HARMONIZATION OF THE ROMANIAN LEGISLATION WITH EUROPEAN POLICIES IN THE FIELD OF PREVENTION AND COMBATING MONEY LAUNDERING, IN THE FIELD OF CRYPTOASSETS

Lecturer Ph.D., Alina V. POPESCU
"Constantin Brâncoveanu" University of Pitesti, Romania
E-mail: avpalina_16@yahoo.com

Abstract: *Preventing and combating money laundering is a priority of the policies developed by the European Union in order to ensure a safe, transparent economic area and to prevent the use of certain financial instruments to disguise illicitly obtained proceeds or to finance organizations engaged in illegal activities. At the European and international level, one of the major money laundering risks identified is crypto-assets transactions, which were not covered by the legal regulations on the activities of issuing money or trading financial instruments. Activities in the crypto-assets market were not under the supervision of any national authority, and there was no registration or authorization of providers of exchange services between fiat currency and cryptoassets. In the framework of European policies, several regulations have been adopted to prevent and combat money laundering, but also to regulate the crypto-asset markets, regulations that need to be implemented in Romanian legislation.*

Keywords: *money laundering, market regulation, cryptoassets, cryptocurrency and cryptoassets exchange service providers.*
JEL Classification: *K20.*

1. General considerations

The development of regional policies to prevent and combat money laundering and terrorist financing has proven necessary as these phenomena are often transnational in nature and a national approach alone would not be effective in countering these criminal activities. In practice, international coordination and cooperation have proven to be necessary in order to achieve significant results.

A. At the international level, the Financial Action Task Force (FATF)[1] , which is the main international body in the fight against money laundering and terrorist financing. The Group was set up in 1989 by the G7[2] and issues recommendations to the states and regional bodies that are members of the organization.

Among the FATF's concerns is also to analyze the risks of the cryptoassets market to prevent and combat money laundering and terrorist financing, and the CryptoAssets Contact Group (VACG) has been set up for this purpose[3].

In 2019, the FATF developed the Guidance for a Risk-Based Approach to Virtual Assets (VA) and Virtual Asset Service Providers (VASp), which aims to explain how the FATF Recommendations on VA and VASp activities should be applied (FATF, 2019). The purpose of the guide is to help countries better understand how they should implement the FATF standards effectively and to consider the key principles underlying the FATF Recommendations that are relevant in the context of VA, such as: the objective-based

[1]The Financial Action Task Force
[2]The G7 is an international forum of the governments of economically, technologically and militarily developed countries: Canada, France, Germany, Italy, Japan, the United Kingdom of Great Britain and Northern Ireland and the United States of America,
[3]Virtual Assets Contact Group (VACG)

approach and functional equivalence, technological neutrality and future-proofing, and ensuring fair treatment of all VASp.

Both the public and private sectors should identify and assess the money laundering or terrorist financing risks that may arise in connection with:

- developing new products and new business practices, including new delivery mechanisms;
- use of new or emerging technologies for both new and existing products.

In the case of the private sector, such a risk assessment should be carried out prior to the launch of new products, business practices or the use of new or emerging technologies.

In 2020, the FATF produced the Virtual Assets Red Flag Indicators Report on money laundering and terrorist financing (FATF, 2020). These indicators have been grouped into five categories:

- Red flag indicators linked to transactions:
- Red flag indicators linked to trading patterns;
- Red flag indicators linked to anonymity;
- Red flag indicators about senders or recipients;
- Red flag indicators referring to the source of funds or wealth;
- Red flag indicators linked to geographical risks.

However, the FATF points out that these indicators are not exhaustive and are constantly evolving, so risk assessments also need to be dynamic.

In 2021, the FATF developed the Financial Proliferation Risk Assessment and Mitigation Guide. The document analyzes how virtual assets are being misused to potentially violate, fail to implement or avoid targeted financial sanctions (FATF, 2021).

The FATF notes that access to the formal financial system has become more difficult as a result of existing regulatory measures, so that various individuals and entities have used virtual assets as a means of evading internationally imposed financial sanctions. These individuals or entities, not having access to banking services, have found virtual assets attractive as they are not regulated. They used digital wallets from service providers in various countries to disguise the proceeds of various illicit activities, where transactions between cryptoassets and fiat currency could be traced and the amounts could not be recovered.

The guidance points out that identifying customer and transaction vulnerabilities is crucial to the risk assessments made by a financial or non-financial institution. At the same time, private firms should use the know-your-customer process, transaction monitoring and screening, as well as internal audit and regulatory findings. Additional sources of information may be used for risk assessment, such as: known domestic or international typologies, national risk assessments, supranational risk assessments, relevant sectoral reports published by competent authorities, relevant risk reports of other (especially neighboring) jurisdictions on their respective sectors, reports on violations of international sanctions, etc.

The paper recommends that cryptoasset service providers conduct risk assessments and prioritize among identified risks, with risk being considered as a function of threat, vulnerability and consequence. After conducting these assessments, they should track the evolution of risks, should consider adapting/calibrating/improving their policies, controls and procedures to effectively manage and mitigate the identified risks. At the same time, the guide recommends strengthening public-private cooperation.

All these documents are intended to provide practical tools for both the public and private sector in identifying, detecting and ultimately preventing criminal money laundering and terrorist financing activities involving VA.

B. At the European level, specific legislation has been adopted to prevent and combat money laundering, so that regulations are harmonized in all EU countries.

Thus they were adopted:

−Directive (EU) 2015/849 of the European Parliament and of the Council of May 20, 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015)

−Directive (EU) 2024/1640 of the European Parliament and of the Council of May 31, 2024 on mechanisms to be put in place by Member States to prevent the use of the financial system for the purpose of money laundering or terrorist financing, amending Directive (EU) 2019/1937 and amending and repealing Directive (EU) 2015/849 (OJ L, 2024/1640, 19.6.2024). The repeal of Directive (EU) 2015/849 enters into force on July 10, 2027.

−Directive (EU) 2018/843 of the European Parliament and of the Council of May 30, 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (OJ L 156, 19.6.2018,).

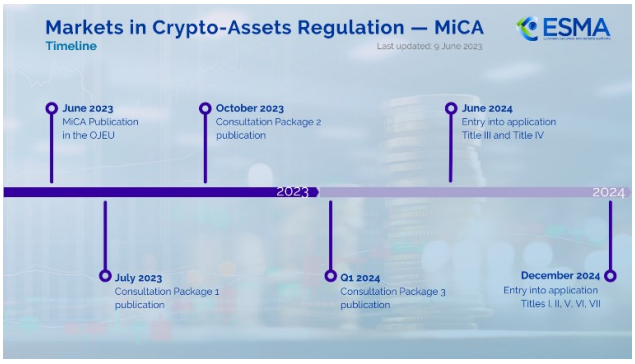
−Regulation (EU) 2023/1113[4] of the European Parliament and of the Council of May 31, 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (OJ L 150, 9.6.2023).

−Regulation (EU) 2023/1114[5] of the European Parliament and of the Council of May 31, 2023 on crypto-asset markets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (OJ L 150, 9.6.2023).

−Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing (OJ L, 2024/1624, 19.6.2024). The Regulation shall apply from July 10, 2027, except in relation to the obliged entities referred to in Article 3(3)(n) and (o), to which it shall apply from July 10, 2029.

[4]Known under the acronym MiCAR
[5]Known by the acronym MiCA

Legislation adopted is mandatory on Member States, either by direct application or by transposition.



Source: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica

2. European policies to prevent and combat money laundering

At European level, common or specific policies have been adopted under adopted legislation, by the authorities responsible for preventing and combating money laundering, which have been given powers in relation to crypto-assets.

A. The role of the European Securities and Markets Authority (ESMA), is to oversee the functioning of financial markets to ensure investor protection, identify trends, issues and risks for these markets, help coordinate national market surveillance initiatives, facilitate the exchange of best practices, provide advice to national authorities[6] on how to address the specific issues facing these markets.

ESMA is also concerned about cryptoassets market developments and interference with traditional financial markets, as well as the protection of investors in these markets, which are known to be highly volatile. In this context, in November 2017 and February 2018, ESMA has issued joint warnings on cryptoassets to alert investors to the high risks of these instruments. The Authority is also cooperating with other international bodies with concerns in this area.

In September 2020, ESMA gave its opinion on regulating the cryptoassets market to set strict requirements for cryptoasset issuers and cryptoasset service providers.

With the adoption of MiCA, ESMA has been empowered to develop technical standards and guidelines containing specific provisions. On 17.12.2024, ESMA published the Final Report (JC, 2024) "Guidelines on conditions and criteria for the qualification of cryptoassets as financial instruments", guidelines which are addressed to competent authorities and cryptoasset service providers and have a 60-day implementation deadline.

The guidelines set out compliance and reporting obligations, as well as nine guidelines on the qualification of cryptoassets as financial instruments.

On December 10, 2024, ESMA together with the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA) issued a Guideline on templates for explanations and opinions and the standardized test for cryptoassets, pursuant to Article 97(1) of Regulation (EU) 2023/1114 (MiCA Regulation) (JC, 2024). As stated in the text of the document - the Status of the Guideline - all "competent

[6]In Romania, this is the Financial Supervisory Authority

authorities, financial market participants and financial institutions should make every effort to comply with the Guideline".

The guidance aims for "a common approach for the regulatory classification of cryptoassets under the Regulation[7] respectively".

On 26.02.2025, ESMA published the Guidance[8] on procedures and policies, including customer rights, in the context of cryptoasset transfer services under the Markets in Crypto Assets Regulation (MiCA), relating to investor protection, which is addressed to competent authorities and cryptoasset service providers and has been developed in close cooperation with the EBA. The text of the document states that those to whom it is addressed should comply with this guidance.

The guidelines contain five guidelines for the actions of cryptoasset service providers, namely:

−sets out transparency obligations for cryptoassurance service providers, i.e. the information they must provide to customers before entering into a contractual relationship, in easy-to-understand language and a clear and simple form;

−establishes obligations to implement and maintain appropriate policies and procedures (including appropriate tools) on the conduct of the contractual relationship with customers (such as providing information on transaction amount, debit date, fees, charges, commissions, etc.). This information should be provided free of charge, if not provided more frequently than once a month;

−establishes obligations to implement and maintain appropriate policies and procedures regarding the cut-off times for instructions to transfer cryptoassets to be considered received on the same business day, maximum execution times depending on the cryptoasset transferred, reasonable estimates of the time interval or number of block confirmations required for the transfer of cryptoassets to be irreversible;

−establishes obligations to implement and maintain appropriate risk-based policies and procedures to determine whether and how to execute, reject, return or suspend a transfer of cryptoassets;

−establishes obligations to implement and maintain appropriate policies and procedures that set out the conditions of the cryptoasset service provider's liability to customers for unauthorized or improperly initiated or executed cryptoasset transfers.

B. The European Banking Authority (EBA, 2024), is an agency of the European Union whose role is to ensure the harmonization of the regulatory and supervisory framework for the banking sector throughout the Union in order to create an efficient and transparent single market for banking products. The EBA centrally manages information on banking supervision in the Member States in order to ensure a transparent framework of activity, financial stability and banking market discipline. The Agency promotes cooperation between national authorities and a transparent, simple and fair EU market that provides protection for consumers of financial products and services.

In the context of the regulation of the crypto-assets market, the EBA has been granted regulatory powers in relation to issuers of crypto-assets. Accordingly, on July 4, 2024, the Guidance on Information Requirements for Transfers of Funds and Certain Crypto-Assets pursuant to Regulation (EU) 2023/1113 ("Guidance on Travel Rules") was issued (EBA,

[7]MiCA Regulation
[8]ESMA 35-1872330276-2032

2024). This document contains guidance for VAsPs on how they establish procedures to detect and handle transfers of funds and cryptoassets that do not contain the required information on the payer/issuer and/or payee/beneficiary, and to ensure that these procedures are effective.

The guidance specifies what the VAsP must do to manage the risk of money laundering (ML) or terrorist financing (TF) when the necessary information on the payer, originator, payee or beneficiary is missing or incomplete.

The guidelines also issue guidance (EBA, 2024) specifying measures relating to the identification and assessment of money laundering and terrorist financing risks associated with the transfer of cryptoassets directed to or from an undisclosed address. The requirements set out in the Guideline relate to the reporting of transfers of funds and certain transfers of cryptoassets under MiCAR.

EBA has disseminated on 18.12.2024, the Guidance[9] on the templates to assist competent authorities in the performance of their duties in supervising compliance of issuers with their obligations under Titles III and IV of Regulation (EU) 2023/1114.

Competent authorities and financial institutions[10] must make every effort to comply with the guidelines, which set out compliance and reporting obligations.

3. Harmonization of the Romanian legislative framework with European policies in the field of preventing and combating money laundering

At national level, Law no. 129/2019 was adopted to prevent and combat money laundering and terrorist financing, as well as to amend and supplement some normative acts (Published in the Official Gazette of Romania, Part I, no 589 of July 18, 2019), which has undergone successive amendments in order to be brought in line with European legislation.

The most recent amendment was made by the adoption of Emergency Ordinance no. 10/2025 on amending and supplementing Law no. 129/2019 on preventing and combating money laundering and terrorist financing, as well as amending and supplementing certain normative acts (Published in the Official Gazette of Romania, Part I, no 589 of July 18, 2019).

According to the preamble of the legislative act, it transposes the amendments (Art. 38 of Regulation 2023/1113) made by Regulation (EU) 2023/1.113 of the European Parliament and of the Council of May 31, 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, which makes a number of amendments to Directive (EU) 2015/849 of the European Parliament and of the Council of May 20, 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) No. 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

The incorporation of these provisions into national law had to be completed by December 30, 2024. The transposition of EU directives is a fundamental obligation of EU Member States, and failure to comply by this date may lead to the European Commission

[9]EBA/GL/2024/16

[10]Unlike ESMA (which supervises VAsPs), the EBA supervises issuers of asset-backed tokens and e-money tokens in the crypto-assets area.

initiating infringement proceedings, followed by a referral to the Court of Justice of the European Union .[11]

The lack of this transposition led to contrary (incomplete) provisions in Law no. 129/2019 with those of the European legislation because Article 30[1] of the law referred only to the authorization of two categories of cryptoasset service providers, namely providers of exchange services between virtual currencies and fiat currencies and digital wallet providers, while MiCA establishes a broader regulatory framework for all categories of cryptoasset service providers (including issuers of cryptoassets).

With the adoption of GEO 10/2025, providers of cryptocurrency services are included in the category of financial institutions, and in the case of cross-border correspondent relationships involving the execution of cryptocurrency services, providers are obliged to adopt additional know-your-customer measures[12] , as follows:

a) determine whether the responding entity is authorized or registered;

b) collect sufficient information about the responding entity to fully understand the nature of its business and to determine, from publicly available information, the reputation of the entity and the quality of supervision;

c) to assess the controls in the area of prevention and combating money laundering and terrorist financing carried out by the respondent entity;

d) obtain senior management approval before establishing each new correspondent relationship;

e) document the responsibilities of each party to the correspondent relationship;

f) in the case of directly accessible crypto-asset accounts, ensure that the respondent entity has verified the identity of the customers who have direct access to the correspondent entity's accounts and has implemented KYC measures for these customers on an ongoing basis and is able to provide relevant KYC data to the correspondent entity upon request.

The legal requirements also stipulate that if crypto-asset service providers decide to terminate correspondent relationships, for reasons related to money laundering and terrorist financing risk management policy, they shall document and record their decision.

The regulatory act provides a reference rule to Article 3 of the MiCA on definitions:

−'*cryptoasset*' means a digital representation of a value or right that can be transferred and stored electronically using distributed ledger or similar technology

−"*cryptoasset service provider*" means a legal person or other enterprise whose occupation or business is the professional provision of one or more cryptoasset services to customers and which is authorized to provide cryptoasset services (excluding cryptoasset advisory services);

−"*cryptoasset service*" means any of the following services and activities relating to any cryptoasset:

(a) providing custody and management of cryptoassets on behalf of clients;

(b) operating a trading platform for crypto-assets;

(c) exchanging cryptoassets for funds;

(d) exchanging cryptoassets for other cryptoassets;

[11]According to the case law of the Court of Justice of the European Union, a Member State may not invoke any internal situation to justify failure to fulfill its obligations or to comply with the deadlines laid down by EU rules (preamble to the O.U.G. no. 10/2025)

[12]Art. I, point 8 of O.U.G. no. 10/2025

(e) execution of orders related to cryptoassets on behalf of clients;
(f) placement of crypto-assets;
(g) receiving and transmitting orders for cryptoassets on behalf of clients;
(h) providing advice on crypto-assets;
(i) providing cryptoasset portfolio management;
(j) providing cryptoasset transfer services on behalf of clients;

It also defines that an "*untrusted address*"[13] means distributed registry address that is not linked to either:

(a) a crypto-asset service provider;
(b) an entity which is not established in the Union and which provides services similar to those of a cryptoasset service provider.

Cryptoasset service providers are required to identify and assess the money laundering and terrorist financing risk associated with transfers of cryptoassets to or from an undisclosed address.

O.U.G. no. 10/2025, gives the Financial Supervisory Authority exclusive regulatory, supervisory and control powers[14] , regarding the application of Law no. 129/2019 on cryptoasset service providers: central securities depositories, investment firms, market operators, management companies of undertakings for collective investment in transferable securities or alternative investment fund managers applying for authorization to provide cryptoasset services, according to art. 60 of Regulation (EU) 2023/1.114.

At the same time, the competences of the National Bank of Romania regarding the exclusive powers of supervision and control, on a risk-based basis, of compliance with the provisions of Law no. 129/2019 are extended to cryptoasset service providers, which are also credit institutions or electronic money institutions and which apply for authorization to provide cryptoasset services, in accordance with the provisions of Article 60 of Regulation (EU) 2023/1.114.

Another element of legislative novelty is the repeal of Article 30^1 of Law 129/2019, which provided that authorization and/or registration of providers of exchange services between virtual currencies and fiat currencies and providers of digital wallets is required. Therefore, according to the new provisions, cryptoasset providers are only subject to regulation, supervision and control, but additional obligations are set for them and they are still required to submit suspicious transaction reports.

4. Conclusions

We can conclude that the field analyzed is a dynamic one, and legislative regulation must keep pace. Practice has shown that there is a need for continuous improvement of the legislation so that the prevention and combating of money laundering is effective and adapted to the evolution of the financial system.

The crypto-assets market is characterized by high volatility, which can affect customers, and this was the rationale behind the adoption of the new regulations.

It can be seen that the new legal act brings significant changes by broadening the notion of cryptoasset providers, defining cryptoassets and establishing national competences in the regulation, supervision and control of the cryptoasset market.

[13]By a rule of reference to Art. 3 of MiCAR - definitions
[14]Art. 1, point 12 of O.U.G. no. 10/2025

References

1. Directive (EU) 2015/849 of the European Parliament and of the Council of May 20, 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015)
2. Directive (EU) 2024/1640 of the European Parliament and of the Council of May 31, 2024 on mechanisms to be put in place by Member States to prevent the use of the financial system for the purpose of money laundering or terrorist financing, amending Directive (EU) 2019/1937 and amending and repealing Directive (EU) 2015/849 (OJ L, 2024/1640, 19.6.2024). The repeal of Directive (EU) 2015/849 enters into force on July 10, 2027.
3. Directive (EU) 2018/843 of the European Parliament and of the Council of May 30, 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (OJ L 156, 19.6.2018,).
4. EBA - Guidance on the information requirements for transfers of funds and certain crypto-assets under Regulation (EU) 2023/1113 ("Guidance on travel rules")
5. EBA - Guidance on templates to assist competent authorities in the performance of their duties in supervising compliance by issuers with their obligations under Titles III and IV of Regulation (EU) 2023/1114
6. Emergency Ordinance no. 10/2025 on amending and supplementing Law no. 129/2019 on preventing and combating money laundering and terrorist financing, as well as amending and supplementing certain normative acts
7. ESMA, Final report "Guidelines on conditions and criteria for the qualification of crypto-assets as financial instruments".
8. ESMA, EBA, EIOPA, Guidance on templates for explanations and opinions and the standardized test for crypto-assets
9. ESMA - Guidance on procedures and policies, including clients' rights, in the context of cryptoasset transfer services under the Crypto Markets Regulation
10. FATF, 2019. *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.* FATF, Paris.
11. FATF, 2020. *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets.* FATF, Paris.
12. FATF, 2021. *Guidance on Proliferation Financing Risk Assessment and Mitigation.* FATF, Paris.
13. Law no. 129/2019 on preventing and combating money laundering and terrorist financing, as well as amending and supplementing some normative acts.
14. Regulation (EU) 2023/1113[15] of the European Parliament and of the Council of May 31, 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (OJ L 150, 9.6.2023).
15. Regulation (EU) 2023/1114[16] of the European Parliament and of the Council of May 31, 2023 on crypto-asset markets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (OJ L 150, 9.6.2023).

[15]Known under the acronym MiCAR
[16]Known by the acronym MiCA

16. Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing (OJ L, 2024/1624, 19.6.2024). The Regulation shall apply from July 10, 2027, except in relation to the obliged entities referred to in Article 3(3)(n) and (o), to which it shall apply from July 10, 2029.