E-ISSN 3008-6299

THE CRIMINAL SCIENCES JOURNAL
TCSJ
"AL.I. CUZA" POLICE ACADEMY

BETWEEN CRIMINAL LAW AND DIGITAL TRUST: ARTICLE 250 OF THE CRIMINAL CODE AND THE CHALLENGE OF NON-CASH PAYMENT FRAUD IN ROMANIA

MIHAI CURTEANU[1]

Abstract: *Romania's transition to electronic payment systems has generated new vulnerabilities that require appropriate legislative responses. Article 250 of the Criminal Code criminalizes unauthorized transactions carried out through electronic payment instruments or the identification data associated with them, basing criminal liability on the manipulation of automated computer systems. The research analyses the operational effectiveness of this criminal law in the context of the increase in electronic payment fraud. The legal framework integrated by Law no. 209/2019 and the NBR regulations establishes reimbursement obligations for payment service providers in parallel with individual criminal sanctions. Judicial interpretation has evolved to cover technological developments, as the High Court of Cassation and Justice acknowledged that contactless use without entering a PIN is tantamount to traditional card fraud. The technology-neutral approach to regulation allows adaptation to emerging payment methods without constant legislative updates. The paper brings certain clarifications in the field of delimitation of criminal liability for frauds committed through electronic payment instruments, establishing the connection between the manipulation of automated computer systems and the prejudice of individual or collective assets.*

Keywords: *criminal liability in electronic payment frauds; manipulation of automated information systems; unauthorized operations through contactless instruments; coordination of criminal law with NBR regulations*

1. Introduction

Romania's payment system has moved decisively to a cash-less settlement, with contactless cards, mobile wallets and instant account-to-account rails now facilitating most retail transactions. The National Bank's 2024 Financial Stability Report notes a double-digit growth

[1] Senior Police Instructor I, Department of Gendarmerie of the Police Faculty, "Alexandru Ioan Cuza" Police Academy, Romania, Corresponding author: mishucurteanu@gmail.com

Copyright: ©2025 by the authors. Open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license
https://creativecommons.org/licenses/by/4.0/

TCSJ, Vol. 3, no. 1/2025, pp. 24-32

in electronic payments value over the past year and, tellingly, a similar growth in unauthorized card operations, with roughly half of them involving contactless interfaces[1]. The European Central Bank and European Banking Authority observe this national development as part of a broader European trend, with fraud totaling €2 billion on major payment instruments in the first half of 2023 despite the widespread adoption of strong customer authentication. Although PSD2[2] security requirements became mandatory in September 2019 and reduced specific attack methods, their protection remains inconsistent when criminals utilize credential-stuffing and social-engineering techniques that circumvent possession-based authentication factors[3].

In this context, the Romanian legislation incorporated Article 250 into the Criminal Code to make it illegal to perform any withdrawal, loading, unloading or transfer operations using an electronic instrument or identification data linked to its use when the legitimate owner has not authorized it[4]. The provision links to the technologically neutral definitions of "computer system" and "computer data" in Article 181 of the Criminal Code, which establishes liability based on deceptive automated infrastructure manipulation instead of physical device theft. Article 250 exists within a larger legal framework: the Law no. 209/2019 establishes a payment-service provider obligation to refund the payer within one working day after an unauthorized transaction[5], National Bank Regulation no. 5/2019[6] requires electronic-money institutions to maintain adequate capital and safekeeping standards, and Regulation no. 2/2020 forces all providers to report major operational or security incidents to the supervisor within a four-hour period which aims to preserve ephemeral forensic evidence[7]. At European level, Directive 2019/713 requires Member States to criminalize both device and data misuse related to non-cash payment instruments[8], and it provides a standardized framework into which Article 250 of the Criminal Code fits perfectly.

[1] National Bank of Romania, Financial Stability Report 2024, NBR Publishing House, Bucharest, 2024, p. 45.
[2] PSD2 stands for Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC, published in the Official Journal of the European Union, L series, No. 337/35 of December 23, 2015, as subsequently amended and supplemented.
[3] European Banking Authority & European Central Bank, Six-Monthly Payment-Fraud Statistics Report 2024, Frankfurt/London, 2024, p. 12.
[4] Law no. 286 of 17 July 2009 on the Criminal Code, published in the Official Gazette of Romania, Part I, no. 510 of 24 July 2009, as subsequently amended and supplemented.
[5] Law no. 209 of November 8, 2019 on payment services and amending certain normative acts, published in the Official Gazette of Romania, Part I, no. 913 of November 13, 2019, as subsequently amended and supplemented.
[6] Regulation of the National Bank of Romania no. 5 of December 13, 2019 on electronic money institutions published in the Official Gazette of Romania, Part I, no. 1021 of December 19, 2019, as subsequently amended and supplemented.
[7] Regulation of the National Bank of Romania no. 2 of January 30, 2020 on security measures relating to operational and security risks and reporting requirements related to payment services, published in the Official Gazette of Romania, Part I, no. 115 of February 14, 2020, as subsequently amended and supplemented.
[8] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment, published in the Official Journal of the European Union, L series, No. 123 of 10 May 2019.

The research focuses on evaluating the operational effectiveness of this complex legal system in real-world situations. It introduces the doctrinal aspects of Article 250 of the Criminal Code and incorporates recent High Court interpretations that establish contactless misuse without PIN entry as equivalent to traditional card fraud thus extending the provision's coverage to tokenized instruments. The analysis shows how the offence operates inside the administrative system built by PSD2 implementation and central-bank governance and demonstrates how criminal enforcement supports prudential supervision. The empirical evidence from central-bank records along with supranational fraud statistics serves to enhance doctrinal research and allows for a determination of whether increased losses stem from enforcement weaknesses or technological differences or both factors.

The analytical component of this paper examines Article 250 of the Criminal Code liability through a review of protected interests, material and subjective elements, victim configuration, jurisprudential developments and macro-economic effects. The paper evaluates how well the statute will adapt to future financial innovations like programmable money and behavioral biometrics and recommends potential legislative or interpretative improvements.

A unified analysis becomes essential because separate examinations may fail to demonstrate how criminal law, banking regulation and market practice work together to enforce non-cash fraud. A detailed examination of individual components does not explain why refund obligations coexist with ongoing loss growth or explain how evidence requirements change as payment authentication transitions from fixed credentials to flexible tokens. Through a combination of legal analysis with practical examples the research provides regulators and practitioners as well as scholars with evidence-based tools to assess Romania's asset protection system's resilience against digital trust threats that simultaneously support economic activities.

2. Article 250 of the Criminal Code in context: trust, data, and the architecture of criminal liability

Digital payment services have transformed Romanian retail and wholesale finance during the past decade, yet the same infrastructures have multiplied the channels through which offenders can reroute value without the account holder’s knowledge. Parliament’s response is found in the Criminal Code, where Article 250 criminalizes any withdrawal, loading, unloading, or transfer that exploits a cashless payment instrument or the identification data that permit its use when the legitimate holder has not consented. By rooting criminal liability in the reliability of a “computer system” and the integrity of “computer data,” both terms defined in Article 181 of the Criminal Code, the provision renders its protective reach technology-neutral and therefore adaptable to magnetic stripes, NFC tokens, cloud wallets, and blockchain addresses alike. The penal norm does not stand alone. Its deterrent function interlocks with Law no. 209/2019 on payment services, which transposed PSD2 and assigned

immediate refund duties to providers, and with two central-bank regulations that refine prudential and security obligations: NBR Regulation no. 5/2019 on electronic-money institutions, which imposes capital, safeguarding, and reporting rules and NBR Regulation no. 2/2020 on operational and ICT-security incident reporting for all payment-service providers. Together, the three instruments create a dual enforcement track—administrative liabilities borne by institutions and criminal liabilities borne by intentional actors—that sustains both patrimonial protection and public confidence in cash-less settlement.

Romanian scholars place special emphasis on the dual legal object safeguarded by Article 250 of the Criminal Code: the individual's balance and the collective expectation that electronic records tell the truth about value. Recent commentary frames the norm as "poly-offensive", arguing that it fuses classical property interests with the intangible but quantifiable trust that underlies automated clearing and settlement. Judicial practice confirms that perspective. The High Court of Cassation and Justice, in Decision no. 53/2022, held that contact-less misuse of a token amounts to fraudulent performance even without PIN entry, thereby recognizing the bank's internal risk-control protocols as part of the protected sphere. Such rulings underline Parliament's choice to anchor consummation in the moment the system logs the transaction rather than the later point of interbank settlement, which in turn accelerates investigative timelines and preserves digital evidence.

Central-bank data illustrates why deterrence matters. The Financial Stability Report for 2024 notes a fourteen-percent annual rise in unauthorized card operations, half of which relied on contact-less functionality. The European Banking Authority and European Central Bank place Romania within a broader continental pattern: payment fraud across the EEA reached €2 billion in the first half of 2023, dominated in value terms by credit-transfer and card channels. These findings confirm that Article 250 of the Criminal Code addresses a genuine systemic risk rather than an isolated subset of offences. Against that backdrop, the following analysis traces the provision's material and subjective elements, maps the roles of victims and offenders, and evaluates future challenges posed by programmable money and biometric authentication.

3. Operational Dynamics and Regulatory Strings

Article 250 occupies Chapter IV of Title II of the Criminal Code, the cluster devoted to fraud perpetrated through computer systems and electronic means of payment. The provision describes three factual hypotheses that converge on a single dynamic: insertion of an illegitimate instruction into an automated payment architecture. In the primary variant, the perpetrator executes a financial operation—withdrawal, loading, unloading, or transfer—by using, without consent, a non-cash instrument or its identifying credentials. A second variant mirrors the first but covers operations initiated through fictitious or otherwise unauthorized data, such as credentials harvested from phishing kits. A third variant criminalizes the transmission of such data to another person to facilitate future fraud. Penalty ranges of two to

seven years for the first two variants and one to five years for the third mirror the sanction scale of classic misappropriation yet recognize the added societal impact of undermining digital trust.

The provision's ontological prerequisites flow from Article 181 of the Criminal Code definitions: a computer system refers to any ensemble of devices that performs automated data processing, and computer data denotes any representation of facts or concepts that the system can process. Those definitions mark the outer boundary of criminalization; without a computer system, Article 250 does not apply. Hence, physical theft of a paper cheque falls under larceny, whereas cloning a card's NFC handshake squarely invokes Article 250 of the Criminal Code because the act corrupts authentication protocols baked into the payment processor's servers. Romanian courts have embraced the distinction, frequently requalifying indictments when the technical element of system manipulation proves absent.

Material object debates focus on whether the instrument itself—plastic card, smartphone, hardware token—qualifies or whether only the intangible balance does so. The prevailing view adopts a dual conception: whenever the instrument is physically altered or employed, it becomes part of the corpus delicti; when the attack targets data or balances stored remotely, the digital value alone suffices. This elasticity is essential for prosecuting card-not-present fraud and credential-stuffing attacks that never touch the card. It also aligns with the EU's 2019 directive on combating non-cash payment fraud, which obliges Member States to criminalize misuse of both devices and data.

Turning to subject roles, active liability extends to any natural or legal person possessing criminal capacity. Passive status is bifurcated because civil law declares that deposited funds belong to the bank, even as the customer retains a claim for equivalent value under Articles 2184–2191 of the Civil Code. Decision no. 53/2022 therefore recognized both entities as injured parties, granting each procedural rights such as access to evidence and the ability to attach civil claims in the criminal file. This arrangement streamlines litigation, fosters cooperation between financial institutions and customers, and preserves the evidentiary chain that might otherwise splinter across forums.

Mens rea is most often direct intent: the offender knows that authorization is lacking yet proceeds. Indirect intent suffices where the perpetrator accepts that the transaction may be unauthorized but pursues the action anyway, common in credential-stuffing against online banking portals. The data-transmission variant demands purpose aimed at facilitating future fraud, a requirement courts satisfy through temporal and contextual inference- for instance, when credentials dump onto an illicit forum shortly before a cluster of withdrawals hits (Pavel, 2025, pp.1-20)[1]. If proof of purpose falters, prosecutors may pivot to Article 249 of the

[1] Pavel, T., (2025), "*Defining Cybercrime in Romania: An Analysis of Official Policies and National Strategies*" , Romanian Journal of Forensic Science, vol. 26, no. 1/2025, Bucharest, pp. 1-20.

Criminal Code on illegal access, though that downgrade narrows sentencing exposure and weakens the restitution leverage that Article 250 affords victims.

Attempts are expressly punishable under Article 252 of the Criminal Code. Doctrine treats an attempt as complete once the unauthorized credentials reach a payment interface that rejects the transaction, whether for insufficient funds or because velocity filters flag anomaly[1]. Preparatory acts—installing skimmers, scripting phishing sites—lie outside the provision unless they constitute conspiracy. Regulators counterbalance that lacuna by imposing administrative fines under Regulation no. 2/2020, which obliges payment-service providers to report major operational or security incidents within four hours. Such rapid reporting accelerates criminal referrals and preserves volatile evidence.

Economic effects radiate beyond immediate victim loss. Central-bank analysts label payment fraud an amplifier of credit risk; refund obligations erode capital buffers, nudge funding costs upward, and may tighten credit supply. Regulation no. 5/2019 mitigates part of that risk by requiring electronic-money issuers to ring-fence customer funds, yet the expense of continuous monitoring, behavioral analytics, and cyber-insurance ultimately diffuses into higher service fees. At the continental level, the EBA-ECB fraud report confirms the macro dimension: despite strong customer authentication, credit transfers remain the costliest channel, while card fraud dominates by volume. These data demonstrate that Article 250's deterrent objective aligns with financial-stability mandates, making criminal law a complementary tool to macro-prudential oversight.

Case law tracks technological evolution as early dockets centered on counterfeit magnetic stripes; the past five years have featured malware that injects rogue beneficiary fields into browser sessions and over-the-air pairing that converts stolen cards into mobile tokens (Urs, 2015, pp. 173-180)[2]. Courts regard the initial pairing plus the chain of subsequent taps as a continuous offence, fixing exhaustion at the last unauthorized transaction, a methodology that prevents offenders from atomizing liability through rapid micro-withdrawals[3]. More recently, authorized push-payment scams—where social engineering deceives the payer into initiating the transfer—have tested doctrinal limits. Several appellate panels have ruled that consent vitiated by sophisticated deception is equivalent to absence of consent, keeping such schemes within Article 250's ambit and avoiding gaps that offenders could exploit.

The provision's extraterritorial flexibility has proved vital in joint investigations. Mutual-legal-assistance treaties and Europol's cybercrime platforms allow Romanian prosecutors to rely on foreign server logs, hash databases, and witness statements when unauthorized

[1] Răducanu, R., (2017), "*Brief Considerations on the Sanctioning of Frauds Committed through Computer Systems and Electronic Payment Instruments*" , Annals of 'Al. I. Cuza' University of Iași – Legal Sciences Series, vol. LXIII, no. 2/2017, Iași, pp. 33-40.

[2] Urs, B.-A., (2015), "*Security Issues and Solutions in E-Payment Systems*" , Fiat Iustitia, no. 1/2015, Cluj-Napoca, pp. 173-180.

[3] High Court of Cassation and Justice (Romania), Decision No. 53 of 28 September 2022 on the settlement of legal issues (RIL), published in the Official Gazette of Romania, Part I, No. 1120 of 21 November 2022.

operations produce effects on Romanian territory. Because Regulation no. 2/2020 compels local institutions to record incident metadata in standardized formats, digital-forensic teams can map cross-border transactional flows with heightened precision, a capability that has already facilitated convictions in skimming rings spanning three continents.

Looking forward, the payment landscape is poised for further disruption. The National Bank is testing a retail central-bank digital currency layer, while private consortia pilot smart-contract engines that release funds only when predefined parameters fire. These innovations could blur the statute's current vocabulary: is a line of self-executing code an "instrument," and is a smart-contract variable "identification data" ? Judicial inventiveness may answer in the short term, yet durable clarity will require legislative foresight. Meanwhile, Regulation no. 2/2020's focus on incident taxonomy and rapid disclosure offers a template for incorporating programmable-money risks without rewriting the Criminal Code each time a new protocol launches.

Biometric authentication presents a parallel test. Voiceprint and gait-analysis libraries reduce credential theft but raise privacy stakes; a breached biometric cannot be re-issued like a password. Regulators may extend strong-customer-authentication mandates to encompass behavioral biometrics, but Article 250 of the Criminal Code will still form the punitive backstop when attackers deep-fake the required patterns or coerce victims into recording them. The statute's technology-neutral stance again proves advantageous: as long as the fraudulent instruction traverses a computer system, liability attaches.

4. Conclusions

Article 250 of the Romanian Criminal Code represents a legislative attempt to address electronic payment fraud through technology-neutral provisions, yet its practical implementation reveals significant gaps between normative intent and operational reality. The provision attempts to criminalize unauthorized operations using cashless payment instruments or their identification data, anchoring liability in computer system manipulation rather than physical device theft.

The legal framework integrates with European directives and administrative regulations, creating a dual enforcement system where payment service providers bear refund obligations while individual perpetrators face criminal sanctions. However, National Bank data demonstrates the system's limited effectiveness: unauthorized card operations increased by fourteen percent annually, with half exploiting contactless functionality despite PSD2 strong authentication requirements. This growth suggests that current legal and technical safeguards are insufficient against sophisticated credential-stuffing and social engineering attacks. Judicial interpretation has evolved to address technological developments, with the High Court recognizing contactless misuse without PIN entry as equivalent to traditional card fraud. Courts treat sequential unauthorized transactions as continuous offenses, preventing

liability fragmentation through micro-withdrawals. Yet enforcement faces practical limitations: the four-hour incident reporting obligation may accelerate criminal referrals, but institutional capacity to process complex technological cases remains constrained.

The provision's technology-neutral approach enables adaptation to emerging payment methods without constant legislative updates, covering magnetic stripes, NFC tokens, and potentially smart contracts. However, this flexibility creates interpretive challenges: whether self-executing code constitutes an "instrument" or smart-contract variables represent "identification data" remains unclear. Similarly, biometric authentication systems present new vulnerabilities that existing legal frameworks may not adequately address. Cross-border cooperation has improved through mutual legal assistance treaties and Europol platforms, enabling Romanian prosecutors to utilize foreign server logs and witness statements. Standardized incident reporting formats facilitate digital forensic mapping of transnational flows, though jurisdictional discrepancies continue to create enforcement gaps.

The victim configuration recognizing both banks and clients as injured parties streamlines litigation but may generate conflicts when their procedural strategies diverge. The subjective element requiring fraudulent intent faces evidentiary challenges in automated attack scenarios, particularly when establishing the causal link between data transmission and subsequent fraud. Future challenges reside in the legal treatment of central bank digital currencies and programmable money systems that blur traditional payment concepts. Authorized push payment scams, where psychological manipulation induces victims to initiate transfers, test doctrinal boundaries between vitiated consent and genuine authorization. The provision's integration with administrative frameworks represents an attempt at regulatory coordination, yet significant enforcement disparities persist. Sustained fraud growth despite regulatory enhancements indicates structural limitations in current approaches. The balance between individual patrimonial protection and systemic confidence in electronic payments requires more coherent alignment between prudential supervision and criminal law enforcement.

Article 250 of the Criminal Code demonstrates a certain level of legislative awareness of digital fraud risks and technological evolution, yet its effectiveness depends on addressing institutional capacity constraints, clarifying emerging technology applications, and improving coordination between administrative and criminal enforcement mechanisms. The provision provides a foundation for fraud prevention but requires continuous adaptation to maintain relevance in rapidly evolving payment landscapes.

References

Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment, published in the Official Journal of the European Union, L 123, 10 May 2019

European Banking Authority & European Central Bank, *Six-Monthly Payment-Fraud Statistics Report 2024*, Frankfurt / London, 2024

High Court of Cassation and Justice (Romania), *Decision no. 53 of 28 September 2022 on the settlement of legal issues (RIL)*, published in the Official Gazette of Romania, Part I, no. 1120 of 21 November 2022

Law no. 209 of 8 November 2019 on Payment Services and amending certain normative acts, published in the *Official Gazette of Romania*, Part I, no. 913 of 13 November 2019

Law no. 286 of 17 July 2009 on the Criminal Code, published in the Official Gazette of Romania, Part I, no. 510 of 24 July 2009

National Bank of Romania, *Financial Stability Report 2024*, BNR Publishing House, Bucharest, 2024

Pavel, Tudor, (2025), "*Defining Cybercrime in Romania: An Analysis of Official Policies and National Strategies*", Romanian Journal of Forensic Science, vol. 26, no. 1/2025, Bucharest

Răducanu, Ruxandra, (2017) "*Brief Considerations on the Sanctioning of Frauds Committed through Computer Systems and Electronic Payment Instruments*", Annals of 'Al. I. Cuza' University of Iași – Legal Sciences Series, vol. LXIII, no. 2/2017, Iași, 2017

Regulation of the National Bank of Romania no. 2 of 30 January 2020 on security measures relating to operational and security risks and reporting requirements for payment services, published in the Official Gazette of Romania, Part I, no. 115 of 14 February 2020

Urs, Bogdan-Alexandru, (2015), "*Security Issues and Solutions in E-Payment Systems*", Fiat Iustitia, no. 1/2015, Cluj-Napoca