Union regulation General Data Protection Regulation [9] resulted in the replacement of the aforementioned law with a new legislative act — Law No.195 of 25 July 2024 on the Protection of Personal Data [11]. The provisions of Article 84 of the Regulation implicitly suggest the necessity of legally classifying identity theft as a criminal offence.

This necessity also derives implicitly from the provisions of Article 9(5) of Directive 2013/40/EU [8]. In the same vein, recital (14) of the Directive's preamble states, *inter alia*, that "*the implementation of effective measures aimed at combating identity theft [...] constitutes a [...] relevant component of an integrated strategy against cybercrime*" [8].

In light of Government Decision No.1171 of 28 November 2018 approving the Regulation on the Harmonization of National Legislation with the acquis of the European Union Government Decision No.1171 of 28 November 2018 [15], the establishment of criminal-law mechanisms aimed at protecting social values and legal relations against identity theft became imperative. In this regard, through Law No.136 of 6 June 2024 amending certain normative acts Law No.136 of 6 June 2024 [14], the Criminal Code of the Republic of Moldova was supplemented with Article 260^7, thereby introducing the criminalization and sanctioning of this offence.

The adjustment of national legal provisions has produced significant effects upon the nature and dynamics of the criminal mechanisms employed by organized criminal groups (OCGs). Whereas, within the classical model of organized crime, personal identity represented an attribute difficult to falsify, intrinsically linked to physical documents and state registries, it has presently evolved into a complex set of data stored and processed within electronic environments, susceptible to unauthorized access, duplication, and exploitation through sophisticated technological means [1, p. 14].

Technological progress has generated not only new modalities of communication

and information storage, but also new systemic vulnerabilities, systematically and professionally exploited by organized criminal structures. This structural transformation has led to the emergence of a distinct category of criminal conduct — digital identity theft — criminalized under Article 260[7] of the Criminal Code of the Republic of Moldova [5].

One of the most sensitive issues debated in recent years, both at the national and international levels, concerns the protection of personal data [21, p. 77]. In this context, the forensic investigation of identity theft committed within or through organized criminal groups (OCGs) encounters a methodological challenge of particular complexity: criminal investigation bodies are compelled to access, process, and evidentially exploit precisely the category of data that the legal regime governing personal data protection, established by Law No.133/2011 [10], subjects to stringent restrictions [20, p. 103].

This interference does not constitute a mere issue of legal application, but rather reflects a structural tension between two equally legitimate constitutional values: the right to private life, guaranteed by Article 28 of the Constitution of the Republic of Moldova Constitution of the Republic of Moldova and by Article 8 of the European Convention on Human Rights [3], and the right of society to security and to the effective repression of organized criminality. Neither of these values may be sacrificed in favour of the other without undermining the very foundations of the rule of law.

The forensic particularity of identity theft committed within organized criminal groups (OCGs) resides in its instrumental character: *the stolen identity does not represent the ultimate purpose of the criminal activity, but rather serves as a mechanism for concealing group members, gaining access to the financial resources of victims, and disguising illicit financial flows.* This instrumentalization of identity confers upon the offence a distinct evidentiary dimension: the forensic investigator must reconstruct not only the mechanism of identity theft itself, but also the entire chain through which the stolen identity is utilized within the criminal scheme of the OCG.

The analysis conducted by the authors of 1,142 judicial decisions delivered in cases involving an OCG component in the Republic of Moldova during the period 2015-2025 demonstrated that false or stolen identities most frequently appeared in the roles of courier (853 references) and intermediary (175 references) — functions which, by their very nature, create an operational distance between the leader of the OCG and the concrete criminal act, while simultaneously reducing the possibilities of identifying the group's actual command structure.

Moldovan forensic doctrine has not, to date, systematically examined the interference between these two normative regimes within the specific context of organized criminal groups (OCGs) and digital identity theft. The contributions of Gheorghiță M. in the field of forensic methodology [1], as well as the works of Ostavciuc D. and Odagiu Iu. concerning the investigation of organized criminality [2] – provide the general methodological framework, yet they do not address the particularities arising from the collision between the evidentiary demands of digital investigations and the legal regime governing personal data protection.

Studies in the field of special investigative activities — including the work of D. Roman concerning the grounds and conditions for special investigative measures (SIMs) [16] — approach the issue of interference with private life primarily from a procedural perspective, without correlating it with the forensic specificities of digital traces in cases involving OCGs. The present study seeks to fill this doctrinal gap by identifying and conceptualizing this interference as an autonomous methodological problem and by formulating reference points for an operational balancing model adapted to the Moldovan legal context.

The existing normative framework provides investigative instruments, yet it does not establish an integrated methodological architecture. The provisions of Articles 132[1]-132[8] of the Criminal Procedure Code of the Republic of Moldova [6] regulate access to various categories of electronic data, though without expressly distinguishing between the categories of data relevant in cases of digital identity theft — namely, the victim's identity data, the traffic data of OCG members, the content of communications, and the metadata associated with financial transactions.

This absence of methodological differentiation leads, in practice, to the application of uniform standards to situations characterized by radically different degrees of intrusiveness, thereby generating either the excessive use of intrusive measures in circumstances where less restrictive means would suffice, or the abandonment of efficient investigative techniques out of concern for exceeding the legal threshold. Both methodological errors directly affect the quality of criminal prosecution and contribute to the high rates of legal reclassification documented within the analyzed case law.

Methods and materials applied. The research employs an integrative methodology, combining doctrinal analysis, comparative normative analysis, jurisprudential analysis, and the empirical-statistical method. The selection of these methods was determined by the interdisciplinary nature of the subject under examination, situated at the intersection of forensic science, criminal procedural law, and the normative framework governing personal data protection, thereby requiring a synthetic approach capable of integrating distinct analytical perspectives within a coherent framework.

From a doctrinal perspective, the research examined the contributions of Gheorghiță M. in the field of forensic methodology [1], the works of Ostavciuc D. and Odagiu Iu. concerning the investigation of organized criminality [2], the studies of D. Roman regarding the conditions for conducting special investigative measures (SIMs) [16], as well as national and international scholarly works addressing cybercrime, digital evidence, and the legal regulatory framework applicable to personal data protection. In addition, guidance documents issued by Europol and reports of the United Nations Office on Drugs and Crime concerning global trends in organized crime within the digital environment were also consulted.

From a normative perspective, the analysis is grounded in the provisions of Article 260[7] of the Criminal Code of the Republic of Moldova [5]; Law No.133/2011 on the Protection of Personal Data [10]; Articles 132[1]-132[8] and 134[3]-134[5] of the Criminal Procedure Code of the Republic of Moldova [6]; Law No.59/2012 on Special Investigative Activity [12]; Law No.50/2012 on the Prevention and Combating of Organized Crime [13]; as well as the standards established by the Budapest Convention on Cybercrime [4] and Article 8 of the European Convention on Human Rights [3].

The comparative analysis also encompassed the examination of the Romanian normative framework in the field of cybercrime — particularly Law No.161/2003 and the relevant provisions of the currently applicable Romanian Criminal Code — with a view to identifying regulatory models potentially applicable of "lege ferenda" within the Republic of Moldova.

The empirical component of the research constitutes the original foundation of the study and confers upon it a high degree of practical relevance. A total of 1,142 judicial decisions delivered in cases involving an organized criminal group (OCG) component in the Republic of Moldova during the period 2015-2025 were analyzed, all of which were available through the official judicial platform instante.justice.md. Of these, 1,126 contained exploitable PDF text, representing 98.6% of the total sample.

Each judicial decision was examined from the perspective of the typology of predicate offences, the numerical structure of the OCG, the categories of evidentiary means administered, the presence of transnational elements, the indicators concerning the use of false or stolen identities, and the criminal investigation authority involved. Data processing was conducted through both quantitative and qualitative methods, the results being systematized into thematic categories relevant to the methodological issues under examination.

This empirical basis — unique within Moldovan forensic doctrine due to its scale — enabled the identification of patterns regarding the use of fictitious identities, the typologies of electronic traces most frequently administered as evidence, and the evidentiary obstacles generated by the interference with the legal regime governing personal data protection.

Discussions and results obtained. I. Identity Theft as an Instrument of the Organized Criminal Group. The analysis of the 1,142 judicial decisions demonstrated that false or stolen identities are instrumentally employed by organized criminal groups (OCGs) in diverse and systematic ways, constituting an element of criminal infrastructure rather than an objective in itself. The predominant offence in which this practice was identified is drug trafficking (486 cases, representing 42.6% of the total sample), where fictitious identities are used primarily for the role of courier — the most frequently documented function within the examined case files (853 references) — and for the role of intermediary (175 references).

The use of false identities within these operational roles fulfills a distinct function in the internal economy of the OCG: it creates a layer of operational protection between the leader of the group and the concrete criminal act, thereby reducing the exposure of the command structure to the risks of identification and criminal liability.

In cases involving fraud (225 cases) and smuggling (150 cases), false identities serve the purpose of creating fictitious legal entities, fraudulently accessing financial services, and concealing the origin of criminal proceeds. This systemic use demonstrates that, within the context of organized criminal groups (OCGs), identity theft does not constitute an isolated offence, but rather an instrument integrated into the broader mechanism of organized criminal activity, thereby requiring a distinct methodological approach from that applicable to the investigation of identity theft committed by individual offenders.

The empirical analysis further revealed that, in 5 cases within the examined sample, the OCG was coordinated from within penitentiary institutions. In such circumstances, false identities acquire additional significance as instruments facilitating conspiratorial communication and the execution of instructions issued by the incarcerated leader.

From a forensic perspective, it is particularly significant that transnational elements were identified in 55.9% of the analyzed cases, the states most frequently referenced being Romania (325 cases), Ukraine (288 cases), and Germany (238 cases). This transnational dimension substantially increases the complexity of the investigation, given that the stolen identity data frequently originate from information systems located in other states, while the electronic evidence is often stored on extraterritorial servers. The authors' original empirical conclusion — confirmed by the structure of the examined case files — is that the investigation of identity theft committed by transnational OCGs predominantly involves interaction with at least one additional national legal system, thereby exponentially multiplying the procedural obstacles encountered during criminal proceedings. The empirical analysis revealed that electronic traces constitute the dominant category of evidence in organized crime cases: data extracted from mobile phones was used in 926

cases (82.2%), IMEI data in 921 cases (81.8%), communications through digital platforms – Telegram, Viber, and Facebook – in 547 cases (48.6%), and GPS location data in 179 cases (15.9%).

Electronic transactions were relied upon as evidentiary means in 147 cases (13.1%), while video surveillance footage (CCTV) was utilized in 102 cases (9.1%). This evidentiary structure demonstrates that the forensic investigation of organized criminal groups (OCGs) is, in its very essence, an investigation of electronic traces, thereby placing it structurally within the sphere of interference with the legal regime governing the protection of personal data.

II. The three Dimensions of the Interference. Building upon the empirical data presented and the normative analysis conducted, we propose the identification of three distinct dimensions in which the interference between personal data protection and the exigencies of forensic investigation concretely manifests itself in cases of identity theft committed by organized criminal groups (OCGs).

The first dimension concerns the collection and evidentiary exploitation of digital traces specific to identity theft. Such traces – including IP addresses, session cookies, metadata associated with forged documents, the history of electronic transactions, and GPS location data – constitute personal data within the meaning of Law No.133/2011, which implies that access thereto by criminal investigation bodies is subject to differentiated judicial authorizations regulated under Articles 132¹-132□ of the Criminal Procedure Code of the Republic of Moldova [6].

In this context, Gheorghiță M. observes that "the global changes that are rapidly intensifying across all spheres of modern society, connected to scientific and technological progress in the field of computerized electronic technologies, dictate new directions within national forensic science" [1, p. 15], thereby requiring the continuous adaptation of investigative methodologies to emerging typologies of digital traces.

The interference arises where evidentiary urgency necessitates the immediate access to such data, while the authorization procedure – legitimate in itself – introduces operational delays capable of leading to the irreversible loss of digital traces.

An essential forensic particularity of electronic traces in cases involving identity theft committed by organized criminal groups (OCGs) resides in their ephemeral character: unlike traditional material traces, which physically persist at the crime scene, digital data are subject to automatic deletion cycles configured by service providers, may be overwritten upon the reactivation of the information system, or become inaccessible through the mere modification of access credentials.

The empirical analysis demonstrated that OCG members deliberately exploit this vulnerability by using applications based on ephemeral messaging systems and prepaid telephone cards characterized by short operational cycles. Roman D. emphasizes that the conditions governing the conduct of special investigative measures (SIMs) represent "the totality of principles and rules which ensure, on the one hand, the balance of the individual's interests – namely the right to the secrecy of private life – and, on the other hand, the interests of society in the effectiveness of combating criminality, in the timely detection of offences, and in their prevention and suppression" [16, p. 117].

In cases of digital identity theft, however, this balance becomes particularly difficult to calibrate precisely because of the speed with which electronic traces disappear or become inaccessible.

The second dimension concerns access to data stored on extraterritorial servers belonging to encrypted communication platforms. Organized criminal groups (OCGs)

operating in the Republic of Moldova systematically use Telegram, Viber and WhatsApp for the coordination of criminal activities – these platforms being identified in 547 cases within the analyzed empirical database. OCG members deliberately avoid communication through conventional mobile telephony precisely because the traffic data retained by telecommunications operators are accessible to criminal investigation bodies through the procedures established under Articles 134⁴-134⁵ of the Criminal Procedure Code of the Republic of Moldova [6].

The data stored on the servers of these platforms are subject to the legislation of the states in whose territory the respective servers are located, which renders national access procedures, in practice, either inapplicable or excessively slow. This methodological gap is further aggravated by the absence, within the Criminal Procedure Code of the Republic of Moldova, of a distinct procedure governing the search and seizure of computer data, analogous to that provided by the Budapest Convention on Cybercrime [4]. This legislative deficiency requires urgent remedial action and constitutes a "lege ferenda" issue with a direct impact upon investigative efficiency.

The third dimension concerns the particularities of international cooperation in cases involving organized criminal groups (OCGs) with a digital component. Requests for mutual legal assistance aimed at obtaining electronic data involve lengthy procedures that are incompatible with the evidentiary urgency specific to the investigation of OCGs. The Budapest Convention on Cybercrime (Budapest, 2001) establishes mechanisms for expedited cooperation; however, their practical effectiveness depends upon the degree of ratification and implementation within the requested states, the technical capacity of the authorities of the requested state, and the political willingness to cooperate [4].

The transnational dimension identified in 55.9% of the analyzed OCG cases – with frequent references to Romania, Ukraine, and Germany – illustrates the scale of this problem for Moldovan judicial practice and highlights the necessity of developing specific cooperation protocols adapted to the urgency inherent in digital investigations.

III. Specific Evidentiary Vulnerabilities and Their Methodological Consequences. The identified normative interference generates, within investigative practice, a series of specific evidentiary vulnerabilities that affect both the quality and the admissibility of digital evidence in cases involving identity theft committed by organized criminal groups (OCGs). The first vulnerability concerns the risk of exclusion of evidence obtained in violation of the authorization procedures established under Articles 94-96 of the Criminal Procedure Code of the Republic of Moldova [6].

Where the investigator, acting under the pressure of evidentiary urgency, accesses personal data without the corresponding judicial authorization, the evidence thereby obtained becomes susceptible to exclusion from the criminal proceedings, in some instances irreversibly compromising the prosecution. This reality is reflected in the 30.4% rate of reclassification of charges involving an OCG component identified within the analyzed case law, which signals, inter alia, the existence of systematic evidentiary difficulties in proving organized criminal activity within the digital environment.

The second vulnerability concerns the integrity of the chain of custody of digital evidence. Unlike traditional material evidence, electronic data may be altered, copied, or deleted without leaving visible traces, thereby requiring the use of specialized technical procedures for extraction and preservation – including cryptographic hashing, forensic imaging of storage devices, and audit logs – capable of guaranteeing the authenticity and integrity of the data relied upon as evidence.

The absence of nationally regulated methodological standards explicitly governing

this matter constitutes a legislative and operational gap identified within the present research, with direct consequences for the admissibility of digital evidence before judicial authorities.

The third vulnerability concerns the risk of overlap between the personal data of victims and those of OCG members within the investigative process. Identity theft, by its very nature, involves the exploitation of the victim's personal data, which acquire a dual evidentiary relevance: they document both the offence suffered by the victim and the criminal activity of the perpetrators.

This overlap creates parallel – and at times conflicting – obligations for criminal investigation bodies: on the one hand, the obligation to use the victim's data as evidentiary material; on the other hand, the obligation to safeguard the victim's private life in accordance with Law No.133/2011 [10]. The management of this dual obligation requires the development of specific methodological protocols, which are currently absent from the practice of criminal investigation authorities in the Republic of Moldova.

From the perspective of the implications for investigative practice, we consider that criminal investigation bodies and the PCCOCS – identified as the investigative authority in 263 of the analyzed cases – must develop specialized competencies in the digital investigation of identity theft committed by organized criminal groups (OCGs). Such competencies should include, inter alia: the initiation and execution of data preservation procedures addressed to electronic service providers, the use of forensic extraction tools for mobile phones and information systems, and the evidentiary exploitation of metadata in compliance with the admissibility standards established in the case law of the European Court of Human Rights.

The specialized training of investigators in these fields constitutes a prerequisite for the effectiveness of any improved normative framework.

IV. The Framework for Normative and Operational Balance. The analysis of the case law of the European Court of Human Rights demonstrates that not every access by criminal investigation authorities to an individual's electronic data automatically constitutes a violation of the right to private life guaranteed under Article 8 of the European Convention on Human Rights. The Court has developed a tripartite test – legality, legitimate aim, and necessity and proportionality – which does not exclude digital investigations, but rather disciplines them by imposing adequate procedural safeguards against arbitrary use [3].

Applied in cases involving organized criminal groups (OCGs), this test presupposes that access to the identity data of group members is justified where there exists a documented reasonable suspicion and where the investigative measures employed are proportionate to the seriousness of the offences under examination and to the investigative alternatives available. The case law of the European Court of Human Rights in the cases of Klass and Others v. Germany and Uzun v. Germany established that the state enjoys a margin of appreciation in configuring surveillance measures, provided that effective safeguards against abuse exist — safeguards equally applicable within the context of the digital investigation of OCGs.

We consider that the resolution of the identified interference cannot consist in subordinating one value to the other – neither may data protection be sacrificed in favour of repressive efficiency, nor may forensic investigation be paralysed by excessive protectionism. We propose the articulation of a balancing model structured around three interdependent components.

The starting point consists in the explicit regulation of the obligation of immediate

preservation of digital data – a freeze-type procedure – adapted to the specific nature of volatile electronic traces and distinct from the general procedures governing the seizure of objects regulated under Articles 126-128 of the Criminal Procedure Code of the Republic of Moldova [6].

This procedure, recommended by the Budapest Convention on Cybercrime [4], would enable criminal investigation authorities to request service providers to preserve data without effectively accessing them, the actual access subsequently being authorized through the ordinary judicial procedure. In this manner, the urgency of preservation would be separated from the judicial authority governing access.

The second component concerns the differentiation of authorization regimes according to the categories of data involved and the degree of intrusiveness of the measure employed. Access to traffic metadata – namely, who communicated with whom, when, and from where – requires a different authorization standard from that applicable to access to the actual content of communications, whereas treating these categories uniformly generates either unjustified overprotection of metadata or the trivialization of access to content.

Such differentiation is already recognized within the European doctrine of data protection and in the case law of the European Court of Human Rights, and therefore requires explicit transposition into the Criminal Procedure Code of the Republic of Moldova [6], through the establishment of clear authorization thresholds correlated both with the degree of intrusiveness of each category of data and with the nature of the offences under investigation.

The third component concerns the strengthening of international cooperation specific to OCG cases involving a digital component, through accelerated protocols and operational contact points capable of overcoming the inherent slowness of traditional mutual legal assistance procedures, while relying upon the already existing mechanisms of Europol, Interpol, and the Budapest Convention on Cybercrime [4].

The implementation of this balancing model requires not only legislative reforms, but also substantial investments in the institutional capacity of criminal investigation bodies. The digital investigation of identity theft committed by organized criminal groups (OCGs) necessitates specialized equipment for forensic data extraction, software applications designed for the analysis of metadata and electronic connections, as well as personnel possessing specialized training in digital forensic science.

The PCCOCS – identified as the investigative authority in 263 of the analyzed cases – represents the institution with the greatest potential to develop such specialized capacity at the national level, benefiting from the experience accumulated in the investigation of transnational organized criminality.

We consider that the allocation of dedicated resources for the training of investigators in digital forensic science and for the acquisition of forensic extraction equipment constitutes an institutional priority with a direct impact upon investigative efficiency, complementary to any normative reform.

Conclusions. The present scientific undertaking has demonstrated that the interference between personal data protection and the exigencies of forensic investigation in cases of identity theft committed by organized criminal groups (OCGs) constitutes an autonomous methodological problem, manifested concretely across three distinct dimensions: the collection of volatile digital traces under differentiated authorization regimes, access to data stored extraterritorially on encrypted communication platforms, and international cooperation conducted under conditions of evidentiary urgency. The

identification and conceptualization of this issue as an independent methodological entity represents the principal original contribution of the present research.

The analysis of 1,142 judicial decisions delivered during the period 2015-2025 revealed that electronic traces – telephone data (82.2%), IMEI data (81.8%), and communications conducted through digital platforms (48.6%) – constitute the dominant evidentiary category in OCG cases within the Republic of Moldova, while the transnational dimension identified in 55.9% of the cases substantially increases the complexity of accessing such evidence. These empirical findings, unprecedented within national forensic doctrine, confirm that the examined interference does not represent a marginal phenomenon, but rather an ordinary reality of Moldovan judicial practice.

We consider that resolving this interference requires not a choice between the two competing values, but the articulation of a model of normative and operational balance founded upon the immediate preservation of digital data, the differentiation of authorization regimes, and the strengthening of specialized international cooperation. The introduction into the Criminal Procedure Code of a distinct procedure governing the search and seizure of computer data, in coherence with the obligations assumed by the Republic of Moldova through its accession to the Budapest Convention on Cybercrime, constitutes a priority direction of legislative reform with a direct impact upon the effectiveness of the forensic investigation of OCGs within the digital environment.

The interference analyzed in the present study transcends the national context: it reflects a structural challenge faced by all legal systems adhering to European standards of data protection, under conditions in which digitalized organized criminality evolves more rapidly than the normative response capacity of states. Consequently, the methodological and legislative solutions developed at the national level must remain compatible with European and international developments in the field, so as not to generate new gaps in cross-border cooperation relating to the investigation of OCGs with a digital component.

Bibliographical references

1. Gheorghiță M. Tratat de metodică criminalistică. Chișinău: CEP USM, 2015. 450 p.
2. Ostavciuc D., Odagiu Iu. Metodica cercetării infracțiunilor comise de grupuri criminale organizate. Chișinău: Academia „Ștefan cel Mare", 2020. 168 p.
3. Convenția Europeană pentru Apărarea Drepturilor Omului și a Libertăților Fundamentale. Roma, 04.11.1950. Ratificată de Republica Moldova prin Hotărârea Parlamentului nr.1298-XIII din 24.07.1997.
4. Convenția Consiliului Europei privind criminalitatea informatică (Budapesta, 23.11.2001). Ratificată de Republica Moldova prin Legea nr.6-XVI din 02.02.2009. În: Monitorul Oficial al Republicii Moldova, nr.40-41/114 din 27.02.2009.
5. Codul penal al Republicii Moldova nr.985-XV din 18.04.2002, republicat. În: Monitorul Oficial al Republicii Moldova, nr.72-74/195 din 14.04.2009, cu modificările ulterioare.
6. Codul de procedură penală al Republicii Moldova nr. 122-XV din 14.03.2003, republicat. În: Monitorul Oficial al Republicii Moldova, nr.248-251/699 din 05.11.2013, cu modificările ulterioare.
7. Directiva 95/46/CE a Parlamentului European și a Consiliului din 24.10.1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date. Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex:31995L0046.
8. Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013

privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului. Disponibil: https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=celex:32013L0040.
9. Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27.04.2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE. Disponibil: https://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX%3A32016R0679.
10. Legea Republicii Moldova nr.133 din 08.07.2011 privind protecția datelor cu caracter personal. În: Monitorul Oficial al Republicii Moldova, nr.170-175/547 din 14.10.2011.
11. Legea privind protecția datelor cu caracter personal nr.195 din 25.07.2024. În: Monitorul Oficial nr.367-369/574 din 23.08.2024.
12. Legea Republicii Moldova nr.59 din 29.03.2012 privind activitatea specială de investigații. În: Monitorul Oficial al Republicii Moldova, nr.113-118/373 din 08.06.2012.
13. Legea Republicii Moldova nr.50 din 22.03.2012 privind prevenirea și combaterea criminalității organizate. În: Monitorul Oficial al Republicii Moldova, nr. 103/343 din 29.05.2012.
14. Legea pentru modificarea unor acte normative (modificarea Codului penal și a Codului contravențional), nr.136 din 06.06.2024. În: Monitorul Oficial al Republicii Moldova, 2024, nr.245-246, 353.
15. Hotărârea Guvernului Republicii Moldova pentru aprobarea Regulamentului privind armonizarea legislației Republicii Moldova cu legislația Uniunii Europene, nr.1171 din 28.11.2018. În: Monitorul Oficial al Republicii Moldova, 2018, nr.499-503, 1314.
16. Roman D. Temeiurile și condițiile de efectuare a măsurilor speciale de investigații. Teză de doctor în drept. Chișinău, 2020. 210 p.
17. Botnari I. Particularitățile cercetării infracțiunilor comise de grupuri criminale organizate dirijate din penitenciare. În: Legea și Viața, 2023, nr.5, p.312-319. Disponibil: https://ibn.idsi.md/sites/default/files/imag_file/312-319_4.pdf.
18. Brînza S., Stati V. Furtul de identitate: anatomia unei infracțiuni în era digitală. În: Studia Universitatis Moldaviae, Revista științifică a Universității de Stat din Moldova, 2025, nr.8(188). p.35-44. Disponibil: https://ojs.studiamsu.md/index.php/stiinte_sociale/article/view/6840/9203.
19. Gheorghiță M. Caracteristica și modelul criminalistic al infracțiunilor. În: Avocatul Poporului, 2012, nr.7-8, p.14-18. Disponibil: https://ibn.idsi.md/sites/default/files/imag_file/5.Caracteristica%20si%20modelul%20criminalistical%20al%20infractiunilor.pdf.
20. Gugulan E. Analiza cadrului normativ privind datele cu caracter personal. În: Anale ştiinţifice ale Academiei „Ştefan cel Mare" a MAI al RM: Ştiinţe Juridice. Nr. XVIII(2) / 2018 / ISSN 1857-0976. p.103-110. Disponibil: https://ibn.idsi.md/sites/default/files/imag_file/103-110_5.pdf.
21. Ostavciuc D. Protecția datelor cu caracter personal în procesul penal – analiza doctrinei și standardele UE. În: Conferința "European integration through the strengthening of education, research, innovations in Eastern Partnership Countries", 2th Edition, Chisinau, Moldova, May 16-17, 2022. p.77-85. Disponibil: https://ibn.idsi.md/sites/default/files/imag_file/p-77-85_0.pdf.