TERRORIST FINANCING AS THE ASSOCIATED PREDICATE OFFENCE OF MONEY LAUNDERING IN THE CONTEXT OF THE NEW EU CRIMINAL LAW FRAMEWORK FOR THE PROTECTION OF THE FINANCIAL SYSTEM

Nikola Paunović, LLM, PhD Candidate

Assistant at Ministry of Foreign Affairs of the Republic of Serbia
Kneza Milosa 24-26, Belgrade Serbia
dzoni925@gmail.com

ABSTRACT

The nexus between criminal and terrorist groups constitute an increasing security threat to the EU, especially in the area of the abuse of the financial system for the purposes of terrorist financing as the associated predicate offence of money laundering (hereinafter: terrorist financing). In that regard, Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing constitutes the main EU legal instrument not only in the context of the detection and investigation but also the prevention it from occurring. However, emerging new trends, in particular regarding the way terrorist groups finance and conduct their operations, including those related to the misuse of prepaid cards and virtual currencies, have brought to light. On the other side, it is noted that there is lack of appropriate cooperation between financial intelligence units and with law enforcement authorities, especially in the area of the access to relevant information of financial organizations on transactions involving high-risk third countries. Therefore, it became undisputed that the Directive (EU) 2015/849 should be amended. In that context, the EU has adopted on 30 May 2018 amended Directive (EU) 2018/843 so as to include the changes to Directive (EU) 2015/849. This is precisely the main reason why the first part of the paper covers the new EU rules in identifying the financial operations of terrorist networks as well as in detecting their financial backers. Furthermore, since the objective of Directive (EU) 2018/843, namely the protection of the financial system by means of prevention, detection and investigation of terrorist financing, cannot be sufficiently achieved only by the Member States with individual measures adopted by them to protect their financial systems, it seems compulsory to take into consideration significant improvements achieved in this area at international level in order to examine whether the new amended EU framework is in compliance with existing international standards. For that reason, the second part of the article deals with the international standards on combating terrorist financing, especially those made by the Financial Action Task Force. Finally, since the Republic of Serbia has, in the context of accession and negotiations process to EU, recently adopted the new framework concerning money laundering and terrorist financing, the third part of the paper is dedicated to the analysis of the national framework in this area in order to examine its compliance with EU framework. In concluding remarks, it is noted that although in the recent period there have been significant improvements in the

framework on terrorist financing and money laundering both at the international and EU level but also at the national level, there is still lack of effective implementation of adopted standards. Bearing in mind the above, some recommendations for accelerating the implementation of adopted measures on preventing terrorist financing are listed.

Keywords: *terrorist financing, money laundering, criminal law, EU, Directive (EU) 2015/849, Directive (EU) 2018/843*

1. INTRODUCTION

Recent terrorist attacks have brought to light emerging new trends, in particular regarding the way terrorist groups finance and conduct their operations.[1] Methods and techniques for acquiring funds and then using them for financing the terrorist activities have become very subtle, often unnoticeable and difficult to recognize which made it difficult to track money flows.[2] As their fund-raising activities were substantially curtailed, terrorist groups were forced to evolve and find new ways of financing their terrorist activities by creating hybrid criminal/terrorist entities with an internal system of funding, which enabled them to engage in terrorist activities in order to increase their profits. Therefore, nowadays the nexus between criminal and terrorist groups are much more complex and sophisticated and can be viewed from different aspects.[3] In this sense, in this paper firstly, it will be analyzed and discussed one aspect of that nexus concerning criminal offense terrorist financing as the predicate offense of money laundering. Furthermore, the focus will be on the new EU framework on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing as well as the international standards of the importance in this area, especially those made by the Financial Action Task Force. Finally, the relevant framework of the Republic of Serbia will be considered. To start with the link between criminal offenses of money laundering and terrorist financing and the stages through they occur.

As a specific form of organized crime, money laundering threatens all significant values of society since it encourages terrorists to engage in and expand their criminal activities. The essential feature of the money laundering process is that it is extremely changeable and adaptable to the circumstances and conditions in which it takes

1 Pedić, Ž., *Neprofitni Sektor I Rizik Od Financiranja Terorizma*, Ekonomska misao i praksa, *Vol.* 19, No. 1, p. 139

2 Manojlović, S., *Predlog zakona o sprečavanju finansiranja terorizma,* Bilten sudske prakse Vrhovnog suda Srbije, No. 2, 2006, p. 83

3 Prokić, A., *The Link Between Organized Crime And Terrorism*, Facta Universitatis, *Vol.* 15, No, 1, 2017, pp. 85-86

place.[4] Money laundering is a process of concealing the illicit origin of money or assets acquired through crime.[5] The money laundering has three essential stages. During the first stage, so-called *the investment* phase, the perpetrator breakdowns the direct link between money and the illegal activity through it has acquired, introducing the illegally acquired money into the financial system most often in the form of some legal activity in which payment is made in cash. After the money had entered the legal financial system in the second *concealment* stage it is transferred from the account to which it is placed on other accounts in order to hide the link between money and criminal activity from which it originates. Finally, in the context of the last *integration* stage, laundered money appears as money from some legal activity.[6]

The link between money laundering and terrorist financing is reflected in the fact that the second one crime could be the associated predicate offence of the first one. Precisely, financing terrorism is a preparatory action to secure or collect funds or assets, intending to be used or knowing that they can be used, in whole or in part, for the commission of a terrorist act by a terrorist or by terrorist organizations.[7] Like money laundering, terrorist financing also has several stages.[8] The first phase includes the acts of the *collection of funds* derived either from the clandestine legitimate business of the entity that is connected or even guided by terrorist organizations or individuals or from criminal activities. A significant source of these funds is donations by individuals who support the goals of terrorist organizations, as well as charities funds that raise funds and channel them to terrorist organizations. In the second phase, the collected funds are *stored* in various ways, including banks accounts opened by intermediaries, individuals or companies. The third phase is the *transfer of these funds* to terrorist organizations or individuals for operational use, through the use of fund transfer mechanisms, such as international electronic transfers between banks or money remittances, the use of charity organizations, alternative systems or money transfer networks, through couriers or smuggling over state borders. However, there are three main methods by which terrorists move money or transfer value.

---

4 Milošević, B., *Money Laundering As A Form Of Economic Crime In The Role Of Financing Terrorism*, Facta Universitatis, *Vol*. 14, No. 4, 2016, p.550

5 Važić, N. *Pranje Novca- Materijalni I Procesni Aspektu Međunarodnom I Domaćem Zakonodavstvu,* Bilten sudske prakse Vrhovnog suda Srbije, No. 2, 2008, p.121-122. See also, Cvitanović. L., *et.al.*, *Kazneno pravo- posebni dio*, Pravni fakultet Sveučilišta u Zagrebu, 2018, pp. 381-389

6 Sinanović, B., *Pranje novca,* Bilten sudske prakse Vrhovnog suda Srbije, No. 2, 2011, p.63-64

7 Bolta D., *Sprječavanje financiranja terorizma*, Policija i sigurnost, *Vol.*. 19, No. 4, 2010, p.420. Derenčinović, D., *The Review Of The Harmonisation Of The Croatian Criminal Law With International Legal Documents On Combating Terrorism*, Hrvatski ljetopis za kazneno pravo i praksu, *Vol*. 10, No. 2, 2003, p. 959; Derenčinović, D., *et. al.*, *Posebni dio kaznenog prava*, Pravni fakultet Sveučilišta u Zagrebu, 2013, p. 32. See also, Cvitanović, *op.cit.*. note 5, pp. 41-42

8 Stanković N., *Terorizam i finansiranje terorizma*, Evropski Univerzitet Brčko, Brčko, 2014, pp.63-64

The first is through the use of the financial system, the second involves the physical movement of money (for example, through the use of cash couriers) and the third is through international trade.[9] The last stage is their *use* for the activities of terrorist organizations, such as the purchase of explosives, weapons of telecommunications equipment, the support of regular cell activities, financing camps for training or paying political support and shelter in suitable countries.[10]

2. THE NEW EU CONCEPT FOR THE PROTECTION OF FINANCIAL SYSTEM FROM MONEY LAUNDERING AND TERRORISM FINANCING

Although, Directive (EU) 2015/849 of the European Parliament and of the Council[11] represents the main EU legal instrument in the prevention of the use of the Union financial system for the purposes of money laundering and terrorist financing there was some legal gaps in the area of the prevention of the use of the financial system for the purposes of terrorist financing. Therefore it became essential for EU to extend the scope of Directive (EU) 2015/849 so as to adopt amended so-called the 5th Anti-Money Laundering Directive (EU) - 2018/843 which introduces several new or upgraded rules such as: 1) lifting the rules concerning the application of certain customer due diligence measures with respect to electronic money products; 2) extending anti-money laundering and counter-terrorism financing rules to virtual currencies and traders in works of art; 3) broadening the criteria for assessing high-risk third countries and improving checks on transactions involving such countries; 4) setting up centralized bank account registers or retrieval systems; 5) enhancing the powers of EU Financial Intelligence Units as well as between financial supervisory authorities and facilitating their cooperation.[12] The 5th Anti-Money laundering Directive has been adopted and entered into force on 9 July 2018.[13] Member States

---

9 Financial Action Task Force, *Terrorist Financing*, Paris, 2008, p.21. Cmiljanić, B., *Zabrana finansiranja terorizma u svetlu međunarodnog prava i propisa Republike Srbije*, Temida No. 2, 2011, p.42

10 National Strategy on the combating of Money Laundering and the Financing of Terrorism, Official Gazette of the Republic of Serbia, No 89/08

11 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Official Journal of the European Union, L 141/73 of 5 June 2015, (hereinafter: Directive (EU) 2015/849)

12 Fahmy, M., *The Fifth Money Laundering Directi*ve, Global Risk Profile, Geneva, 2016, p.8

13 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Official Journal of the European Union, L 156/43 of 19 June 2018, (hereinafter: Directive (EU) 2018/843)

will have to implement these new rules into their national legislation by 10 January 2020.[14]

2.1. Lifting the rules concerning the application of customer due diligence measures with respect to electronic money products

First of all, the *Article 12* concerning the application of certain customer due diligence measures[15] with respect to electronic money products has been amended by lifting maximum monthly payment transactions limit as well as the maximum amount stored electronically allowed.[16] In other words, instead of the limit of EUR 250 prescribed by Directive (EU) 2015/849, amended Directive (EU) 2018/843 sets that limit up to EUR 150 (*Article 12 paragraph 1*). Precisely, *Article 12 paragraph 1* of Directive (EU) 2018/843 is amended in the following way. By way of derogation from certain customer due diligence measures and based on an appropriate risk assessment which demonstrates a low risk, a Member State may allow obliged entities not to apply certain customer due diligence measures with respect to *electronic money*, where all of the following risk-mitigating conditions are met: a) the payment instrument is not reloadable, or has a maximum monthly payment transactions limit of EUR 150 which can be used only in that Member State; b) the maximum amount stored electronically does not exceed EUR 150; c) the payment instrument is used exclusively to purchase goods or services; d) the payment instrument cannot be funded with anonymous electronic money; e) the issuer carries out sufficient monitoring of the transactions or business relationship to enable the detection of unusual or suspicious transactions. However, this derogation is not applicable in the case of redemption in cash or cash withdrawal of the monetary value of the electronic money where the amount redeemed exceeds EUR 50 (*Article 12 paragraph 2*) and not EUR 100 as it was prescribed by Directive (EU) 2015/849.[17] In the context of payments carried out with anonymous prepaid cards Member States may decide either not to accept on their territory payments carried out by using them or that credit institutions and financial institutions acting as acquirers only accept payments carried out with anonymous

---

14 Jourová V., *Strengthened EU rules to prevent money laundering and terrorism financing*, European Commission, 2018, p.2

15 Generally speaking, these measures shall comprise of: a) identifying the customer and verifying the customer's identity; b) identifying the beneficial owner and taking reasonable measures to verify that person's identity; c) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; d) conducting ongoing monitoring of the business relationship. Article 13 of Directive (EU) 2015/849

16 Fletzberger, B., *5th Anti-Money Laundering Directive – a summary of the main points*, PayTechLaw, 2018, p.3

17 Colin, N., *Adoption of fifth Anti-Money Laundering Directive*, White & Case, 2018, p. 2

prepaid cards issued in third countries where such cards meet requirements equivalent to those above-mentioned (*Article 12 paragraph 3*).[18] It could be concluded that in the context of the electronic money products the Member States should be allowed to exempt from certain customer due diligence measures, such as the identification and verification of the customer and of the beneficial owner and the assessing and, as appropriate, obtaining information but not from the monitoring of transactions or of business relationships.

2.2. Extending anti-money laundering and counter-terrorism financing rules to the providers of virtual as well as fiat currencies and traders in works of art

Secondly, in *Article 2 paragraph 1* of the amended Directive (EU) 2018/843 anti-money laundering and counter-terrorism financing framework has been extended so as to include providers of virtual as well as fiat currencies, custodian wallet providers and traders in works of art as the new obliged entities (added points g, h, i and j of the Article 2 paragraph 1 of amended Directive (EU) 2018/843 in relation to Directive (EU) 2015/849).[19] Precisely, amended Directive (EU) 2018/843 shall also apply to the following obliged entities: a) providers engaged in exchange services between virtual currencies and fiat currencies; b) custodian wallet providers; c) persons trading or acting as intermediaries in the trade of works of art, including when this is carried out by art galleries and auction houses, where the value of the transaction or a series of linked transactions amounts to EUR 10 000 or more;[20] d) persons storing, trading or acting as intermediaries in the trade of works of art when this is carried out by free ports, where the value of the transaction or a series of linked transactions amounts to EUR 10 000 or more.[21] For the purposes of this Directive, *virtual currencies* means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically. On the other side, *fiat currencies* mean coins and banknotes that are designated as legal tender and electronic money, of a country, accepted as a medium of exchange in the issuing

---

18 Internal Audit, Risk, Business & Technology Consulting, *Anticipating the Fifth EU AML Directive*, Internal Audit, Risk, Business & Technology Consulting, London, 2017, p. 3

19 Haffke, L.; Fromberger, M.; Zimmermann P., *Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and how to Address them*, pp. 9-12. Available at SSRN: [https://ssrn.com/abstract=3328064] or [http://dx.doi.org/10.2139/ssrn.3328064] Accessed 15.04.2019

20 Deloitte, *Five insights into the art market and money laundering*, Deloitte Development LLC, London, 2018, p. 5

21 Tomić S., *New EU Directive On The Prevention Of The Use Of The Financial System For The Purposes Of Money Laundering And Terrorist Financing*, Bankarstvo, *Vol.* 47, No.2, 2018, p.110

country. Finally, *custodian wallet provider* means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies (*Article 3 points 18 and 19* of the amended Directive (EU) 2018/843).[22]

2.3. Broadening the criteria for assessing high-risk third countries and improving checks on transactions involving such countries

Thirdly, the inserted rule in *Article 18a* of the amended Directive (EU) 2018/843 is focusing on broadening the criteria for assessing high-risk third countries and improving checks on transactions involving such countries.[23] According to the amended Directive (EU) 2018/843, with respect to business relationships or transactions involving high-risk third countries, Member States shall require obliged entities to apply the following *enhanced* customer due diligence measures: a) obtaining additional information on the customer and on the beneficial owner(s); b) obtaining additional information on the intended nature of the business relationship; c) obtaining information on the source of funds and source of wealth of the customer and of the beneficial owner(s); d) obtaining information on the reasons for the intended or performed transactions; e) obtaining the approval of senior management for establishing or continuing the business relationship; f) conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination (*Article 18a paragraph 1*). In addition to these measures the Member States shall require obliged entities to apply, where applicable, one or more additional mitigating measures to persons and legal entities carrying out transactions involving high-risk third countries. Those measures shall consist of one or more of the following: a) the application of additional elements of enhanced due diligence; b) the introduction of enhanced relevant reporting mechanisms or systematic reporting of financial transactions; c) the limitation of business relationships or transactions with natural persons or legal entities from the third countries identified as high-risk countries. (*Article 18a paragraph 2*).Finally, in addition to the abovementioned measures, the Member States shall apply, where applicable, one or several of the following measures with regard to high-risk third countries in compliance with the Union's international obligations such as: a) refusing the establishment of subsidiaries or branches or representative offices of obliged enti-

---

22 Keatinge, T.; Carlisle, D.; Keen, F., *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, European Parliament, Brussels, 2018, pp. 50-53

23 Council of Bars and Law Societies of Europe, *CCBE comments on the proposal of 5 July 2016 to amend Directive 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing*, Council of Bars and Law Societies of Europe, Bruxelles, 2016, p. 4

ties from the country concerned, or otherwise taking into account the fact that the relevant obliged entity is from a country that does not have adequate regimes; b) prohibiting obliged entities from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate regimes; c) requiring increased supervisory examination or increased external audit requirements for branches and subsidiaries of obliged entities located in the country concerned; d) requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned; e) requiring credit and financial institutions to review and amend, or if necessary terminate, correspondent relationships with respondent institutions in the country concerned (*Article 18a paragraph 3*). However, it should be noticed that when enacting or applying these measures Member States shall take into account, as appropriate relevant evaluations, assessments or reports drawn up by international organizations and standard setters with competence in the field of preventing money laundering and combating terrorist financing, in relation to the risks posed by individual third countries. Finally, it is prescribed that the Member States shall notify the Commission before enacting or applying these measures (*Article 18a paragraph 4 and 5*).

2.4. Setting up centralized bank account registers or retrieval systems

Fourthly, the amended Directive (EU) 2018/843 introduces the new one rule in *Article 32a* regarding setting up centralized bank account registers or retrieval systems.[24] In this sense, the Member States shall put in place centralized automated mechanisms, such as central registries or central electronic data retrieval systems, which allow the identification, in a timely manner, of any natural or legal persons holding or controlling payment accounts and bank accounts identified by IBAN and safe-deposit boxes held by a credit institution within their territory ensuring that the information held in the centralized mechanisms is directly accessible in an immediate and unfiltered manner to national Financial Intelligence Units and to national competent authorities as well in a timely manner (*Article 32a paragraph 1 and 2*).[25] The following information shall be accessible and searchable through the centralized mechanisms[26]: a) for the customer-account holder and any person purporting to act on behalf of the customer: the name, complemented by either the other identification data required under the national provisions or a unique

[24] Finn, H., *The fifth anti-money laundering and terrorist financing directive (AML 5)-Key aspects and changes* Arendt & Medernach, , Luxembourg, 2018, p. 5

[25] Fletzberger, *op.cit*., note 16, p. 4

[26] Colin, *op.cit.,* note 17, p.3

identification number; b) for the beneficial owner of the customer-account holder: the name, complemented by either the other identification data required under the national provisions or a unique identification number; c) for the bank or payment account: the IBAN number and the date of account opening and closing; d) for the safe-deposit box: name of the lessee complemented by either the other identification data required under the national provisions or a unique identification number and the duration of the lease period (*Article 32a paragraph 3*). The list is not limited since the Member States may consider requiring other information deemed essential for Financial Intelligence Units and national competent authorities (*Article 32a paragraph 4*). Anyway, the goal is set and implies that by 26 June 2020, the Commission shall submit a report to the European Parliament and to the Council assessing the conditions and the technical specifications and procedures for ensuring secure and efficient interconnection of the centralized automated mechanisms (*Article 32a paragraph 5*).

2.5. Enhancing the powers of EU financial intelligence units as well as between financial supervisory authorities and facilitating their cooperation

Finally, the amended Directive (EU) 2018/843 in the inserted *Articles 50a*, as well as, *57a* prescribe the rules concerning the facilitation of cooperation between competent authorities of the Member States and competent authorities supervising credit and financial institutions and other authorities bound by professional secrecy as well.[27] In the context of the cooperation between competent authorities of the Member States, it is not allowed to be prohibited or placed unreasonable or unduly restrictive conditions on the exchange of information or assistance between competent authorities. In particular the Member States shall ensure that competent authorities do not refuse a request for assistance on the grounds that: a) the request is also considered to involve tax matters; b) national law requires obliged entities to maintain secrecy or confidentiality, except in those cases where the relevant information that is sought is protected by legal privilege or where legal professional secrecy applies; c) there is an inquiry, investigation or proceeding underway in the requested Member State, unless the assistance would impede that inquiry, investigation or proceeding; d) the nature or status of the requesting counterpart competent authority is different from that of requested competent authority (*Article 50a paragraph 1*).

[27] Mitsilegas,V.;Vavoula,N., *The Evolving Eu Anti-Money Laundering Regime Challenges For Fundamental Rights And The Rule Of Law*, Maastricht Journal of European and Comparative Law, *Vol.* 23, No. 2, 2016, pp. 288-289

On the other side, when it comes to the cooperation between competent authorities supervising credit and financial institutions and other authorities bound by professional secrecy Member States shall require that all persons working for or who have worked for competent authorities supervising credit and financial institutions and auditors or experts acting on behalf of such competent authorities shall be bound by the obligation of professional secrecy.[28] Without prejudice to cases covered by criminal law, confidential information which these persons receive in the course of their duties may be disclosed only in summary or aggregate form, in such a way that individual credit and financial institutions cannot be identified. Abovementioned shall not prevent the exchange of information between competent authorities supervising credit and financial institutions within a Member State or in different Member States in accordance with Directive (EU) 2018/843 or other legislative acts relating to the supervision of credit and financial institutions, including the European Central Bank (*Article 57a paragraph 1 and 2*).[29] However, competent authorities supervising credit and financial institutions receiving confidential information shall only use this information: a) in the discharge of their duties under Directive (EU) 2018/843 or under other relevant legislative acts, of prudential regulation and of supervising credit and financial institutions, including sanctioning; b) in an appeal against a decision of the competent authority supervising credit and financial institutions, including court proceedings; c) in court proceedings initiated pursuant to special provisions provided for in Union law adopted in the field of Directive (EU) 2018/843 or in the field of prudential regulation and supervision of credit and financial institutions (*Article 57a paragraph 3*). It should be concluded that the goal of the amended Directive is to allow that competent authority supervising credit and financial institutions cooperate with each other to the greatest extent possible, regardless of their respective nature or status. Such cooperation also includes the ability to conduct, within the powers of the requested competent authority, inquiries on behalf of a requesting competent authority, and the subsequent exchange of the information obtained through such inquiries (*Article 57a paragraph 4*).

3. INTERNATIONAL STANDARDS FOR THE PROTECTION OF FINANCIAL SYSTEM FROM MONEY LAUNDERING AND TERRORISM FINANCING

Starting from the above-mentioned five new or upgraded rules of the 5th Anti-Money laundering EU Directive 2018/849 significant improvements achieved in

[28] Finn, *op.cit.*, note 24, p.5

[29] Jourová*, op.cit.,* note 14, p. 2

this area at international level, will be taken into consideration, especially those made by Financial Action Task Force[30] (hereinafter: FATF) since the objective of Directive, namely the protection of the financial system by means of prevention, detection and investigation of terrorist financing cases, cannot be sufficiently achieved only by the Member States with individual measures adopted by them and should be fully compliant with the FATF standards.[31]

3.1. Customer due diligence measures with respect to electronic money

First of all, when it comes to the rules concerning the application of certain customer due diligence measures with respect to electronic money it should begin from the fact that FATF standards indicate that financial institutions should be required to undertake customer due diligence measures when: 1) establishing business relations; 2) carrying out occasional transactions: a) above the applicable designated threshold (USD/EUR 15,000); or b) that are wire transfers; 3) there is a suspicion of money laundering or terrorist financing; or 4) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data. These measures to be taken are as follows: a) identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information; b) identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, this should include financial institutions understanding the ownership and control structure of the customer; c) understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship. d) conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.[32] These requirements should apply to all new customers including those who use electronic money products. However, to avoid confusion, FATF has set the distinction between electronic money and real or fiat currencies, on the one hand, and virtual or digital currencies, on the other

---

30 Schott, P., *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism*, The World Bank and The International Monetary Fund, Washington DC, 2006, p. 128; See also Borlini L.; Montanaro, F., *The Evolution Of The Eu Law Against Criminal Finance: The "Hardening" Of FATF Standards Within The EU* George Town Journal Of International Law, *Vol.* 48, 2017, p. 1011

31 Kordík, M.; Kurilovská, L., *Protection of the national financial system from the money laundering and terrorism financing*, Entrepreneurship and Sustainability Issues, *Vol.* 5, No.2, 2017 p. 243

32 The Financial Action Task Force, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation- The FATF Recommendations*, Paris, 2016, p. 14

side.[33] In that sense, e-money means a digital transfer mechanism for fiat currency since it electronically transfers value that has legal tender status, while fiat currency is the coin and paper money of a country that is designated as its legal tender and is customarily used and accepted as a medium of exchange in the issuing country. On the other side, the digital currency can mean a digital representation of either virtual currency (non-fiat) or e-money (fiat) and thus is often used interchangeably with the term virtual currency. Finally, virtual currency is distinguished from fiat currency or real currency since it is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency as digital representation of value that can be digitally traded as a medium of exchange, a unit of account and/or a store of value.[34]

3.2. Money laundering and counter-terrorism financing risks concerning virtual currencies

Secondly, in the context of the issue regarding virtual currencies, it should be noted that the development and widespread use of the Internet, personal computers, mobile devices, and related platforms and services, has had a vast impact on financial transactions.[35] The ability of new financial innovations, such as pre-paid cards and online and mobile payment platforms, to enable rapid cross-border payments presents elevated terrorist financing risks. For that reason, financial institutions should identify the money laundering as well as terrorist financing risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.[36] In that regard, in 2014, the FATF took up the specific topic of virtual currencies linking cryptocurrencies with the anonymity risks because customer identification features such as name and address are not attached to a user's Bitcoin address, and because the system has no central service provider that has oversight of transactions and can be held accountable. According to the FATF's assessment, suspicious activity may therefore not only be more difficult to detect, but the source of payments may be blurred in contrast to traditional credit or debit cards, or payment systems such as PayPal and Western Union. Since the existence of the anonymity risks in relation to cryptocurrencies, there are increasing concerns about the use of virtual currencies by terrorist orga-

---

33 Cindori, S.; Petrović, T., *Indikatori Rizičnosti Bankarskog Sektora U Okvirima Prevencije Pranja Novca*, Zbornik PFZ, *Vol.* 66, No. 6, 2016, pp. 770-772

34 Financial Action Task Force, *Virtual Currencies – Key Definitions And Potential Aml/Cft Risks- The FATF Report*, Paris, 2014, p. 4

35 Keatinge, *el.al.*, *op.cit.,* note 22, p. 21

36 Financial Action Task Force, *op.cit.*, note 32, p.17

nizations, especially with evidence of websites connected to terrorist organizations seeking Bitcoin donations or providing instructions of how to purchase weapons using Bitcoin. The report made by the FATF on terrorist financing for recruitment purposes from 2018 highlights an instance in which an ISIS propaganda through a website, whose owner is unidentified, was used to solicit donations in Bitcoin, some of which was used to pay for the site's web-hosting services.[37]

Furthermore, cases such as Liberty Reserve and Silk Road has shown that criminal organizations are already using digital currencies, not only to finance their terrorist activities but also to launder their proceeds of crime. Digital currencies have the potential to make it easier for criminals to hide the source of their proceeds and move their funds across borders without detection. However, these cases have also shown that, although difficult, the investigation of the ownership of digital currencies is not impossible since digital currency networks usually record transactions in a distributed public ledger, which can be subjected to analytical monitoring tools capable of highlighting suspect transactions.[38] In the context of the investigation, the use of virtual currencies such as Bitcoin for money-laundering purposes is going to highlight the distinction between objective elements of the crime (an act in itself, as well as objects and tools of crime) and subjective (intent, purpose, complicity, etc.). The use of virtual currency as objective elements of the criminal offence of money-laundering can be brought down to the following aspects. In terms of placement, when criminally obtained funds are introduced in the financial circulation, the procurement of the virtual currency through an exchanger may be used as a relevant element of the crime. In terms of layering (the process in which criminally derived funds are legalized and their ownership and source is disguised), the essential features of virtual currency can be brought forward as an element of money-laundering offence where the prosecution will be willing to prove the case that the virtual currency was selected precisely for these features, in order to conceal the criminal origin of funds. In terms of integration (the process by which the property legalized through layering is re-introduced into the economy), the use of virtual currency may be one of the elements, for instance, if the laundered proceeds are re-invested into the virtual currency market, this may be an additional element of offence that can be used. On the other hand, in terms of proof of intent, as a subjective element of the crime, which is an essential feature of money-laundering offences, the focus should be on the following aspects of bitcoin. Firstly, anonymity and general lack of face-to-face interaction may be a valid proof of intent to commit offence related to illegal use of virtual currencies

---

37 Keatinge, *el.al.*, *op.cit.* note 22, pp.21-23

38 International Centre For Asset Recovery, *Tracing Illegal Assets - A Practitioner's Guide*, International Centre For Asset Recovery, Basel 2015, p.115

and secondly, difficult traceability, including lack of paper/document trail could be specifically noted as an element of intent, as well.[39]

3.3. Countermeasures regarding high-risk third countries and transactions involving such countries

Thirdly, regarding the criteria for assessing high-risk third countries and improving checks on transactions involving such countries it should be noted that FATF standards point out that financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from higher- risk countries if a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing.[40] Countries should be able to apply appropriate countermeasures such as: a) requiring financial institutions to apply specific elements of enhanced due diligence; b) introducing enhanced relevant reporting mechanisms or systematic reporting of financial transactions; c) refusing the establishment of subsidiaries or branches or representative offices of financial institutions from the country concerned, or otherwise taking into account the fact that the relevant financial institution is from a country that does not have adequate systems; d) prohibiting financial institutions from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate systems; e) limiting business relationships or financial transactions with the identified country or persons in that country; f) prohibiting financial institutions from relying on third parties located in the country concerned to conduct elements of the customer due diligence process; g) requiring financial institutions to review and amend, or if necessary terminate, correspondent relationships with financial institutions in the country concerned; h) requiring increased supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions based in the country concerned; i) requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned. Finally, it should be noted that such countermeasures should be effective and proportionate to the risks.[41]

---

[39] United Nations Office on Drugs and Crime, *Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies*, United Nations Office on Drugs and Crime, Vienna, 2014, pp.85-86

[40] Financial Action Task Force, *op.cit.,* note 32, p. 19

[41] FATF Recommendation 19, [https://cfatf-gafic.org/index.php/documents/fatf-40r/385-fatf-recommendation-19-higher-risk-countries] Accessed 11.03.2019

3.4. Potential sources of obtaining the requested information on the beneficial ownership

Fourthly, in the terms of setting up centralized automated mechanisms, FATF standards prescribe that countries may choose the mechanisms they rely on to achieve the objective of having access in a timely manner, adequate, accurate and current information on the beneficial ownership and control of companies and other legal persons.[42] Potential sources of obtaining the requested information on the beneficial ownership are: a) central registries; b) other competent authorities that hold information such as tax authorities which collect information on beneficial ownership and c) other agents and service providers such as investment advisors or managers, lawyers, or trust and company service providers.[43] In that respect, competent authorities should have access to certain basic information about the obliged entities, which, at a minimum, would include information about the legal ownership and control structure of the company, including the status and powers of the company, its shareholders and its directors.[44]

3.5. Cooperation between competent authorities supervising credit and financial institutions and other authorities

Finally, in the context of the process of facilitation of cooperation between competent authorities supervising credit and financial institutions and other authorities bound by professional secrecy FATF standards made the difference between principles applicable to all forms of international cooperation and those applicable to specific forms of international cooperation such as: 1) exchange of information between Financial Intelligence Units; 2) exchange of information between financial supervisors; 3) exchange of information between law enforcement authorities; 4) exchange of information between non-counterparts. However, for both categories regarding the international principles of cooperation, the following rules are of the most relevance. Firstly, when making requests for cooperation, competent authorities should make their best efforts to provide complete factual and, as appropriate, legal information, including indicating any need for urgency, to enable timely and efficient execution of the request, as well as the foreseen use of the information requested. Furthermore, countries should not prohibit or place unreasonable or unduly restrictive conditions on the provision of exchange of informa-

---

42 FATF Recommendation 24, [https://cfatf-gafic.org/index.php/documents/fatf-40r/390-fatf-recommendation-24-transparency-and-beneficial-ownership-of-legal-persons] Accessed 11.03.2019

43 FATF Recommendation 25, [https://cfatf-gafic.org/index.php/documents/fatf-40r/391-fatf-recommendation-25-transparency-and-beneficial-ownership-of-legal-arrangements] Accessed 11.03.2019.

44 FATF Recommendation 24, [https://cfatf-gafic.org/index.php/documents/fatf-40r/390-fatf-recommendation-24-transparency-and-beneficial-ownership-of-legal-persons] Accessed 11.03.2019

tion or assistance. In particular competent authorities should not refuse a request for assistance on the grounds that: a) the request is also considered to involve fiscal matters; and/or b) laws require financial institutions (except where the relevant information that is sought is held in circumstances where legal privilege or legal professional secrecy applies) to maintain secrecy or confidentiality; and/or c) there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding; and/or d) the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart. Finally, law enforcement authorities, as well as financial supervisors, should be focused to exchange domestically available information with foreign counterparts or non-counterparts for intelligence or investigative purposes relating to money laundering, associated predicate offences or terrorist financing, including the identification and tracing of the proceeds and instrumentalities of crime.[45]

4. THE NEW NATIONAL FRAMEWORK IN AREA OF THE PROTECTION OF FINANCIAL SYSTEM FROM MONEY LAUNDERING AND TERRORISM FINANCING

Bearing in mind that the Republic of Serbia has, in 2017, adopted the new framework concerning money laundering and terrorist financing,[46] this part of the paper is dedicated to the analysis of the national framework in this area.[47] In order to examine its compliance with EU framework further remarks will focus on the five abovementioned new EU adopted or updated rules from the Directive (EU) 2018/843.[48]

4.1. Customer due diligence actions and measures as well as the exemptions from customer due diligence in relation to electronic money

To start with the rules concerning the application of certain customer due diligence measures with respect to electronic money products it should be pointed

---

45 FATF Recommendation 40, [https://cfatf-gafic.org/index.php/documents/fatf-40r/406-fatf-recommendation-40-other-forms-of-international-cooperation]. Accessed 11.03.2019

46 Law on the prevention of money laundering and the financing of terrorism, Official Gazette of the Republic of Serbia, No. 113/17 of 17 December 2017

47 See also Milošević, M., *Novi Zakon o sprečavanju pranja novca i finansiranja terorizma*, Časopis "Izbor sudske prakse", No. 3, 2018, pp. 9-13

48 Kostić, J., *Harmonizacija nacionalnog zakonodavstva Republike Srbije sa Konvencijom o zaštiti finansijskih interesa Evropske unije*, Evropsko zakonodavstvo, *Vol.* 13, No. 47/48, 2014, p. 187-202; See also Kostić, J., *Krivičnopravna zaštita finansijskih interesa Evropske unije*, Institut za uporedno pravo, Beograd, 2018, pp. 22-24

out that in line with the relevant solution of Directive EU 2018/843, the Serbian law on the prevention of money laundering and the financing of terrorism in *Article 7* prescribes that unless otherwise provided for under this Law, the obliged entity shall: 1) identify the customer; 2) verify the identity of the customer based on documents, data, or information obtained from reliable and credible sources; 3) identify the beneficial owner and verify their identity in the cases specified in this Law; 4) obtain and assess the credibility of information on the purpose and intended nature of a business relationship or transaction, and other data in accordance with this Law; 5) obtain and assess the credibility of information on the origin of property which is or which will be the subject matter of the business relationship or transaction, in line with the risk assessment; 6) regularly monitor business transactions of the customer and check the consistency of the customer's activities with the nature of the business relationship and the usual scope and type of the customer's business. However, in accordance with *Article 16* certain difference exists in the terms concerning the exemption from customer due diligence in relation to electronic money. Namely, electronic money issuers are not obliged to apply customer due diligence actions and measures if it has been established, according to the risk analysis, that there is low risk of money laundering or terrorist financing and if the following conditions are met: 1) the amount of electronic money stored on a payment instrument cannot be recharged, or there is a monthly payment limit amounting to the RSD equivalent of EUR 250 that can only be used in the Republic of Serbia; 2) the total amount of stored electronic money does not exceed the RSD equivalent of EUR 250; 3) the money stored on a payment instrument is only used for purchase of goods and services; 4) the payment instrument may not be funded by anonymous e-money; 5) an electronic money issuer monitors transactions or business relationship to a satisfactory extent which enables it to detect unusual or suspicious transactions. Notwithstanding this rules shall not be applied if there are reasons for suspicion of money laundering or terrorist financing, as well as in case of redemption of electronic money for cash or in cases of withdrawal of cash in the value of electronic money, when the amount redeemed does not exceed the RSD equivalent of EUR 100. In this sense, it should be noted that instead of the limit of EUR 250 prescribed by Directive (EU) 2015/849 and the Serbian Law, amended Directive (EU) 2018/843 sets that limit up to EUR 150. Therefore, it should be concluded that Serbian law contains the solution regarding the exemption from customer due diligence in relation to electronic money which does not include the lifting rule concerning the application of certain customer due diligence measures with respect to electronic money products as it prescribed by the amended Directive (EU) 2018/843. The following is related also to the rule which prescribes that this derogation is not applicable in the case of redemption in cash or cash withdrawal of the monetary value of the

electronic money where the amount redeemed exceeds EUR 100 according to Directive (EU) 2015/849 and the Serbian Law, while amended Directive (EU) 2018/843 sets that limit up to EUR 50.

4.2. Providers of virtual currencies as the new obliged entities

Secondly, in the matter of extended EU anti-money laundering and counter-terrorism financing framework so as to include providers of virtual currencies and traders in works of art as the new obliged entities, it should be mentioned that Serbian Law *in Article 4 point 17* recognizes as obliged entities only providers of virtual currencies defining as persons providing the services of purchasing, selling or transferring virtual currencies or exchanging of such currencies for money or other property through internet platform, devices in physical form or otherwise, or which intermediate in the provision of these services.[49] However, it should be mentioned that Serbian law does not contain any further provision which defines virtual currencies. In that regard, the Serbian law should be amended, according to the meaning of virtual currencies referred to in Directive (EU) 2018/843, since it is incomprehensible that it recognized as obliged entities persons providing the services of purchasing, selling or transferring virtual currencies, but that did not include the definition of virtual currencies in the list of terms used in the Law. Moreover, comparing to the amended provisions of the Directive (EU) 2018/843 concerning virtual currencies, Serbian Law does not recognize the term of custodian wallet provider as an obliged entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies. To conclude, it should be noted that Serbian law is incompletely harmonized with EU *acquis* in this area and in the context of *de lege ferenda* amendments it would be necessary to introduce these solutions.

4.3. Enhanced customer due diligence actions concerning the countries which do not implement international standards in the area of the prevention of money laundering and terrorism financing

Furthermore, in the context of the criteria for assessing high-risk third countries and improving checks on transactions involving such countries it should be pointed out that Serbian law in *Article 41* prescribes that when establishing a business relationship or carrying out a transaction amounting to EUR 15,000 or more, in case when a business relationship has not been established, with a customer from a country which has strategic deficiencies in the system for the prevention

[49] See also Lukić T., *Borba Protiv Pranja Novca I Finansiranja Terorizma U Republici Srbiji*, Zbornik radova Pravnog fakulteta u Novom Sadu, No. 2, 2010, p. 202

of money laundering and terrorism financing, the obliged entity shall apply enhanced customer due diligence actions.[50] Precisely, the obliged entity shall: 1) apply the enhanced customer due diligence in the manner and scope proportionate to high risk associated with having a business relationship with such customer; 2) obtain data on the origin of the property which is the subject matter of the business relationship or transaction; 3) obtain additional information on the purpose and intended nature of the business relationship or transaction; 4) conduct additional inspection of submitted identity documents; 5) undertake other additional measures to eliminate the risks. Finally, if having a business relationship with a country which has strategic deficiencies in its system for the prevention of money laundering and terrorism financing is especially risky, and competent authorities muy: 1) prohibit the financial institutions for whose registration they are relevant from establishing branches and business units in such countries; 2) prohibit the establishment of branches and business units of financial institutions from such countries; 3) limit financial transactions and business relationships with customers from such countries; 4) request financing institutions to assess, amend and, if necessary, break correspondent or similar relationships with financial institutions from such countries; 5) other adequate measures. Considering the Serbian law in relation to the application of enhanced customer due diligence actions it should be noted that it is harmonized with Directive (EU) 2018/843 in this part.

4.4. Establishing and verifying the identity of a customer or a legal person

Moreover, when it comes to the rules regarding the setting up central registries or central electronic data retrieval systems as it prescribed in the Directive (EU) 2018/843, the Serbian law does not contain a provision in that sense, although in *articles 17-26* introduces some situations for identification of any natural or legal persons. Precisely, the Serbian law prescribes the rule regarding: a) Establishing and verifying the identity of a natural person, legal representative and empowered representative (Article 17); b) Identifying and verifying the identity of a natural person using a qualified electronic certificate (Article 18); c) Establishing and verifying the identity of an entrepreneur (Article 19); d) Identifying and verifying the identity of a legal person (Article 20); e) Establishing and verifying the identity of the representative of a legal person and a person under foreign law (Article 21); f) Establishing and verifying the identity of a person under civil law (Article 23) g) Establishing and verifying the identity of a procura holder and empowered representative of a legal person, person under foreign law and entrepreneur (Article

[50] Decision On Guidelines For The Application Of The Provision Of The Law On Prevention Of Money Laundering And Financing Terrorism For Obliged Entities National Bank Of Serbia Perform Supervision [http://www.apml.gov.rs/REPOSITORY/2015_2_smernice-nbs.pdf, p.17] Accessed 11.03.2019

22) and h) Identification of the beneficial owner of a customer articles 25 and 26). In that regard, the obliged entity shall obtain the referred data by inspecting the original personal identity document with the mandatory presence of the identified person or by inspecting original or a certified photocopy of the documentation from a register maintained by the competent body of the country where the legal person or the customer has a registered office. However, in order to be fully harmonized with Directive (EU) 2018/843 the Serbian law should be amended in that manner which inserts provisions on setting up central registries or central electronic data retrieval system.

4.5. Cooperation between competent authorities supervising credit and financial institutions and other authorities

Finally, concerning the provisions on cooperation between competent authorities supervising credit and financial institutions and other authorities bound by professional secrecy, Serbian law in *Article 90* implies that the obliged entity, and/or its staff, including the members of executive, supervisory and other governing authority, as well as other persons having access to the data of content of records, must not disclose to the customer or the third party the following: 1) that the competent authority has been received information and documentation on a client or a transaction suspected of being related to money laundering or terrorist financing; 2) that the competent authority has issued an order to suspend temporarily the transaction; 3) that the competent authority has issued an order to monitor the financial operations of the customer; 4) that a procedure against a customer or a third party has been initiated or may be initiated in relation to money laundering or terrorist financing. However, this prohibition does not apply to the following situations: 1) when the data, information and documentation obtained and maintained by the obliged entity is necessary to establish facts in a criminal procedure and if such data are requested by the competent court in line with the law; 2) if the data is requested by the authority in the supervision of the implementation of the provisions of this Law; 3) if the auditing company, licensed auditor, legal or natural person offering accounting services or the services of tax advising attempt to dissuade a customer from illegal activities; 4) when the obliged entity is a part of an international group and shall apply programmes or procedures relevant for the whole group with the aim of preventing money laundering and terrorism financing and 5) when information exchange occurs between two or more obliged entities in cases related to the same customer and the same transaction, on condition that these obliged entities are from the Republic of Serbia or a third country that prescribes obligations related to the prevention of money laundering and terrorism, which are equivalent to the requirements as

prescribed by the Law, on condition that they engage in the same line of business as well as being subject to professional secrecy and personal data protection laws. Observing this solution in the context of Directive (EU) 2018/843 and comparing to the Serbian Law it is worth mentioning that Serbian Law contains a wider list of exemptions when it is allowed the use of received confidential information.

5. CONCLUDING REMARKS

Proceeds derived from or obtained, directly or indirectly, through the commission of an offence of organized criminal groups are significantly used by terrorist groups to finance their terrorist activities. In the area of prevention of money laundering and the financing of terrorism Directive (EU) 2018/843 in compliance with existing international standards, introducing several remarkable new or updated provisions and thus represents step forward strengthening EU framework on the protection of EU financial system. The only thing that remains is the need for its proper implementation. In that regard, there are a few significant recommendations for the acceleration of the implementation of adopted measures on combating money laundering and the financing of terrorism. In the area of early detection of sources of terrorist financing, the investigative focus should be on the recognition and analysis of indicators for identifying suspected money laundering and the financing of terrorism transactions especially in certain groups of obliged entities who, due to new modalities for terrorist financing, were not covered by the normative framework relating to the protection of EU financial system. This applies particularly to entities providing the services of purchasing, selling or transferring virtual currencies or exchanging of such currencies for money or other property through an internet platform, devices in physical form or otherwise, or which intermediate in the provision of these services. The next recommendation for the adequate implementation of adopted measures on preventing terrorist financing implies timely reporting of suspected transactions that indicate money laundering or terrorist financing, based on information received by the competent authorities in the process of supervising. Furthermore, in order to achieve better identification of information concerning beneficial ownership, the goal linked to setting up of centralized bank register should be realized. Finally, the comprehensive response to the prevention of money laundering and the financing of terrorism risks includes as broad as possible cooperation between criminal law systems including mutual support among national financial units such as the competent authorities supervising credit and financial institutions and other authorities as well.

When it comes to the Serbian Law on the prevention of money laundering and the financing of terrorism it can be noticed that national legislation is almost com-

pletely in compliance with the new EU framework on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. However, there are certain parts of that Law which are not completely in line with the new EU framework. Firstly, in the area of customer due diligence measures with respect to electronic money products, there is different level for the amount of stored electronic money as well as the maximum monthly payment transactions limit which do not exceed the RSD equivalent of EUR 250 according to Serbian law and EUR 150 as stated by EU law. Furthermore, the difference also exists concerning the fact that this rule is not applicable in the case of redemption in cash or cash withdrawal of the monetary value of the electronic money where the amount redeemed exceeds EUR 50 in a line with EU law or EUR 100 as claimed by the Serbian law. In addition, when it comes to the issue of obliged entities it should be mentioned that Serbian Law recognizes as obliged entities only providers of virtual currencies, while EU law includes as the new obliged entities providers of fiat currencies and traders in works of art, too. Finally, since EU law has set the goal in the sense of setting up centralized central registries or central electronic data retrieval systems, which allow the identification, in a timely manner, of any natural or legal persons by 26 June 2020 it is undisputed that Serbian law must be amended including this provision as well.

To conclude, bearing in mind, emerging new trends, in particular regarding the way terrorist groups finance and conduct their operations it is extremely important to constantly collect data on new trends for the commission of a criminal offense of terrorist financing. In that regard, it is necessary to work through the training program to develop the skills and capabilities of persons involved in the suppression of terrorist financing to enable them to be prepared for all methods and techniques used by terrorist groups. Precisely the risk of the new threats in the area of the abuse of the financial system for the purposes of terrorist financing requires application of the multinational approach in order to combat this phenomenon, since it is unrealistic to expect that one or several countries, without others, will achieve any results at the level of prevention. Therefore, owing to the fact that the abuse of the financial system through the terrorist financing as a phenomenon cannot be eradicated, it should be aware that by working together the whole international community can achieve much more in the context of controlling this phenomenon.

REFERENCES

BOOKS AND ARTICLES

1. Bolta D., *Sprječavanje financiranja terorizma*, Policija i sigurnost, *Vol*. 19, No. 4, 2010, pp.417-430.
2. Borlini L.; Montanaro, F., *The Evolution Of The Eu Law Against Criminal Finance: The "Hardening" of FATF Standards Within The EU* George Town Journal Of International Law, *Vol*. 48, 2017, pp. 1009-1062
3. Cindori, S.; Petrović, T., *Indikatori Rizičnosti Bankarskog Sektora U Okvirima Prevencije Pranja Novca*, Zbornik PFZ, *Vol*. 66, No.6, 2016, pp. 761-784
4. Cmiljanić, B., *Zabrana finansiranja terorizma u svetlu međunarodnog prava i propisa Republike Srbije*, Temida No. 2, 2011, pp. 41-59
5. Colin, N., *Adoption of fifth Anti-Money Laundering Directive*, White & Case, 2018
6. Council of Bars and Law Societies of Europe, *CCBE comments on the proposal of 5 July 2016 to amend Directive 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing*, Council of Bars and Law Societies of Europe, Bruxelles, 2016
7. Cvitanović. L., *et.al.*, *Kazneno pravo- posebni dio*, Pravni fakultet Sveučilišta u Zagrebu, 2018
8. Deloitte, *Five insights into the art market and money laundering*, Deloitte Development LLC, London, 2018
9. Derenčinović, D., *The Review Of The Harmonisation Of The Croatian Criminal Law With International Legal Documents On Combating Terrorism*, Hrvatski ljetopis za kazneno pravo i praksu, *Vol*. 10, No. 2, 2003, pp. 941-962
10. Derenčinović, D., *et. al., Posebni dio kaznenog prava*, Pravni fakultet Sveučilišta u Zagrebu, 2013
11. Fahmy, M., *The Fifth Money Laundering Directive*, Global Risk Profile, Geneva, 2016
12. Financial Action Task Force, *Terrorist Financing*, Paris, 2008
13. Financial Action Task Force, *Virtual Currencies – Key Definitions And Potential Aml/Cft Risks- The FATF Report*, Paris, 2014
14. Financial Action Task Force, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation- The FATF Recommendations*, Paris, 2016
15. Finn, H., *The fifth anti-money laundering and terrorist financing directive (AML 5)-Key aspects and changes* Arendt & Medernach, Luxembourg, 2018
16. Fletzberger, B., *5th Anti-Money Laundering Directive – a summary of the main points*, PayTechLaw, 2018
17. Haffke, L.; Fromberger, M.; Zimmermann P., *Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and how to Address them*. Available at SSRN: [https://ssrn.com/abstract=3328064] or [http://dx.doi.org/10.2139/ssrn.3328064]
18. Internal Audit, Risk, Business & Technology Consulting, *Anticipating the Fifth EU AML Directive*, Internal Audit, Risk, Business & Technology Consulting, London, 2017

19. International Centre For Asset Recovery, *Tracing Illegal Assets - A Practitioner's Guide, International Centre For Asset Recovery*, Basel 2015
20. Jourová V., *Strengthened EU rules to prevent money laundering and terrorism financing*, European Commission, 2018
21. Keatinge, T.; Carlisle, D.; Keen, F., *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, European Parliament, Brussels, 2018
22. Kordík, M.; Kurilovská, L., *Protection of the national financial system from the money laundering and terrorism financing,* Entrepreneurship and Sustainability Issues, *Vol*. 5, No. 2, 2017 pp. 243-262
23. Kostić, J., *Harmonizacija nacionalnog zakonodavstva Republike Srbije sa Konvencijom o zaštiti finansijskih interesa Evropske unije*, Evropsko zakonodavstvo, *Vol*. 13 No. 47/48, 2014, pp. 187-202
24. Kostić, J., *Krivičnopravna zaštita finansijskih interesa Evropske unije*, Institut za uporedno pravo, Beograd, 2018
25. Lukić T., *Borba Protiv Pranja Novca I Finansiranja Terorizma U Republici Srbiji,* Zbornik radova Pravnog fakulteta u Novom Sadu, No. 2, 2010, pp. 197-215
26. Manojlović, S., *Predlog zakona o sprečavanju finansiranja terorizma*, Bilten sudske prakse Vrhovnog suda Srbije, No. 2, 2006, pp.83-91
27. Milošević, B., *Money Laundering As A Form Of Economic Crime In The Role Of Financing Terrorism*, Facta Universitatis, *Vol*. 14, No. 4, 2016, pp.549-560
28. Milošević, M., *Novi Zakon o sprečavanju pranja novca i finansiranja terorizma*, Časopis "Izbor sudske prakse", No. 3, 2018, pp. 9-13
29. Mitsilegas,V.; Vavoula,N., *The Evolving Eu Anti-Money Laundering Regime Challenges For Fundamental Rights And The Rule Of Law*, Maastricht Journal of European and Comparative Law, *Vol*. 23, No. 2, 2016, pp. 261-293
30. Pedić, Ž., *Neprofitni Sektor I Rizik Od Financiranja Terorizma*, Ekonomska misao i praksa, *Vol*. 19, No. 1, pp.139-156
31. Prokić, A., *The Link Between Organized Crime And Terrorism*, Facta Universitatis, *Vol*. 15, No, 1, 2017, pp. 85-94
32. Schott, P., *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, The World Bank and The International Monetary Fund*, Washington DC, 2006
33. Sinanović, B., *Pranje novca*, Bilten sudske prakse Vrhovnog suda Srbije, No. 2, 2011, pp.61-68
34. Stanković N., *Terorizam i finansiranje terorizma*, Evropski Univerzitet Brčko, Brčko, 2014
35. Tomić S., *New EU Directive On The Prevention Of The Use Of The Financial System For The Purposes Of Money Laundering And Terrorist Financing*, Bankarstvo, *Vol*. 47, No.2, 2018, pp. 108-113
36. United Nations Office on Drugs and Crime, *Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies*, United Nations Office on Drugs and Crime, Vienna, 2014
37. Važić, N. *Pranje Novca- Materijalni I Procesni Aspektu Međunarodnom I Domaćem Zakonodavstvu*, Bilten sudske prakse Vrhovnog suda Srbije, No. 2, 2008, pp. 114-141

EU LAW

1. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Official Journal of the European Union, L 141/73 of 5 June 2015
2. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Official Journal of the European Union, L 156/43 of 19 June 2018

LIST OF NATIONAL REGULATIONS, ACTS AND COURT DECISIONS

1. Law on the prevention of money laundering and the financing of terrorism, Official Gazette of the Republic of Serbia, No. 113/17 of 17 December 2017
2. National Strategy on the combating of Money Laundering and the Financing of Terrorism, Official Gazette of the Republic of Serbia, No 89/08
3. Decision On Guidelines For The Application Of The Provision Of The Law On Prevention Of Money Laundering And Financing Terrorism For Obliged Entities National Bank Of Serbia Perform Supervision [http://www.apml.gov.rs/REPOSITORY/2015_2_smernice-nbs.pdf, p.17] Accessed 11.03.2019

WEBSITE REFERENCES

1. FATF Recommendation 19, [https://cfatf-gafic.org/index.php/documents/fatf-40r/385-fatf-recommendation-19-higher-risk-countries] Accessed 11.03.2019
2. FATF Recommendation 24, [https://cfatf-gafic.org/index.php/documents/fatf-40r/390-fatf-recommendation-24-transparency-and-beneficial-ownership-of-legal-persons] Accessed 11.03.2019
3. FATF Recommendation 25, [https://cfatf-gafic.org/index.php/documents/fatf-40r/391-fatf-recommendation-25-transparency-and-beneficial-ownership-of-legal-arrangements] Accessed 11.03.2019
4. FATF Recommendation 40, [https://cfatf-gafic.org/index.php/documents/fatf-40r/406-fatf-recommendation-40-other-forms-of-international-cooperation] Accessed 11.03.2019