CZU: 343.72.004.056

ARTICLE 260 OF THE CRIMINAL CODE OF THE REPUBLIC OF MOLDOVA IN THE CONTEXT OF CONCURRENT OFFENSES: IMPLICATIONS AND INTERPRETATIONS REGARDING THE IMPORT, PRODUCTION, AND MARKETING OF SOFTWARE PRODUCTS AND TECHNICAL MEANS

Sergiu LISNIC,
PhD student,
"Stefan cel Mare" Academy of the Ministry of Internal Affairs,
Republic of Moldova
ORCID: 0009-0000-1406-7052

Summary

This study addresses the critical aspects of Article 260 of the Criminal Code of the Republic of Moldova, focusing on the concurrence of offenses in the context of emerging technologies such as artificial intelligence (AI). It analyzes how criminal legislation can and must adapt to the challenges posed by the use of AI in offenses involving software and technical means. Additionally, the article discusses the necessity for rigorous interpretation of the law to enhance the effectiveness of combating cybercrimes and to ensure equitable justice in the digital age.

Keywords: cyber offenses, artificial intelligence, cybersecurity, concurrence of offenses, malicious software.

Introduction. In the digital age, the exponential growth of technology has been accompanied by a similar evolution in cybercrime, challenging legal systems to continuously adapt to new forms of criminality. The Republic of Moldova, like other countries, faces the increased complexity of cybercrimes which not only breach various legislative provisions, but often overlap, leading to concurrent offenses. These situations present unique challenges in the interpretation and application of the law, given that different actions can simultaneously trigger multiple articles of the Criminal Code.

This article aims to explore and analyze how concurrent offenses are treated in the criminal legislation of the Republic of Moldova, with a particular focus on cybercrimes. By examining Articles 260, 237, 259, 260^{1}-260^{3}, 260^{5}, and 260^{6}, the author seeks to identify and discuss the legal and interpretative challenges that arise when these offenses are committed concurrently. It also attempts to clarify the impact of these concurrencies on determining penalties and resolving strategies, providing comparative perspectives and recommendations for improving current legislation. Through this analysis, the goal is not only a better understanding of the dynamics of cybercrimes within the legal framework of the Republic of Moldova, but also to formulate concrete suggestions for clarifying and enhancing the legal responses to these complex challenges.

In the legal landscape of the Republic of Moldova, the clear articulation of criminal legislation is essential for the effective and fair application of justice. Article 33 of the Criminal Code of the Republic of Moldova establishes the legal basis for understanding and managing the concurrence of offenses, a crucial aspect in cases where a single person commits multiple offenses before being definitively convicted for any of them. Thus, Article 33, paragraph (1) of the Criminal Code of the RM, clearly clarifies the conditions under which a concurrence of offenses is considered to have occurred: "*A concurrence of offenses is considered to be the commission by a person of two or more offenses if the person has not been definitively convicted for any of them and if the statute*

of limitations for criminal liability has not expired, except in cases where the commission of two or more offenses is provided in the articles of the special part of this code as a circumstance that aggravates the punishment" [1]. This definition is essential for understanding how to approach multiple criminal acts committed by the same person and reveals the complexity of legal interpretation in cases of concurrent offenses.

This regulatory framework not only legally defines the concurrence of offenses but also highlights the need for careful consideration regarding the sanctioning of such situations, particularly in the context of rapid technological evolution. The complexity of concurrent offense cases becomes even more pronounced in the digital age, where criminal acts can be facilitated or masked through the use of advanced technologies.

The impact of technology on criminal legislation becomes increasingly evident as technological innovations continue to advance rapidly. In the context of concurrent offenses, these innovations significantly influence the interpretation and application of laws, presenting unique challenges in adapting the existing legal framework to effectively respond to cybercrimes.

A crucial aspect is how technology facilitates the simultaneous commission of multiple, often interconnected offenses. For instance, complex cyber attacks, such as those involving ransomware, can simultaneously violate laws concerning unauthorized access to information systems and bank fraud. These actions, carried out through a single remote command, can have multiple implications, forcing legislators to reevaluate definitions and punishments to reflect the unified and complex nature of the attacks.

Furthermore, the proliferation of internet-connected devices introduces new challenges. These devices provide new access points for criminals, creating scenarios where vulnerabilities in a single device can be exploited to affect entire infrastructures, thus highlighting the need for a more holistic approach to cyber security in criminal legislation.

Additionally, the use of artificial intelligence (AI) and algorithms for committing or preventing crimes stimulates debates over criminal responsibility. When AI is involved in the commission of offenses, determining the actual perpetrator becomes a complex legal issue, which may necessitate a reevaluation of notions of intent and culpability in the context of concurrent offenses.

According to R.Cojocaru, "The offenses that constitute concurrence can be materialized through both typical forms of criminal activity (consummated offense), and atypical forms (preparation or attempt of an offense). From this perspective, it is irrelevant whether the perpetrator had the same role or different roles (author, organizer, instigator, or accomplice) in committing the offenses" [2].

In analyzing the qualification process of concurrent offenses, it is crucial to understand how the law is applied in practice. As highlighted in the specialized literature.

Exploring in detail the applicable legislation and theoretical complexities of concurrent offenses, it is essential to return to the practical reality of how these laws are enforced in the courts. An illustrative example that highlights these challenges, as well as potential errors in the application of the law, is the case of Bulgarian citizens M.V., V.D., and K.P., involved in banking fraud operations. This case provides us an opportunity to examine how the preparation of offenses intersects with their actual commission and how different stages of criminal activity are treated under the Criminal Code of the Republic of Moldova. A detailed analysis of this case will help us better understand not just the specific application of Articles 260 and 237, but also the broader implications of Article 26 regarding the preparation of offenses.

In July 2014, M.V., V.D., and K.P., citizens of the Republic of Bulgaria were involved in a scheme to install skimming devices in ATMs (Automated Teller Machines, commonly known as cash machines) across the Republic of Moldova, aiming to steal information from users' bank cards. Their actions were classified under art. 46 and 260; art. 46 and art. 259 par. (2) letters b), e), h); art. 26, 46 and art. 237 par. (2) letters c), d) of the Criminal Code of the RM [3].

The importance of preparation in this case is underscored by invoking Article 26 of the Criminal Code, which defines the preparation of an offense as "establishing the plan of the offense or creating conditions for its commission". According to this article, M.V. and his accomplices were involved not only in committing the actual offenses, but also in preparing them by procuring and installing skimming devices.

In the legal context, it is essential to differentiate between preparatory actions and substantive acts, which are integral parts of committing the offense. In this case, the importation of skimming devices constitutes an active part of executing the criminal plan, surpassing the preparation stage which involves planning and logistical organization. This distinction is crucial for the correct application of the law, avoiding overlapping charges and ensuring that each stage of the criminal plan is judged appropriately.

Similarly, in the context of concurrent offenses and the specific application of legal articles, it is vital to understand that each offense requires a clear demonstration of intent and preparation. A. Pareniuc and A. Ghimpu describe the first step in a cyber attack as "*researching the computer system to obtain important information that can be used in the attack*" [4, p. 57]. This perspective is crucial in analyzing the case of the Bulgarian citizens accused of installing skimming devices, as it underscores the necessity of having concrete evidence that the defendants took specific preparatory steps, rather than acting randomly.

To convincingly establish the preparation for the offense of illegal access to a computer system, according to Article 259, it would be necessary to demonstrate that M.V., V.D., and K.P. had prior knowledge about the specific types of ATMs they intended to target. Such details not only show meticulous planning, but are essential to differentiate between a prepared act and an opportunistic attempt. In cases where preparation is involved, it is expected that the defendants would have previously identified which ATMs are susceptible to attacks and would have had detailed knowledge about their security systems.

The need to demonstrate specific and deliberate knowledge can also depend on how evidence is gathered and presented. In some legal situations, demonstrating such prior knowledge can be decisive in determining the severity of the charges and the penalties applied. This illustrates how important it is for prosecutors and lawyers to be meticulous in collecting and presenting evidence that supports each aspect of the charge in cases of concurrent offenses.

Thus, in the case mentioned above, the court applied separate penalties for each offense, reflecting the seriousness of their actions. This case illustrates the legal complexity in cases of actual concurrent offenses, where the preparation and execution of the offenses are closely linked and require careful assessment by the courts.

This analysis reveals how the preparation of offenses can complicate the interpretation and application of the law, especially in the case of advanced technological and transnational crimes. Discussing this case underscores the need for legislative clarifications and the improvement of authorities' training to effectively manage the technological and legal complexities of modern crimes, while ensuring that the distinction between different phases of the crime is clear and well-founded.

Furthermore, in analyzing the qualification process of concurrent offenses, it is crucial to understand how the law is applied in practice. As highlighted in the specialized literature, "The basic rule in qualifying concurrent offenses resides in the fact that the person authorized with the application of criminal law, implicitly with the qualification of offenses, will indicate in the procedural-legal document (the order to initiate criminal prosecution, the order of indictment, the indictment, the conviction sentence) all the articles, as applicable, paragraphs, letters from the special part of the Penal Code that incriminate the specific criminal acts committed that are in concurrence, and in the case of uncompleted offenses or those committed in participation, the norms from the general part of the Penal Code" [5, p.23].

If we talk about an actual concurrence of offenses, we could use, for example, the situation where an offender initially developed malicious software to manipulate the computer systems of a financial institution, an action that falls under the provisions of Article 260 of the Penal Code of the RM. Subsequently, the same offender used this software to alter the financial data of customers and redirect funds to their accounts, according to Article 260^6 of the Penal Code of the RM, which defines computer fraud. These two offenses, although connected by their method and objective, are treated as separate acts within the legislation, each with its specific involvement in the criminal scheme. This situation illustrates how separate, though interconnected, activities can constitute a real concurrence of offenses, with each offense being punished according to its specifics.

For the existence of an actual concurrence, the size of this interval does not matter, that is, the duration of time that has passed between the commission of the concurrent offenses. It is important that this time interval between the commission of the two offenses is not equal to the statute of limitations prescribed for the respective offense. In this case, if there are only two offenses in concurrence, we can no longer speak of a concurrence, there being only a single offense [6, p.234].

Similarly, it is worth noting that according to D. S. CIKIN: "A variety of the single offense is the offense which, as a result of the change in the perpetrator's intention, has transformed into another offense, usually more dangerous from a social viewpoint. In this case, the committed acts must be qualified based on the article of the Special Part of the Penal Code that provides for the liability for the more dangerous offense committed" [7, p.10].

The concurrence of offenses is crucial in cases involving advanced technologies, where seemingly independent actions can contribute to a combined criminal outcome, such as the use of illegal software for bank fraud and unauthorized access to personal data. In the USA, the concept of concurrence of offenses is treated in two main forms: actual concurrence (committing multiple offenses through separate acts) and formal concurrence (multiple offenses committed through a single act). For example, committing hacking to illegally access information and using this information for financial fraud can be treated as a formal concurrence of offenses. For instance, in the case of computer crimes:

Actual Concurrence: According to Title 18, Section 1030 ("Fraud and related activity in connection with computers"), committing separate acts involving unauthorized access to computers and the illegal use of obtained information can constitute separate offenses. If an individual commits hacking to illegally access a system and then separately commits financial fraud using the obtained data, this could be considered an actual concurrence of offenses.

Formal Concurrence: The same title and section mentioned above can be applied in a context of formal concurrence, when a single action, such as a cyber attack that simultaneously exposes confidential information and causes material damage to a company, commits multiple offenses through the same conduct [8].

To clarify how the concurrence of offenses is addressed in European countries, we can take the example of Germany, where criminal legislation provides specific treatments for offenses related to malicious software. In Germany, the Penal Code (Strafgesetzbuch – StGB) regulates offenses related to malicious software, such as the distribution of computer viruses. Offenses related to unauthorized access to information (paragraph 202a StGB), data damage (paragraph 303b StGB), and computer sabotage (paragraph 303b StGB) are strictly treated. If a person, using a single act, commits multiple offenses, such as unauthorized access to a computerized system and using this access to install malicious software that damages data, these actions will be treated as an ideal concurrence of offenses. This means that the respective action or inaction meets the elements of several separate offenses [9].

Reflecting on the concept of ideal concurrence of offenses, we observe that it involves a

complex legal situation where a single action or inaction of an individual fulfills the constitutive elements of several different offenses. As stipulated in Art.33, para.(4) of the Penal Code of the RM: "Ideal concurrence exists when a person commits an action (inaction) that meets elements of several offenses", demonstrating the intersection and overlap of legal norms [1]. This interpretation not only highlights the direct applicability of criminal law, but also opens the discussion on how various branches of law can interact in evaluating and sanctioning such cases.

To deepen the understanding of the ideal concurrence of offenses, we can consider the case of a programmer who develops malicious software intended to commit cybercrimes, simultaneously violating Art. 260 and Art. 185^1 of the Criminal Code of the RM. This programmer, by creating and distributing the software, not only facilitates the commission of cybercrimes, but also violates the copyright of the source code used without permission.

Through this single action of development and distribution, the perpetrator fulfills the constitutive elements of both offenses: Art. 260 of the Criminal Code which penalizes the production and distribution of technical means intended for the commission of cybercrimes; and Art. 185^1 par. (1) letter a) of the Criminal Code of the RM, which sanctions the unauthorized reproduction and use of works protected by copyright. This example illustrates the complexity and legislative interdependence between technological offenses and intellectual rights, underscoring the need for a careful and integrated judicial approach that simultaneously reflects the aspects of computer law and intellectual property within the same legal framework.

The distinction between ideal and actual concurrence is relevant in terms of evaluating the dangerousness of the offender, as generally, actual concurrence indicates a higher social danger than formal concurrence of offenses [10, p.378-379].

Returning to the discussion on artificial intelligence (AI), it is important to emphasize the complexity that this technology brings to the application of laws concerning the concurrence of offenses. Its use in committing offenses, particularly in the context of Art. 260 of the Penal Code of the RM, which refers to the illegal production, import, and distribution of malicious software, presents complex opportunities for committing an ideal concurrence of offenses. In the digital age, AI can facilitate the automation and escalation of cybercrimes, leading to situations where a single programmatic action can meet the criteria for multiple offenses simultaneously.

For example, a program developed with AI to penetrate security systems can simultaneously commit unauthorized access to information (Art. 259 of the Criminal Code), manipulate data (Art. 260^2 of the Criminal Code), and disrupt the operation of a computer system (Art. 260^3 of the Criminal Code of the R.M.). This is a classic example of ideal concurrence, where a single action – the launch of malicious software – fulfills the elements of several offenses.

The use of AI in committing offenses underscores a crucial challenge: determining culpability. When AI is programmed to perform actions that violate the law, we must explore not only who created or operated the software, but also how current laws can be adapted to address these new forms of criminality.

A critical aspect is how a person can instruct AI to carry out potentially harmful actions without explicitly specifying the nature of the offense. For instance, suppose a person commands an AI system to "optimize profits" for a company by any means necessary. Without clear ethical or legal parameters, the AI might decide to implement illegal strategies, such as manipulating financial data or accessing confidential information without authorization.

This raises serious questions about legal responsibility: who is to blame when AI commits an offense in the absence of a direct and explicit command? Is it the responsibility of the person who configured the AI without setting clear legal limits, or should we look at the creators and operators of the technology for the way they allowed the AI to act independently?

The European Commission also highlights how AI, by its complex and autonomous nature, can intensify the challenges related to the application and interpretation of existing laws in the

context of cyber offenses, which is directly relevant to the discussion on multiple offenses and the concurrence of offenses. In particular, the European Commission document on artificial intelligence emphasizes the need for a consolidated European approach to ensure that the development and implementation of AI align with European values, respecting fundamental rights, including data protection and privacy. It proposes a regulatory framework to manage risks associated with AI, including aspects related to transparency, human oversight, and the reliability of the technology. These concerns are essential when discussing the use of AI in committing offenses, whether it's about producing malicious software or exploiting computer systems in an unauthorized way [11].

Continuing this analysis, it is crucial to develop a legislative framework that can effectively manage not only the technical aspects of crimes committed with the help of AI, but also their ethical and moral implications. This includes revising the notions of intent and action within a legal framework, reflecting the fact that AI can act independently of direct human commands.

Thus, advancing the understanding and regulation of AI's influence on criminality requires a multidisciplinary approach, involving experts from legal, technological and ethical fields. This would help create a justice system adapted to the realities of the 21st century, capable of responding to both current and future technological challenges.

At the same time, in an era defined by rapid technological advances and increasing complexity of crimes, lawyers, prosecutors and judges will face significant challenges in managing cases of concurrent offenses. This reality necessitates a reassessment of how legal professionals are trained and continuously educated to effectively respond to these cases.

Integrating emerging technologies into the legal education curriculum becomes essential. Legal practitioners must not only be familiar with legal principles, but also competent in using data analysis tools and artificial intelligence. These tools are vital for analyzing patterns of criminal behavior and efficiently managing digital evidence, which are increasingly prevalent in modern litigation.

Moreover, a multidisciplinary approach in legal education that combines legal expertise with knowledge of computer science, criminology and ethics is crucial. This not only enriches the understanding of the context in which crimes are committed, but also ensures that legal decisions are informed and adapted to contemporary realities.

These changes in legal training are imperative to ensure that the justice system remains efficient and relevant in the context of rapid technological and social changes. Thus, the laws regarding the concurrence of offenses, as well as their interpretations, must constantly evolve to reflect new challenges, ensuring that justice is administered with integrity and full knowledge.

Bibliographical references:

1. Criminal Code of the Republic of Moldova. No. 985-XV of 18.04.2002 Republished. In: Official Monitor of the Republic of Moldova, 14.04.2009, No. 72-74/195, Official Monitor of the R. Moldova, 13.09.2002, No. 128-129/1012.
2. Cojocaru, R. Defining features and forms of concurrence of offenses according to the Penal Code of the Republic of Moldova [Trăsăturile definitorii şi formele concursului de infracţiuni potrivit codului penal al Republicii Moldova]. In: Scientific Annals of the "Ştefan cel Mare" Academy of the Ministry of Internal Affairs of the Republic of Moldova: Legal Sciences [Anale ştiinţifice ale Academiei „Ştefan cel Mare" a MAI al RM: ştiinţe juridice], XI(2), p. 15-20. 2011. ISSN: 1857-0976. Available: https://ibn.idsi.md/sites/default/files/imag_file/5.Trasaturile%20definitorii%20si%20formele%20concursului%20de%20infractiuni.pdf (Accessed: 06.04.2024).
3. Decision of the Criminal College of the Chisinau Court of Appeal from 15.06.2015. Case No. 1a-805/2015. Available: https://cac.instante.justice.md/ro/pigd_integration/pdf/87ea8f58-4316-e511-b888-005056a5d154 (Accessed: 06.04.2024).

4. Pareniuc A., Ghimpu A. Types and methods of committing informational offenses [Tipurile şi metodele de săvârşire a infracţiunilor informaţionale]. In: Law and Life [Legea şi Viaţa], No. 1-2, p. 54-60. 2021. ISSN 2587-4365.
5. Martin D., Copeţchi S. Qualification of the concurrence of offenses. Part I [Calificarea concursului de infracţiuni. Partea I]. In: National Law Review [Revista Naţională de Drept], No. 1, p. 23-28. 2015.
6. Dongoro, V., Kahane S., Oancea I., Fodor I., Iliescu N., Bulai C., Stănoiu, R. Theoretical explanations of the Romanian Penal Code. General Part, Vol. I, 2nd Edition [Explicaţii teoretice ale codului penal român. Partea generală, vol. I, ediţia a II-a]. Bucharest: Romanian Academy and ALL BECK Publishing. 2003.
7. Чикин, Д.С. Complex single crimes: criminal-legal characteristics, problems of qualification, and legislative Construction [Сложные единичные преступления: уголовно-правовая характеристика, проблемы квалификации и законодательного конструирования]. Dissertation Abstract for the Degree of Doctor of Legal Sciences. Krasnodar. 32p. 2013.
8. The United States Code, Title 18, Section 1030. Available online: https://uscode.house.gov/view.xhtml?req=(title:18%20section:1030%20edition:prelim) (Accessed: 04.04.2024).
9. Penal Code of Germany (Strafgesetzbuch – StGB). Available: https://www.gesetze-im-internet.de/englisch_stgb/ (Accessed 04.04.2024).
10. Hotca M.A. Penal Code. Comments and explanations [Codul penal. Comentarii şi explicaţii]. Bucharest: C.H. Beck Publishing. 2007.
11. White Paper on Artificial Intelligence: a European approach to excellence and trust. Published 19.02.2020. Available: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en (Accessed: 01.04.2024).