SARA **L**aw **R**esearch **C**enter
International **J**ournal of **L**egal and **S**ocial **O**rder, https://www.ccdsara.ro/ijlso
ISSN 2821 – 4161 (Online), ISSN 2810-4188 (Print), ISSN-L 2810-4188
N°. 1 (2026), pp. 1-9

CONFISCATION OF THE PROCEEDS OF CRIME IN CASES INVOLVING VIRTUAL ASSETS

V. COMAN

Received 25.05.2026; accepted 17.08.2026
First online publication: 19.08.2026
DOI: https://doi.org/10.55516/ijlso.v6i1.318

Vasile COMAN
PhD Candidate, Faculty of Law, Titu Maiorescu University of Bucharest
Cluj Court of Appeal – Criminal Division and Division for Juvenile Cases
E-mail: *v.comann@yahoo.com / vasile.coman@just.ro*
ORCID ID: https://orcid.org/0009-0006-9225-2310

Abstract *In the context of the increasing prevalence of cyber and financial crime, technological advancements and the emergence of virtual assets such as cryptocurrencies, tokens, and non-fungible tokens (NFTs) have generated new challenges for criminal law, particularly with regard to the confiscation of the proceeds of crime. The decentralized nature of these assets, the anonymity of transactions, and the volatility of their value significantly hinder the identification, seizure, and recovery of assets obtained through illicit means.*

The paper examines a number of conceptual, substantive criminal law, and procedural difficulties related to the application of precautionary measures and special confiscation as regulated by the Criminal Code and the Criminal Procedure Code, in light of the specific characteristics of digital assets, with reference also to relevant European legislation. It addresses issues such as the localization of virtual assets within the legal sphere, the identification of the beneficial owner of a digital wallet, international judicial cooperation in cross-border cases, and the challenges associated with the enforcement of confiscation measures.

At the same time, the paper highlights the risks of inefficiency in combating cybercrime from the perspective of confiscation, as well as the need to adapt the legal framework to emerging technological realities, with a view to identifying a balanced approach between safeguarding the public interest and strengthening confidence in the ability of the criminal justice system to respond effectively to new forms of digital criminality.

Key words: *confiscation, cybercrime, virtual (digital) assets, precautionary measures.*

INTRODUCTION

The digital transformation of the global economy has brought about significant changes in the structure and dynamics of legal, financial, and commercial relations. The emergence of technologies based on distributed ledger technology (DLT) and the development of virtual assets have opened a new chapter in the circulation of economic value, in which traditional notions of ownership and transfer are being reconfigured. Cryptocurrencies, digital tokens, and other instruments derived from blockchain technology constitute not only technical innovations, but also entities with substantial legal potential, capable of concentrating economic value outside regulated financial circuits.

This decentralization of financial infrastructures has generated benefits such as increased efficiency, technological transparency, and the democratization of access to investment; at the same time, however, it has amplified risks of a criminal nature. The absence of a centralized intermediary and the pseudonymous character of transactions facilitate the emergence of complex forms of cyber and economic crime, such as money laundering through cryptocurrencies, cyber fraud, digital tax evasion, or the financing of terrorism through virtual instruments. By virtue of their transnational character and the volatility of the digital environment, these criminal manifestations place considerable strain on traditional mechanisms of investigation, prosecution, and recovery of the proceeds of crime.

In this context, the confiscation of assets derived from criminal conduct becomes not merely an instrument of repression, but also a guarantee of the effectiveness of criminal policy and of the protection of the economic public order. However, the application of such measures to virtual assets gives rise to unprecedented conceptual and technical challenges, which call for a reassessment of traditional paradigms of substantive criminal law and criminal procedure. From determining the legal nature of virtual assets to identifying their location and beneficial owner, the criminal justice system is confronted with an urgent need to adapt to the realities of a digitalized economy, in which the boundaries between legality, anonymity, and illegality are increasingly difficult to delineate.

The evolution of digital environments has redefined the notion of "public security," extending it beyond physical and institutional boundaries into a virtual space in which economic stability, information protection, and trust in the financial system constitute essential components of public order. In such a context, virtual assets, by virtue of their decentralized nature and their capacity to facilitate anonymous transactions, may become instruments through which criminal activity acquires a global dimension that is difficult to control and to sanction by means of traditional criminal law mechanisms. The anonymity afforded by blockchain technology, peer-to-peer networks, or end-to-end encryption systems ensures a level of confidentiality which, while beneficial for the protection of legitimate users, simultaneously creates the premises for a grey area of non-attribution and non-identification of offenders.

This reality has direct consequences for financial security and, implicitly, for public security in its broader sense. The vulnerability of national economic systems to illicit flows of digital capital may undermine public confidence in state institutions, in the effectiveness of justice, and in the integrity of markets. At the macro-legal level, the proliferation of anonymous transactions and the inability to effectively confiscate the proceeds of crime jeopardize the preventive and coercive functions of criminal law, thereby affecting the balance between economic freedom and the legal order. The confiscation of such assets, where they constitute the result of criminal conduct, becomes a strategic instrument for restoring legality and strengthening social trust in the mechanisms of the rule of law. From this perspective, the legal challenges associated with the identification, seizure, and recovery of virtual assets transcend the narrow interest of law enforcement, being integrated into a broader framework of public interest protection, financial stability, and the defense of the fundamental values of the democratic order.

The central objective of the present study is to analyze, from both a doctrinal and an applied perspective, the limits and challenges faced by the criminal law system when applying confiscation measures to virtual assets derived from the commission of criminal offences. In an era of digital globalization, in which economic structures are reshaped under the pressure of blockchain technology and decentralized markets, the effectiveness of traditional criminal law instruments is put to the test. The analysis seeks to highlight the tension between the repressive purpose of confiscation—namely, depriving the offender of the illicit proceeds—and the technical and legal characteristics of virtual assets, which complicate the identification, seizure, and recovery of digital property. In the absence of a physical location, a formal account holder, or a financial intermediary, the application of precautionary measures provided for by the Criminal Procedure Code becomes problematic, thereby requiring a reinterpretation of the notions of "asset," "value," and "possession" in the digital context.

I. THE CURRENT NATIONAL LEGAL FRAMEWORK

1.1. The Criminal Code (Law No. 286/2009). Special Confiscation and Extended Confiscation

From the perspective of special confiscation of assets, Article 112 of the Criminal Code *(Law No. 286/2009)* constitutes the cornerstone of the legal regime governing special confiscation, a substantive criminal law institution that reflects the legislature's intent to deprive the offender of assets involved in criminal activity, with a view to restoring the legal order and preventing the commission of further unlawful acts. This safety measure targets the asset itself, irrespective of the formal holder of the right, and does not have a retributive nature, but rather an eminently preventive and neutralizing function. In the classical conception, the object of confiscation consisted of tangible assets, identifiable within the offender's patrimony. However, in the context of the digitalization of the economy and the emergence of virtual assets, this normative framework encounters evident limits of applicability, insofar as digital assets do not fully fit within the traditional notion of "asset" as understood in criminal law.

a. The Concept of "Asset Obtained through the Commission of the Offence" [Article 112(1)(a)]

This hypothesis covers assets resulting directly from criminal activity as the proceeds of the offence. In the case of virtual assets, the difficulty lies in determining the material character of the proceeds: cryptocurrencies, tokens, or NFTs do not have a physical existence, but a purely digital one, essentially consisting of cryptographic data recorded on a distributed ledger. Recent doctrine argues that, from the perspective of economic and legal functionality, a virtual asset may be assimilated to a patrimonial asset capable of confiscation, since it meets the requirements of economic value and titularity, the possession of the private key being equivalent to control over the asset. Consequently, even though their intangible nature runs counter to the classical paradigm of tangible property, cryptocurrencies may be subject to confiscation under Article 112(1)(a), insofar as they are obtained through the commission of a criminal offence, for example in cases of cyber fraud, ransomware attacks, or data trafficking.

b. Assets Used or Intended to Be Used for the Commission of the Offence [letters (b)–(c)]

With regard to virtual assets, this hypothesis may apply to digital wallets, trading accounts, or software tools used in the commission of the offence. The practical difficulty lies in determining ownership of the asset and the degree of knowledge of the third party in possession thereof, given that many blockchain services are operated by non-resident, anonymous, or decentralized entities. The application of Article 112(1)(b) and (c) is limited in situations where the digital wallet cannot be reliably attributed to a specific person and the platform hosting it does not hold identification data in accordance with KYC (Know Your Customer) requirements. In such cases, confiscation by equivalent value, as provided for in paragraphs (3) and (5), remains the only viable option, although its effective enforcement often proves to be illusory.

c. Assets Acquired through the Commission of the Offence [letter (e)]

This provision is the most relevant for the confiscation of virtual assets. It concerns assets representing the equivalent value of the proceeds of the offence, insofar as they are not returned to the injured party. From an applied perspective, the main difficulty lies in the traceability of digital funds: unlike tangible assets, cryptocurrencies may be converted, mixed ("mixing"), or transferred between anonymous wallets within an extremely short period of time, rendering the individualization of the asset subject to confiscation almost impossible.

For this reason, a functional and extended interpretation of the notion of "asset acquired" is required, encompassing within this category the equivalent economic value of the virtual asset, even where it can no longer be individually identified (for example, through the confiscation of the monetary equivalent of lost cryptocurrencies). In such cases, the proportionality of the measure in relation to the gravity of the offence must be carefully adjusted, given that the volatility of cryptocurrency values may lead to imbalances between the actual damage and the value of the assets confiscated. Accordingly, the proportionality assessment must take into account the moment of valuation, the applicable exchange rate, and the stability of the digital market.

From the perspective of extended confiscation of assets acquired through criminal activity, as provided for in Article 112^1 of the Criminal Code, it must be noted that, in the field of virtual assets, the aim is to address situations in which the offender, through the use of modern technologies and decentralized financial structures, succeeds in concealing the proceeds of crime by fragmenting them or converting them into seemingly lawful assets. In this context, the rationale of extended confiscation becomes all the more relevant: cryptocurrencies may be rapidly converted into other forms of value (NFTs, stablecoins, tokens), transferred across jurisdictions without leaving banking traces, and stored in wallets not associated with an identifiable entity. Consequently, extending confiscation beyond the direct proceeds of the offence constitutes a necessary solution for ensuring the effectiveness of the criminal law response.

With regard to the conditions for application, the requirement of a conviction for profit-generating cyber offences is relatively easy to establish in cases involving offences such as computer fraud *(Article 249 of the Criminal Code)*, the carrying out of fraudulent financial operations, money laundering arising from such offences *(Law No. 129/2019)*, or participation in an organized criminal group *(Article 367 of the Criminal Code)*. These offences frequently generate illicit financial flows that are converted into virtual assets, for which reason extended confiscation becomes the primary instrument for recovering values concealed within the digital environment.

In this case as well, proportionality is essential and may be established through the identification of unjustified digital transactions, cryptographic wallets holding substantial amounts, or investments in NFTs and tokens lacking any genuine economic correspondence. In the applied context, the major difficulty lies in the absence of a public register of digital assets and in their value volatility, which requires an additional evidentiary effort on the part of judicial authorities in order to establish their illicit origin.

By contrast, from the perspective of the temporal scope of confiscation (paragraphs (2) and (3)), extended confiscation applies to assets acquired within a period of five years before and after the commission of the offence. In the case of virtual assets, this aspect is of particular relevance, as many cryptocurrencies or tokens may be held over long periods of time in inaccessible or anonymous wallets. Accordingly, identifying the moment of “acquisition” requires an analysis of blockchain traces, transaction histories, and successive conversions, in order to determine whether the asset is temporally linked to the criminal conduct.

At the same time, as regards the determination of the value of assets and confiscation by equivalent value, paragraphs (5) and (6) of the aforementioned article enshrine the principle of confiscation by equivalent (including partial confiscation) where the assets can no longer be identified or seized. In the case of virtual assets, the challenge lies in market volatility and the absence of centralized control, which often render the effective recovery of the asset impossible. In such circumstances, the principle of proportionality requires that the value subject to confiscation be adjusted to the level of the actual damage or to the illicit value obtained, in order to avoid a disproportionate sanction.

Likewise, from the perspective of derived assets and income obtained therefrom (paragraph (7)), there is increased relevance in relation to virtual assets capable of generating passive returns (such as staking, mining, yield farming, etc.). Under this hypothesis, not only the cryptocurrencies obtained directly from the offence are subject to confiscation, but also the interest, derivative tokens, or other assets resulting from their subsequent exploitation. This approach ensures the full confiscation of the patrimonial advantage and prevents the perpetuation of illicit gains through reinvestment within the digital ecosystem.

There are, however, inherent limits to the confiscation measure, stemming from the protection of the fundamental right to property. Accordingly, paragraph (8) introduces an essential safeguard: confiscation may not exceed the value of assets that surpass the lawful income of the convicted person. This ensures the compatibility of the institution with the principle of proportionality and with the presumption of the lawful acquisition of property, as guaranteed by Article 44(8) of the Constitution and Article 1 of Protocol No. 1 to the European Convention on Human Rights. In the context of virtual assets, the application of this safeguard becomes particularly challenging: the precise determination of the value of “lawful assets” requires the identification of legitimate sources of cryptocurrencies, which in turn entails complex technical expertise, blockchain analysis, and international cooperation.

1.2. The Criminal Procedure Code (Law No. 135/2010). Precautionary Measures

The institution of precautionary measures constitutes an indispensable procedural component for the effective implementation of special and extended confiscation, serving as the instrument through which assets liable to such measures are preserved.

The primary purpose of these measures is set out in Article 249 of the Criminal Procedure Code, namely to prevent the removal of assets from criminal proceedings, to ensure the enforcement of fines and civil compensation, and, above all, to guarantee the recovery of the proceeds of crime. In the context of the digital economy, this function acquires crucial importance: the absence of оперативе and technologically adapted measures renders the subsequent application of confiscation to virtual assets impossible, as such assets may be transferred instantaneously, fragmented, or converted..

The application of provisions governing precautionary measures to virtual assets raises specific issues, such as the significantly heightened risk of dissipation compared to traditional assets, since a digital wallet may be transferred through a single cryptographic transaction, without any possibility of subsequent reversal. The identification of the asset requires specialized technical expertise, as the prosecutor must locate the relevant blockchain address or digital wallet and establish its connection to the suspect. Consequently, in order to prevent the irreversible loss of digital assets, precautionary measures should be ordered as a matter of urgency, in some cases concurrently with cyber searches and orders for the preservation of electronic data.

Precautionary measures most often consist in the immobilization of movable or immovable property through the imposition of a seizure. Applying the classical concept of “seizure” to virtual assets requires significant adaptation, since in a decentralized environment a physical seizure cannot be effected, but only a digital one, namely, the restriction of access to the wallet through the taking of the private key, the freezing of accounts held on trading platforms, or the prohibition of transactions in relation to a specific blockchain address. In such cases, the seizure measure must be technically implemented by the entities exercising operational control over the wallet, most often exchange-type platforms, under the supervision of the judicial authority. In the absence of a clear normative basis in domestic law, prosecutors resort to an analogy with the seizure of movable property, treating the private key as an instrument of access to the economic value of the asset and, therefore, as an asset in itself, susceptible to seizure and preservation.

From the perspective of the persons subject to such measures, it should be noted that they may be ordered only in respect of the assets of the suspect or defendant (for the purposes of confiscation) or, as the case may be, of the civilly liable party (for the purposes of compensation). In cases involving virtual assets, however, the delineation between the offender's assets and those of third parties is particularly complex, since ownership of a digital wallet is not established through traditional legal instruments, but through possession of the private key. Accordingly, mere technological control gives rise to a presumption of titularity, while any third party claiming a legitimate right must rebut this presumption, which entails technical expertise and digital traceability.

In practice, the major difficulty in cases involving digital assets lies in the confidential nature of cryptographic keys, as defendants frequently challenge the measure on the grounds that disclosure of the private key would infringe the right to remain silent or would amount to indirect self-incrimination.

Difficulties also arise in the effective execution of the measure (Articles 251–253), since, in the case of virtual assets, this stage entails the seizure of devices containing electronic wallets (hardware wallets, computers, mobile phones), the extraction and secure preservation of private keys in encrypted form with the assistance of IT experts, and the recording of blockchain addresses and the approximate value of the cryptocurrencies held. The issue of valuation is particularly sensitive, given that the value of a digital asset fluctuates continuously. Article 253 requires the authority to draw up a seizure report, which must describe in detail the assets, their estimated value, and any objections raised. In the case of digital wallets, such a description must include the transaction hash, the blockchain address, and the equivalent value expressed in fiat currency.

Garnishment (Article 254) represents a form of seizure over sums owed to the defendant by third parties. In the digital environment, garnishment may target accounts held with exchange platforms or wallets managed by centralized service providers (*e.g., Binance, Kraken, Coinbase*). The difficulty lies in the transnational nature of these entities, which necessitates international cooperation and the recognition of seizure orders outside the national jurisdiction. In the absence of a rapid recognition mechanism (similar to EU Regulation 2018/1805 on freezing and confiscation orders), garnishment of virtual assets remains, in practice, difficult to enforce.

From the perspective of the restitution of items unrelated to the offence or belonging to another person, as well as the lifting of the seizure (Article 255), it should be noted that, in cases involving cryptocurrencies, restitution raises technical issues concerning the lawful transfer of a temporarily seized digital asset without losing control over it. In this regard, ensuring traceability may be achieved through the use of advanced electronic signatures applied to each component of the transaction.

In matters concerning the restoration of the prior situation (Article 256), within the digital environment such restoration entails the return of assets to victims or their reinstatement into the legitimate patrimony of the injured party through the retransfer of cryptographic funds. The practical application of this measure is limited, since blockchain technology, by its immutable nature, does not allow for the deletion or reversal of transactions. Consequently, restoration may occur only through compensatory operations, namely, equivalent transfers or restitution of value, rather than through the annulment of the original digital act.

1.3. Law No. 129/2019 on the Prevention and Combating of Money Laundering and Terrorist Financing

From the perspective of confiscating the proceeds of crime in cases involving virtual assets, a normative act of particular significance is Law No. 129/2019 on the prevention and combating of money laundering and terrorist financing, which provides the indispensable legal infrastructure for the identification, traceability, and ultimately the neutralization of illicit financial circuits. Article 1 establishes the national framework based on a “risk-based approach,” assigning the National Office for the Prevention and Combating of Money Laundering the role of financial intelligence unit and coordination hub for risk assessment. Its relevance is twofold: on the one hand, national and sectoral risk assessments generate risk maps that naturally encompass virtual asset service providers and digital payment channels; on the other hand, the obligation imposed on states and supervisory authorities to publish summaries and statistics creates a genuine feedback loop between reporting, investigation, and judicial outcomes, with a direct impact on the effectiveness of precautionary measures and confiscation. Coordination with criminal investigation bodies, sectoral supervisors (*the National Bank of Romania, the Financial Supervisory Authority, and the National Gambling Office*), and tax authorities enables operational data generated within the compliance ecosystem, including suspicious transaction reports and indicators relating to seized or confiscated assets, to serve as evidence or financial intelligence supporting the ordering of seizures, garnishments, and ultimately the confiscation of digital values that would otherwise be difficult to immobilize.

Conceptually, Article 2(c), which defines “assets” in an extensive manner, expressly includes intangible assets and instruments “in any form, including electronic or digital.” This terminological definition, originating in the AML/CFT compliance framework, also produces effects in substantive and procedural criminal law. It legitimizes the qualification of cryptocurrencies, tokens, or other digital values as patrimonial assets capable of being frozen and confiscated. In practice, the bridge between compliance law and criminal law is built precisely on this identity of object: what qualifies as an “asset” within the meaning of Law No. 129/2019 becomes, mutatis mutandis, the object of criminal seizure, while its traceability through distributed ledgers is evidentially supported by reporting mechanisms and interinstitutional cooperation established under Article 1.

The definitions set out in Article 2 also indirectly anchor the issue of confiscation by standardizing the notions of “credit institution,” “financial institution,” “business relationship,” and “occasional transaction,” which determine when and how customer due diligence and reporting obligations are triggered. To the extent that the intermediation of virtual assets is carried out through entities falling within these categories or subject to sectoral supervision, AML mechanisms generate documentary trails, KYC verifications, and alerts that may be leveraged in criminal proceedings. In other words, Law No. 129/2019 compels market actors to generate and retain data, without which precautionary measures targeting digital wallets would risk remaining purely declaratory.

Article 3, concerning politically exposed persons (PEPs), although seemingly peripheral to the issue of virtual assets, plays a substantive role in justifying enhanced due diligence measures and, by extension, in strengthening the evidentiary basis supporting confiscation. Public exposure increases the risk of corruption and the use of corporate vehicles or digital instruments to conceal the origin of funds; accordingly, the compliance pathways triggered for PEPs, their family members, and close associates generate a denser evidentiary standard. In scenarios involving extended confiscation, the fact that digital assets were accumulated in a PEP context and in disproportion to lawful income may reinforce the court’s conviction as to their illicit origin, while the existence of prior AML measures that were inadequately implemented may even ground heightened diligence obligations for intermediaries.

Perhaps the strongest connecting link between Law No. 129/2019 and the effectiveness of confiscating digital assets is Article 4 concerning the “beneficial owner.” Its definition, oriented toward ultimate control and effective ownership, allows for overcoming corporate formalism and legal constructions designed to dissipate traces, which, in the field of virtual assets, translates into identifying the natural person behind a wallet, a custodial platform, or a structure administering tokens. The quantitative and qualitative criteria (including control through other means) establish an analytical framework for correlating blockchain addresses, devices, and exchange accounts with specific individuals. In criminal proceedings, this mapping of the “beneficial owner” transforms reasonable suspicion into well-founded indications, justifies the imposition of seizure, and subsequently strengthens the basis for confiscation, including in respect of assets transferred to third parties who “should have known” that the purpose was to evade the measure.

II. RELEVANT EUROPEAN REGULATIONS.

2.1. Directive (EU) 2014/42 on the Freezing and Confiscation of Instrumentalities and Proceeds of Crime

Directive (EU) 2014/42 establishes the minimum Union framework for the freezing and confiscation of instrumentalities and proceeds of crime, and its relevance for virtual assets stems from a regulatory technique that is neutral as to the medium in which the asset exists. The definitions of "instrumentalities" and "proceeds" encompass any economic advantage and any asset capable of having patrimonial value, irrespective of whether it is tangible or intangible, thereby allowing cryptocurrencies, tokens, and other digital values to fall within the scope of such measures. A final criminal conviction may result in the deprivation of instrumentalities and proceeds, which, in the digital ecosystem, means that wallets and virtual funds derived from cybercrime or from their subsequent conversion may be confiscated as such. The practical significance is further enhanced by the possibility of confiscation by equivalent value: where a virtual asset has been mixed, converted, or transferred, the state may pursue its economic value, rather than the specific digital units themselves.

The dimension of advanced criminal policy emerges most clearly in the regime of extended confiscation. The Directive requires Member States to allow, in relation to certain profit-generating offences, the confiscation of assets whose lawful origin cannot be justified and which are disproportionate to lawful income, where a conviction has been secured for an offence capable of generating material benefit. Applied to virtual assets, this standard legitimizes the transfer into State ownership of cryptocurrencies and other digital values accumulated during the relevant periods, where the body of indications, such as on-chain flows, the absence of an economic rationale, or interposed structures, supports the conclusion as to their illicit origin. The correlation with domestic law (Article 112^1 of the Criminal Code) is evident: patrimonial disproportionality, assessed also through wallet balances and transaction histories, becomes a central evidentiary pillar for extending the measure beyond the direct proceeds of the offence.

Another essential key lies in third-party confiscation. The Directive requires the establishment of mechanisms allowing assets transferred for the purpose of evading confiscation measures to be pursued in the hands of persons who knew or ought to have known the true purpose of the transfer. In the crypto domain, where layers of interposition, custody through platforms, or wallets controlled by associates are common practices, this rule enables the effective targeting of values, provided that the requisite level of knowledge or the circumstances imposing a duty of diligence can be proven.

Within the logic of the Directive, the freezing regime plays a decisive conservative role. It involves the issuance of rapid orders by competent authorities to prevent the disposal of assets pending a decision on the merits. Although the text does not expressly refer to “digital seizure,” the standards it establishes, namely promptness, effectiveness, and the availability of judicial review, are fully applicable to wallets and accounts held on platforms. In practice, freezing translates into the restriction of the power of disposition over private keys or the blocking of transactions by intermediaries, and the Directive reinforces this objective by requiring Member States to ensure procedural instruments capable of producing real, rather than merely nominal, effects..

The safeguards provided by the right to an effective remedy, the observance of proportionality, and the protection of good-faith third parties and victims shape the application of these measures toward a balance between efficiency and fundamental rights. In the sphere of virtual assets, this requires particular attention to the valuation of assets at relevant moments, to market volatility, and to the segregation of clean funds from tainted ones, including through the use of technical expertise and blockchain analysis tools. The Directive further projects a requirement for the effective management of frozen and confiscated assets, a matter largely left to national organization; in the case of digital values, this entails institutional capacity for secure custody, controlled conversion, or disposal, so that the measure does not remain merely illusory.

Overall, Directive 2014/42 functions as a catalyst for the effectiveness of confiscation in the digital economy. Through a core set of rules governing post-conviction confiscation, confiscation by equivalent value, extension to unjustified assets, and recovery from third parties—complemented by freezing mechanisms and procedural safeguards—it provides the framework within which domestic law can operate coherently with respect to virtual assets. The technological neutrality of the text constitutes a significant advantage: defining “proceeds” as any economic advantage and “property” in patrimonial terms allows crypto-assets to be integrated without conceptual amendments, shifting the focus from the nature of the medium to the purpose of the measure—namely, the recovery of illicit gains and the protection of economic public order. To the extent that Romania aligns these standards with national instruments on seizure, beneficial ownership identification, and interinstitutional cooperation, the confiscation of the proceeds of crime in cases involving virtual assets becomes not only legally possible, but also practically achievable.

2.2. Regulation (EU) 2023/1114 (MiCA) – The Legal Definition of Virtual Assets

Regulation (EU) 2023/1114 on markets in crypto-assets[1], nown by the acronym MiCA, represents the first European normative instrument to provide a unified legal definition of the notion of a virtual asset, integrating it into the architecture of EU financial law. From this perspective, MiCA is of direct relevance for the substantive and procedural criminal law analysis of confiscation

[1] Act normativ disponibil pe https://eur-lex.europa.eu.

of the proceeds of crime, as it establishes the conceptual framework within which virtual assets acquire legal recognition and, implicitly, become capable of being subject to proprietary rights, seizure, and confiscation. Pursuant to Article 3(1)(5), the Regulation defines a "crypto-asset" as a digital representation of value or of a right that may be transferred and stored electronically, using distributed ledger technology or similar technology. This broad definition encompasses all forms of digital assets capable of being held, transferred, and valorized, without being limited to traditional cryptocurrencies. From a legal standpoint, this codification amounts to a recognition of crypto-assets as intangible goods endowed with economic value, thereby rendering them, by analogy, objects of patrimonial rights and, consequently, subject to criminal confiscation measures.

The distinctions introduced by MiCA between the different categories of crypto-assets—asset-referenced tokens, e-money tokens, and other crypto-assets—are essential for criminal law analysis, as they define not only the economic nature of the asset, but also its degree of regulation and traceability. E-money tokens are assimilated to payment instruments and are issued by supervised entities, which facilitates the application of freezing measures and cooperation with financial authorities. By contrast, asset-referenced tokens and so-called "generic" crypto-assets may be issued and traded within a less centralized framework, thereby maintaining a heightened risk of use in illicit activities and of evasion of precautionary measures. Consequently, in relation to the objective of confiscation, MiCA contributes to distinguishing between virtual assets subject to the control of an identified entity and those situated in an area of near-total decentralization, implicitly indicating the level of possible intervention by judicial authorities.

By establishing obligations of authorization and registration for issuers and crypto-asset service providers (Articles 53–59), the Regulation creates a legal chain of accountability and traceability. Service providers, including trading and custody platforms, are required to maintain records of transactions, verify user identities, and cooperate with competent authorities. From a criminal law perspective, this administrative infrastructure constitutes the practical backbone for the application of precautionary measures and the enforcement of confiscation: authorities are able to identify holders, freeze accounts, and track digital value flows in a manner comparable to the regime applicable to bank accounts. MiCA thus confers a legal status upon virtual assets which, prior to the Regulation's adoption, were governed by a plurality of fragmented national regimes, lacking the coherence necessary for the effective operationalization of criminal measures.

Defining virtual assets as digital representations of value that are transferable and storable electronically has direct implications for the criminal law concept of "property." In light of MiCA, cryptocurrencies and tokens can no longer be treated as mere computer data devoid of patrimonial content, but rather as legal entities with an economic function equivalent to that of intangible movable property. Accordingly, when obtained through the commission of an offence, such as cyber fraud, ransomware attacks, or data trafficking, they fall within the scope of special confiscation, and, in cases of unjustified accumulation, they may be subject to extended confiscation. Moreover, the transparency and compliance regime established by MiCA for issuers and service providers facilitates cooperation between criminal justice authorities and supervisory bodies, thereby reducing the risk that digital assets may be concealed under the guise of technological anonymity.

2.3. Regulation (EU) 2023/1113 (Transfer of Funds Regulation) – Traceability of Crypto-Transactions

Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets, known as the Transfer of Funds Regulation (TFR)[2], onstitutes the complementary element to the MiCA Regulation, ensuring the operational dimension of financial traceability within the digital environment. From the perspective of criminal law and confiscation measures, the TFR provides the legal foundation for the traceability of transactions involving virtual assets, transforming the principle of technological anonymity into a regulated system of responsibilities, disclosure obligations, and mechanisms of interinstitutional cooperation. The Regulation fits within the European paradigm of a "digital paper trail," requiring that each transfer of funds or crypto-assets be accompanied by identifiable information concerning the originator and the beneficiary, so that the origin and destination of value can be determined at any time by competent authorities. Implicitly, this normative framework strengthens the applicability of precautionary measures and confiscation with respect to virtual assets, as it removes the major obstacle posed by the lack of traceability.

Through Articles 14–18, the Regulation establishes the obligation for crypto-asset service providers to collect, retain, and transmit complete data on the persons involved in transactions. Each transfer must be accompanied by the name, address, date of birth, account number, and digital wallet address of both the originator and the beneficiary, and the absence of such information requires the suspension or refusal of the transaction. From a criminal law perspective, these provisions amount to an extension of customer due diligence (KYC) obligations at the technological level, ensuring the identification of both the active and passive subjects of the operation. In the context of investigations into cybercrime or money laundering through crypto-assets, these traceability requirements provide a robust evidentiary basis for establishing value flows, identifying the beneficial owner, and substantiating the imposition of seizure and confiscation measures.

Article 20 enshrines the principle of the automated identification of suspicious transactions and obliges service providers to deploy technical systems capable of detecting the absence of mandatory information and of notifying the

[2] Act normativ disponibil pe https://eur-lex.europa.eu.

competent authorities. In the sphere of criminal measures, this requirement translates into a form of preventive monitoring of the crypto market, whereby the reporting of transactional anomalies may generate suspicion reports and trigger urgent precautionary measures. Indirectly, the TFR establishes an early-warning mechanism that enables judicial authorities to act ex ante on digital funds, thereby preventing their loss through concealment or conversion into other assets. The obligation of technical compliance imposed on service providers strengthens the evidentiary value of blockchain data, providing guarantees as to the authenticity and integrity of the information collected, an aspect that is crucial for the legal validity of digital evidence.

From a doctrinal standpoint, the TFR marks a turning point in the relationship between technological freedom and the legal control of financial flows. While MiCA defines the legal nature of the virtual asset, the TFR confers upon it a dimension of mandatory financial–legal traceability, assimilating the digital wallet to a bank account for the purposes of transparency obligations. In this way, the Regulation extends the traditional logic of banking traceability to decentralized technologies, thereby making it possible to apply the same confiscation principles to digital assets.

The relevance of the TFR also extends to cross-border cooperation. The Regulation requires Member States to designate competent authorities capable of rapidly accessing information on crypto-asset transfers and of cooperating with one another in cases involving suspicions of money laundering or terrorist financing. From a criminal law perspective, this mechanism establishes the premises for the transnational tracking of digital assets, which is essential in a context where cybercrime transcends national borders and exploits multiple jurisdictions to conceal the origin of funds. The traceability ensured by the TFR thus becomes the practical complement to the confiscation measures provided for by Directive 2014/42 and by national criminal law instruments, supplying the informational infrastructure that enables the real-time identification and freezing of assets.

In an evolutionary doctrinal interpretation, the TFR achieves what classical criminal law could not guarantee, namely the effectiveness of tracking digital values within a decentralized environment. By enshrining the principle of “same risk, same rules,” the Regulation removes the technological exceptionalism of crypto-assets, subjecting them to the same transparency requirements as traditional funds. From this perspective, traceability is not merely an administrative obligation, but a condition of possibility for criminal confiscation. In the absence of the information mandated by the TFR, the State would be unable to demonstrate the link between the asset and the offence, and the confiscation measure would remain purely declaratory. Conversely, by integrating traceability into the very structure of the digital transaction, the TFR transforms the blockchain from an instrument of opacity into a tool of evidence and legal control.

III. RELEVANT CASE LAW

A case adjudicated by the Brașov Tribunal constitutes a significant jurisprudential benchmark regarding the application of precautionary measures to virtual assets, illustrating the manner in which Romanian criminal procedural law has adapted to the realities of the digital economy. In the case at hand[i], the subject of judicial review was the challenge lodged by the defendant P.B. against the prosecutor's order maintaining the precautionary seizure over a complex portfolio of cryptocurrencies, amounting to values exceeding seven million United States dollars, identified in twenty-two virtual wallets and in an account opened on the Binance platform.

The case originated in a large-scale investigation conducted by the Prosecutor's Office attached to the High Court of Cassation and Justice concerning alleged acts of voter bribery and money laundering, carried out through digital platforms and live-gifting or crypto-payment applications, in the context of the 2024 presidential election campaign. The prosecution maintained that the suspect had financed, through cryptographic mechanisms and donations made on social media platforms, the promotion of a political candidate, using funds whose origin could not be justified.

In essence, the legal issue submitted to the judge of rights and freedoms concerned whether the precautionary seizure of cryptocurrencies could be regarded as lawful and proportionate, given that, at the time of the periodic review, the criminal investigation was still at the *in rem* stage, while the defendant invoked the absence of procedural standing and the significant depreciation of the assets due to the volatility of the crypto market. The Brașov Tribunal upheld the maintenance of the measure, reasoning in a rigorous manner that, pursuant to Article 249(1) and (4^1) of the Criminal Procedure Code, as well as Article 50 of Law No. 129/2019 on the prevention and combating of money laundering, the imposition of precautionary measures is mandatory in respect of assets that may be subject to special confiscation where there are indications of the commission of money laundering offences. The court held that virtual currency, although intangible, constitutes movable property within the meaning of criminal law and is therefore capable of being immobilized, as it possesses concrete economic value and may be used as a means of transferring the proceeds of crime

From a legal standpoint, the court's reasoning rests on an evolutionary interpretation of the notion of "property" within the meaning of Article 44 of the Constitution and Article 1 of Protocol No. 1 to the European Convention on Human Rights, extending protection—and, implicitly, the legal regime of immobilization—to digital assets. This approach aligns with European case-law trends and with the principles laid down in Directive (EU) 2014/42 on the freezing and confiscation of the proceeds of crime, which enshrine a functional understanding of patrimonial value, independent of its material form.

A relevant aspect of the court's analysis concerns the manner in which it addressed the defense argument relating to the loss of value of the seized cryptocurrencies. The judge held that the volatility of virtual assets constitutes a risk assumed by the holder and cannot serve as grounds for lifting the precautionary measure, since its purpose is not the preservation of speculative value, but the prevention of concealment or dissipation of assets liable to confiscation. The court emphasized that the right to property does not entail a guarantee of economic profitability, and that market fluctuations do not undermine the proportionality or necessity of the measure imposed.

Furthermore, in response to the objection that the offence of money laundering allegedly lacked a predicate offence, the judge of rights and freedoms reaffirmed the principle of the autonomy of the money laundering offence, as established in the case-law of the High Court of Cassation and Justice (Decision No. 16/2016 of the Panel for the Resolution of Legal Questions). Accordingly, the existence of precautionary measures does not depend on the existence of a final conviction or on the identification of a specific predicate offence, but solely on the presence of reasonable indications regarding the illicit origin of the assets.

At the procedural level, the decision reaffirms the importance of Article 250^2 of the Criminal Procedure Code, which establishes the obligation of periodic judicial review of the grounds underlying precautionary measures. The court examined the proportionality of the seizure in relation to the gravity of the offences under investigation, the transnational complexity of the case, and the real risk of dissipation or concealment of the assets, concluding that the maintenance of the measure was justified in order to ensure the effectiveness of the criminal investigation. This reasoning was also grounded in the specific nature of virtual assets, characterized by high mobility and a significant degree of anonymity, which necessitate a more stringent procedural regime aimed at preventing evasion of confiscation.

From a critical perspective, the decision also highlights the limitations of the current Romanian normative framework, which lacks clear mechanisms for the management or preservation of the value of seized digital assets. The court implicitly notes that the purpose of seizure is exclusively preventive, and not to ensure the economic profitability of the asset. In the absence of specific regulations governing the administration of confiscated wallets, authorities are confronted with a dilemma between preserving the digital integrity of the asset and the potential loss of economic value due to market volatility.

In another case [ii] djudicated by the Bistrița-Năsăud Tribunal, the established facts revealed a highly sophisticated cyber fraud scheme, based on unauthorized access to computer systems and the redirection of funds to cryptocurrency wallets, intended to ensure the anonymity of the perpetrators and to conceal the origin of the funds. In essence, the injured party, D.K., was misled by unidentified perpetrators who, under the pretext of investments on a fictitious cryptocurrency trading platform, “myneocapital.io,” persuaded her to install the remote access application AnyDesk on her mobile device. Through this application, the perpetrators obtained full access to the victim’s computer system, including her online banking accounts, from which they carried out multiple fraudulent transfers to a Coinbase virtual wallet, totaling approximately EUR 30,000. In parallel, they fraudulently contracted, in the victim’s name, an online loan amounting to RON 81,860, using a falsified electronic signature and manipulated identification data in order to circumvent the bank’s verification procedures.

The acts of criminal investigation revealed that the sums withdrawn from the victim’s accounts were transferred sequentially to a multitude of accounts belonging to different natural persons, many of whom were themselves potential victims of compromised online banking accounts or of so-called “money mule” manipulation schemes. This complex transactional structure, involving the successive routing of funds to and from virtual wallets, necessitated a detailed analysis of financial flows and the correlation of technical data (IP addresses, system logs, devices used, IMEI numbers) in order to accurately establish the money trail and identify the perpetrators.

Against this factual background, the Prosecutor’s Office attached to the Bistrița-Năsăud Tribunal submitted a request based on Article 146^1(1) of the Criminal Procedure Code, in conjunction with Article 138(1)(e) of the same Code, seeking authorization to obtain data relating to financial transactions carried out through a series of bank accounts and cryptocurrency wallets, both at national and international level. The request concerned the acquisition of information regarding account turnover, transactions performed, the location of the devices involved, the identity of authorized persons, and the relevant IT logs, including data obtained from the Coinbase platform, the operator of the virtual wallet used for the suspicious transactions.

The judge of rights and freedoms granted the request, holding that the statutory conditions for authorizing the obtaining of financial data were met, given the existence of a reasonable suspicion as to the commission of the offences of computer fraud (Article 249 of the Criminal Code), fraudulent financial operations (Article 250 of the Criminal Code), and illegal access to a computer system (Article 360 of the Criminal Code). The court considered the measure to be proportionate to the restriction of the fundamental rights of the persons concerned, being justified by the transnational nature and the technical complexity of the acts under investigation. At the same time, it was held that the principle of subsidiarity was respected, as other evidentiary means would not have been capable of obtaining the same information with an equivalent degree of certainty and promptness.

In another case[iii] adjudicated by the Timiș Tribunal, the issue arose of applying precautionary measures in the context of economic and cyber offences involving virtual assets. The facts submitted for judicial review revealed a situation of considerable complexity, in which the criminal activity was carried out through a company operating on a cryptocurrency platform, with the estimated damage exceeding USD 27 million. Specifically, the defendant T.Q.K., an IT specialist with expertise in blockchain technology and a collaborator of the company X.D.A. SRL, was charged with participation in criminal activities allegedly conducted by the company's administrator together with other members of an organized group. These activities reportedly involved the misappropriation of investors' funds and the laundering of the resulting sums through their conversion into cryptocurrencies. According to the indictment, the suspicious transfers were executed from the project's official wallet to virtual wallets controlled by members of the group, through exchange platforms such as Kraken and Binance, with the aim of concealing the origin and the true destination of the funds.

The defense challenged the order issued by the DIICOT prosecutor imposing a precautionary seizure over all immovable property belonging to the defendant, up to the amount of RON 62,445,322. The defense counsel argued that the measure was excessive and unlawful, as there was no concrete evidence demonstrating that the assets originated from the offences under investigation. In support of this position, the defense emphasized the unprecedented nature of the case, describing it as the first embezzlement case involving a blockchain-based company, and asserted that the defendant had not participated in the commission of the offence, but had merely acted as an IT specialist engaged to provide technical assistance for the crypto project. It was further argued that the transactions carried out through the Kraken platform were unrelated to the alleged embezzlement and that all income obtained from cryptocurrency trading had been duly declared to the National Agency for Fiscal Administration (ANAF) and taxed accordingly.

The judge of rights and freedoms dismissed the challenge as unfounded, holding that the measure ordered was lawful, proportionate, and necessary in order to secure special and extended confiscation, as well as the enforcement of judicial costs. In its analysis, the court relied on the provisions of Articles 249 and 250^2 of the Criminal Procedure Code, according to which the prosecutor is empowered to impose seizure in order to prevent the concealment, destruction, or alienation of assets liable to confiscation, and the measure must be maintained for as long as the grounds that justified it persist. At the same time, the judge emphasized the applicability of Article 50 of Law No. 129/2019 on the prevention and combating of money laundering, which provides for the mandatory nature of precautionary measures where money laundering offences are under investigation.

The court's legal reasoning is grounded in a correct and coherent interpretation of the principle of proportionality and in the recognition of the preventive nature of seizure. The court emphasized that, at this procedural stage, the defendant's guilt is not assessed, but rather the existence of a reasonable suspicion that the immobilized assets may derive from criminal activities. Accordingly, the measure is temporary in nature, not constituting a criminal sanction, but rather a procedural instrument intended to ensure the effectiveness of the criminal investigation and the potential recovery of damage. In support of this conclusion, the court relied on the case-law of the European Court of Human Rights concerning the application of Article 1 of Protocol No. 1 to the European Convention on Human Rights, as well as Constitutional Court Decision No. 872/2015, which enshrines the eminently preventive character of criminal seizure.

The Timiș Tribunal further held that the specific features of the case, namely, the use of cryptocurrencies as a vehicle for concealing funds, justify the maintenance of the precautionary measure, given that virtual assets entail an increased risk of rapid alienation and loss of traceability. This line of reasoning is fully consistent with the principles set out in Directive (EU) 2014/42 and in Regulations (EU) 2023/1113 and 2023/1114, which impose on Member States the obligation to ensure effective measures for the identification, freezing, and confiscation of crypto-assets derived from criminal activity. The court emphasized that the traceability of cryptocurrencies and the verification of the origin of investments carried out through exchange platforms are matters pertaining to the merits of the case, to be clarified during the evidentiary phase, and do not affect the lawfulness of the preventive measures ordered in the course of the criminal investigation.

The court also clarified an important conceptual issue for judicial practice: the absence of a preventive measure imposed on the person does not exclude the necessity of ordering precautionary measures in respect of that person's assets. It was thus held that preventive measures and precautionary measures have distinct legal natures and pursue different purposes, the former targeting the person, the latter the patrimony, and that no interdependence exists between them. Through the solution adopted, the Timiș Tribunal confirms the full applicability of the legal regime governing precautionary seizure to digital assets as well, implicitly recognizing that such assets fall within the category of patrimonial property within the meaning of Articles 112 and 112^1 of the Criminal Code. The court reiterates the principle that a reasonable suspicion regarding illicit origin is sufficient to justify the ordering of immobilization measures, without it being necessary to establish the defendant's guilt at that stage.

CONCLUSION

At present, Romanian criminal law is undergoing a phase of conceptual transformation, driven by the need to assimilate virtual assets within the scope of objects subject to special and extended confiscation. This evolution does not entail a departure from the traditional paradigm of patrimonial protection, but rather a functional reinterpretation of the notion of "property," in line with the case-law *of the European Court of Human Rights and with the legal instruments of the European Union, such as Directive (EU) 2014/42, Regulation (EU) 2023/1113, and Regulation (EU) 2023/1114 (MiCA).*

The confiscation of the proceeds of crime in cases involving virtual assets faces a dual challenge: on the one hand, defining and identifying the digital asset as property susceptible to tracing, and, on the other hand, ensuring its traceability, preservation, and effective realization within criminal proceedings. The pseudonymous and decentralized nature of cryptocurrencies, the absence of a single intermediary, and the extreme volatility of their economic value generate significant practical difficulties in applying the precautionary measures provided for by Articles 249 et seq. of the Criminal Procedure Code, thereby testing the limits of the current procedural framework. Nevertheless, recent case-law demonstrates the capacity of national courts to adapt traditional mechanisms to digital realities, interpreting the notion of "property" in a broad, inclusive, and dynamic manner.

From a doctrinal perspective, it is evident that criminal law cannot remain inert in the face of technological innovation, but must actively integrate European regulations in the field of combating money laundering and terrorist financing, which impose enhanced transparency and compliance obligations on crypto-platform operators. Accordingly, National Law No. 129/2019, read in conjunction with Regulations (EU) 2023/1113 and 2023/1114, configures a new legal ecosystem in which virtual assets are treated as components of patrimony capable of being seized, confiscated, and realized. Within this framework, the principles of traceability, beneficial ownership accountability, and cross-border cooperation emerge as central pillars of modern criminal policy.

In conclusion, the confiscation of the proceeds of crime in cases involving virtual assets constitutes an emerging frontier of contemporary criminal law, situated at the intersection of technology, legal sovereignty, and the protection of patrimony. European normative developments and Romanian judicial practice converge toward the full recognition of cryptocurrencies as patrimonial assets for criminal law purposes, without the need for a radical reform, but rather through interpretative and procedural adaptation. The social purpose of confiscation, namely, the restoration of equity and the prevention of the misuse of the digital economy for criminal ends, remains unchanged, even as the instruments through which it is achieved continue to evolve. In this sense, the criminal law of the future will not be solely a law of acts and persons, but also a law of data, digital value, and responsibility within the virtual space.

At the procedural level, the technological autonomy inherent in virtual assets nevertheless generates legal difficulties, particularly with regard to the application of procedural measures. In the case of privately held wallets, judicial authorities are confronted with the fundamental obstacle of the absence of an intermediary subject upon whom obligations of cooperation or custody may be *imposed. From the standpoint of executing seizure measures, a virtual asset held in a private wallet cannot be immobilized through simple orders addressed to third parties; rather, it requires the identification and acquisition of the private key or, failing that, the blocking of the devices or IT accounts in which it is stored. Nevertheless, exclusive possession of the private key gives rise, from a criminal law perspective, to a presumption of ownership, which allows the virtual asset to be assimilated to property in the offender's possession, thereby making confiscation possible under Article 112(a) and (e) of the Criminal Code, where its illicit origin is established*

From a criminal procedural perspective, the application of measures to private wallets therefore requires a balanced approach, capable of reconciling the demands of repressive effectiveness with the guarantees of fundamental rights. The central issue in this area is that of the causal link, which must be established with legal certainty between the illicit act and the asset subject to confiscation. In the context of virtual assets, this link becomes more probabilistic than direct, being constructed through the correlation of technical indicators, blockchain addresses, hash codes, timestamps, and associated wallets, with data obtained through traditional criminal investigation. Although the evidentiary standard remains that of moral certainty, recent case-law tends to accept indirect proof, based on objective circumstances leading to the reasonable conclusion that the digital asset constitutes the proceeds of the offence, a standard borrowed from the field of money laundering. Thus, temporal correlation between the commission of the offence and the appearance of cryptocurrency flows in a wallet controlled by the offender, the absence of a lawful economic explanation, and the nature of the activity carried out may substantiate the court's conviction as to the illicit origin of the asset.

BIBLIOGRAFIE

1. Trandafir, Andra-Roxana; Zlati, George, *Virtual Currencies: Between Obtaining Data on Financial Transactions and the Adoption of Precautionary Measures in Criminal Proceedings*, **Forum Juridic**, no. 1/2022, available at www.drept.unibuc.ro;

2. Zlati, George, *Blockchain Technology, Virtual Currencies and Criminal Law*, **Penalmente Relevant**, no. 1/2021, available at www.portal.penalmente.ro;

3. Oficiul Național de Prevenire și Combatere a Spălării Banilor, *Report on the National Risk Assessment of Money Laundering and Terrorist Financing (2022)*, available at www.onpcsb.ro;

4. Directive (EU) 2014/42 of the European Parliament and of the Council on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union, available at www.eur-lex.europa.eu;

5. Regulation (EU) 2023/1114 of the European Parliament and of the Council on Markets in Crypto-assets (MiCA), available at www.eur-lex.europa.eu;

6. Regulation (EU) 2023/1113 of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets, available at www.eur-lex.europa.eu;
7. National case-law, available at www.rejust.ro.

---

[i] Brașov Tribunal – Criminal Division, *Criminal Interlocutory Decision No. 109 of 27 May 2025*, available at www.rejust.ro
[ii] Bistrița-Năsăud Tribunal – Criminal Division, *Judgment No. 25 of 24 August 2023*, available at www.rejust.ro
[iii] Bistrița-Năsăud Tribunal – Criminal Division, *Criminal Interlocutory Decision No. 57DL of 4 April 2025*, available at www.rejust.ro