Marina M. Matić Bošković*

Review scientific paper
UDK: 004.738.5:343.537
doi: https://doi.org/0.56461/SPZ_22406KJ

CYBERCRIME MONEY LAUNDERING CASES AND DIGITAL EVIDENCE

Abstract

The widespread dependence on digital systems and increased value of digital commerce in the metaverse boosted cyber vulnerability. The cybercrime will be more profitable than the global trade of all major illegal drugs combined, while Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent annually by 2025. Cybercrime changed traditional money laundering methods which is difficult to detect since it could be committed from anywhere in the world. The threat posed by cybercrime money laundering methodologies has been aggravated by the Covid-19 pandemic.

To investigate cyber laundering the e-evidence are crucial, which is confirmed by the EU Commission estimate that 85 percent of criminal investigations require electronic evidence. Additional challenge for law enforcement authorities presents the fact that the organised cybercrime is joining forces and their likelihood of detection and prosecution is estimated to be 0.05 percent in the USA. Furthermore, the digital evidence is often held by service providers as private companies based in another country, which causes many obstacles to access to those data by investigative and law enforcement authorities.

The paper identifies impact of Covid-19 on cybercrime and increased risks of cyber laundering. In relation to investigation and prosecution of cyber money laundering, the paper analyzes challenges for investigative authorities to gather data and evidence in cyber money laundering cases and efforts of EU and USA authorities to facilitate access to digital evidence and relevant data stored by service providers. The paper refers to possible shortcomings of proposed instruments and need for efficient response and adaptation to changes in the cybercrime.

Keywords: *cyber laundering, mutual legal assistance, digital evidence, data gathering, cross-border cooperation.*

* PhD, Senior Research Fellow, Institute of Criminological and Sociological Research, Belgrade
E-mail: *m.m.boskovic@roldevelopmentlab.com*
ORCID: *https://orcid.org/0000-0003-1359-0276*

1. Introduction

The staggering advancement of information and communication technologies over the last few decades has significant impact on the society in different forms and on number of areas ranging from communication and trade to education and agriculture. Besides benefits, innovations in information and communication technologies and its application in the number of areas create opportunities for criminals to conduct crimes in the cyberspace (World Economic Forum, 2021, Chapter 2).

In 2015, cybercrime cost the global economy around $3 trillion (Cybersecurity Ventures, 2020) and it was estimated that in 2021 that figure increased to $6 trillion (Morgan, 2020). According to Cybersecurity Ventures the cybercrime will be more profitable than the global trade of all major illegal drugs combined. Having in mind the relevance of the cybercrime and the threat it causes to functioning of the states and business, it is clear that investigation of these crimes represents the high interest of the criminal justice. To conduct investigation of cybercrime the cross-border access to digital information is of paramount interest. However, the organised cybercrime is joining forces and according to the World Economic Forum their likelihood of detection and prosecution is estimated to be 0.05 percent in the USA (World Economic Forum, 2020, p. 63).

Cybercrime changed traditional money laundering methods which rely on the banking system. Money laundering is a constantly changing criminal phenomenon, with updated modus operandi and evolving business models (Savona, 2014, p. 1). According to several sources, money laundering is an offence that has benefited most from the modern technologies (Souto, 2013, p. 266). Cyber laundering could be committed by using different methods that involves various types of transactions such as wire transfers, relies on use of various types of transactions ranging from wire transfers, withdrawals to money mules and via ATM, use of accounts opened with lost documents or fictitious companies, etc. Electronic payment systems facilitate money laundering since it is more convenient for moving high amount of money and due to speed of transactions difficult to control property or freezing (Financial Action Task Force, 2010).

Cybercrime is not used only for laundering money gained through criminal activities, it is also used for laundering of money obtained by cybercrimes. Modalities to gain money by cybercrime differ from malicious malware and phishing to account takeovers. Common for all methods of cybercrime is that offenders are interested to quickly move the illicit funds to avoid confiscation.

According to the United Nations Office on Drugs and Crime (UNODC), the three stages of traditional money laundering can be distinguished: placement,

layering and integration (See more: United Nations, Money Laundering). However, if money originates from the cybercrime, the money laundering process immediately jumps to the second stage – layering. The UNODC highlighted three main ways of layering: moving funds within the financial system through offshore accounts or anonymous shell accounts, moving funds into unregulated financial e-cash systems such as electronic money or casinos and removing funds from the financial system.

Development of new technologies put additional risks for combating cybercrime, since it provides almost complete anonymity to perpetrators seeking to exploit this arena. In addition, the 59.5 percent of the world population are active internet users (Worldwide digital population as of January 2021). Cybercrime is difficult to detect due to the fact it could be committed from anywhere in the world, relatively easy and without significant costs. For investigators it is difficult to trace identities, while victims of cybercrime do not always want to disclose the fact to investigative authorities. Development of cryptocurrencies, like bitcoin, increased complexity of investigation of money laundering, since criminals start to embrace bitcoin as a partner in their cash-out strategy (van Wegberg, Oerlemans & van Deventer, 2018, p. 420).

In the article the impact of modern technologies and Covid-19 on cyber laundering will be analysed. Measures introduced during Covid-19 incentivised people and business to increase use of modern technologies in daily operations, which increased risk of cybercrime and cyber-attacks. Covid-19 has permanently changed behaviour of both people and business, which will require transformation of government and investigative bodies' response to increased risk of cybercrime. Due to the fact that cyber laundering often involves cross border evidence, the challenges in gathering that evidence in the EU and USA will be elaborated. Furthermore, the author will assess attempts of the national and international institutions (EU and USA) to facilitate access to e-evidence in cyber laundering cases.

2. Impact of Covid-19 on cyber laundering

The threat posed by cybercrime money laundering methodologies has been exacerbated by the Covid-19 pandemic. The International Criminal Police Organization (Interpol) issued a global threat assessment on crime and policing to its 194 member countries (The International Criminal Police Organization, 2020). Furthermore, the Financial Action Task Force (FATF) highlighted an expansion of money laundering originated from Covid-19-related crime, which could include increased misuse of online financial services and virtual assets to

move and conceal illicit funds; and possible corruption connected with governmental stimulus funds or international financial assistance (Financial Action Task Force, 2020).

Introduction of measures to prevent spread of Covid-19 virus in 2020 and to some extend in 2021 influenced the behaviour of citizens and business. Both groups increased online activities and e-commerce. Remote work, introduced during Covid-19, and still in use to certain extent, requires the use of online platforms and exchange of sensitive data. Value of the digital commerce in the metaverse grows and it is estimated to be $800 billion by 2024 (World Economic Forum, 2022). The increase of online financial activities and change of customer behaviour enable criminals to target vulnerable individuals and institutions more easily and take advantage of existing legal gaps.

To overcome challenges caused by measures imposed to prevent spread of virus, such as social distancing and office closure, financial institutions introduced remote onboarding and identity verification. The introduced changes created loopholes for money launderers, especially at the beginning of the process when financial institutions had not been fully prepared to remotely verify identity of customers and clients.

Prior to Covid-19 outbreak, cyber-attacks and money laundering violations exposed financial institutions to significant operational and reputational risks. To ensure effective business operation during pandemic, financial institutions needed additional resources and transformation of some business processes which decreased their capabilities to monitor suspicious transactions. Public authorities were faced with similar problems. As consequence of all challenges, many authorities are prioritising other sensitive areas and therefore postponing anti-money laundering onsite inspections or relying only on off-site monitoring. Some authorities were delaying anti-money laundering reporting and other regulatory requirements to decrease the pressure on the staff (Crisanto & Prenio, 2020, p. 4). Moreover, many countries reported an increase in cash withdrawals during the Covid-19 outbreak (Report in the Financial Times). After stabilisation of situation the cash will return which could provide cover for money laundering activities) (Auer, Cornelli & Frost, 2020).

Pandemic specifically influenced using of money mules for money laundering.[1] While technique of money mules has been used for a long time, Covid-19 lockdowns had an effect on the increase in the typology due to the fact that people's behaviour and daily routines were changed and most of the people worked from their homes. Work from home increased the use of computers. Restriction

[1] Money mules are individuals who wittingly or unwittingly help criminals launder money through their individual and business checking accounts.

of movement had as a result that people were spending more time online and were exposed to ads and dubious schemes. Criminals reacted promptly to the change of people's behaviour, and they were looking for marks online of those unexperienced who can be persuaded to move criminal funds through their accounts. Those schemes were used by criminal gangs to defraud the USA government out of unemployment checks, tax refunds and other financial disbursements. Criminals were using different methods to conduct frauds and apply for state assistance, from stealing identities to purchasing synthetic identities and at the later stage using money mules to move the money.

The recent Financial Crimes Enforcement Network (FinCEN) Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (FIN-2020-A003)[2] issued in July 2020 details some of typologies on money mule schemes. Furthermore, the USA institutions issued warnings on different scams and possible cyber-attacks on citizens and business (Federal Trade Commission Business Blog, 2020; Federal Bureau of Investigation (FBI) Internet Crime Compliant Center Public Service Announcement, 2020).

Furthermore, according to the SIRIUS EU Digital Evidence Situation Report, pandemic led to longer delays in receiving responses from online service providers, which caused challenges for law enforcement and judicial authorities in the EU (European Union Agency for Law Enforcement Cooperation, 2021, p. 6).

3. Evidence Gathering Challenges

For the collection of electronic evidence, the most relevant biding international instrument is the Council of Europe Convention on Cybercrime (Budapest Convention).[3] The Budapest Convention is accompanied by assessment mechanism established in the form of Cybercrime Convention Committee. Currently the Committee is focused on assessing access to electronic evidence on cloud servers by law enforcement authorities. The aim of the Convention is to ensure that criminal law

[2] Document is available at:
https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2020-a003.

[3] Council of Europe, Convention on Cybercrime (EST No. 185). The Convention is supplemented by a First Additional Protocol covering the criminalization of acts of a racist and xenophobic nature committed through computer systems (CETS 189) and a Second Additional Protocol on enhanced international cooperation and disclosure of electronic evidence (CEST 224). Non-binding instrument is Council of Europe Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime, adopted on 13 September 1989 that resulted in the approximation of national legislation regarding certain forms of computer-related crime elaborated by the European Committee on Crime Problems.

is in line with technological developments that could lead to misuse of cyberspace facilities and cause damage (Clough, 2014, p. 702). The main value of the Convention is contribution to the creation of common standards by providing the criminalisation of a list of attacks against and by means of computer systems[4] and by establishment of procedural law tools to make the investigation of cybercrime and the securing of electronic evidence and international police. Furthermore, the Convention enables international police and judicial cooperation on cybercrime and e-evidence by providing legal framework for international cooperation.

The Budapest Convention on Cybercrime provides definitions of terms relevant for cybercrime, like definition of the computer system, computer data, service provider, and traffic data. According to Article 1 of the Convention, the computer data means the representation of facts, information or concepts in a form suitable for processing in a computer system (e.g., photo, video, sound, text), while service provider means any public or private entity that provides to service users the ability to communicate by means of a computer system and any other entity that processes or stores computer data on behalf of such communication service or users of such service.

For collection and analysis of data from computer systems, networks, wireless communication and storage devices in a way that is admissible as evidence in a court of law, the digital forensics as a new discipline has been developed (Craiger, 2006, p. 720). According to Interpol, digital forensics is a discipline that combines elements of the law and computer science that focuses on identifying, acquiring, processing, analysing and reporting on data stored electronically (Interpol, Digital Forensics). Digital evidence is any information and data of value to an investigation that is stored on, received or transmitted by an electronic device and could be found on a computer hard drive, a mobile phone, internet etc. (National Institute of Justice, 2008, p. ix).

The main challenge for collection of digital evidence is that their content and location can be easily and swiftly altered. In addition, one of the challenges for gathering of digital evidence is the practice to conduct digital forensics by law enforcement officers who are not digital forensic scientist (Adams *et al.*, 2013, p. 31). Additionally, most of the forensics labs are linked with law enforcement, either through financial dependence on law enforcement or as institutional part of the law enforcement agencies (Doyle, 2019, p. 7).

[4] The Budapest Convention covers crimes of illegal access, interference and interception of data and system networks, and the criminal misuse of devices. In relation to offences conducted by means of computer systems, the Budapest Convention regulated computer-related fraud, production, distribution and transmission of child pornography and copyright offences.

To overcome existing challenge that the investigators lack competence to attribute, evaluate, interpret, and re-construct digital traces (van Baar *et al*., 2014, p. S58), digital forensics is used in the investigation phase. However, use of digital forensics raise questions of professional bias, protection of innocent defendants and equality of arms in respect to digital forensics aid for the defence (Stoykova, 2021, p.10). Investigation is a process that develops and tests hypotheses to answer questions about events that occurred (Carrier, 2004, p. 9), while digital forensic scientists, evaluate facts to establish their probative strength (Pollitt *et al*., 2019, p. 15).

Frequently, in investigation of cyber laundering cases there is a need for collaboration between digital forensics experts and forensic accountants with experience in analysing financial records and providing an accounting analysis suitable to be used in legal proceedings. Forensic accounting is used in criminal investigations to trace funds, identify assets, recover assets, etc.

According to SANS Institute for information security training and security certification (Braid, 2002, p. 3), law enforcement authorities and forensics should follow specific rules in confiscation of digital evidence to ensure their admissibility in the court. Digital evidence must be collected in line with legal procedure, related directly to the case, and unbiased, while method of extraction should maintain integrity. Having in mind that digital evidence might be complex, the law enforcement authorities should present them to a court in understandable manner.

According to the European Commission estimation from 2019, electronic evidence is necessary in 85 percent of criminal investigations (European Commission, 2019, Recommendation for a Council Decision, Authorising the Opening of Negotiations in View of an Agreement between the European Union and the United States of America on Cross-Border Access to Electronic Evidence for Judicial Cooperation in Criminal Matters). Additionally, in two thirds of these investigations there is a need to obtain evidence from online service providers as private entities that have seat in other country, which requires use of mutual legal assistance instruments to access to evidence (European Commission, 2019, Recommendation for a Council Decision, Authorising the Opening of Negotiations in View of an Agreement between the European Union and the United States of America on Cross-Border Access to Electronic Evidence for Judicial Cooperation in Criminal Matters). Electronic data must be handled with certain scientific procedures to maintain their high probative value, since their legal assessment will lead a judge to reach a conclusion in the case (Karagiannis & Vergidis, 2021, p. 186).

Nevertheless, permanent changes of information and communication technology require from state authorities and criminal justice system to constantly revise and adapt their policies and standard operating procedures to strengthen

the legal framework of a jurisdiction. One of the main challenges for legislators and law enforcement agencies is access to service provider data, since the different jurisdictions are responsible based on different criteria, such as the location of service provider's headquarter, location of clients who access to services or location of servers. The new payment technologies have influenced the increase of abovementioned challenge, since they allow citizens and legal entities to conduct business between different countries and various legal systems (Filipkowski, 2008, p. 17). As a consequence of that globalization, if an offence occurs, several jurisdictions have to be involved which requires the cooperation between different authorities from revenue services to judiciary. Although countries signed many mutual legal assistance treaties, the complexity of cooperation influence on investigation and prosecution of transnational crimes and creates it as one of the most difficult tasks.

The increasing use of internet and transfer of data in digital form led investigation and prosecution authorities to rely on digital evidence. To ensure efficient investigation and prosecution of cybercrime it is necessary to permit law enforcement agencies cross-border access for gathering electronic data.

In the EU member states investigating and prosecuting authorities are relying on cross-border data and evidence in significant number of cases. EU instruments of mutual legal assistance in criminal matters provide legal basis for judicial cooperation and possibility to request needed information also in digital form, from competent authorities of another EU Member States (Stefan, Gonzalez, 2018, p. 8). However, the available judicial cooperation and mutual assistance instruments are too slow and complex for cybercrime cases (Tinoco-Pastrana, 2020, p. 46; Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, 2016, p.5).

Additional problem for cross-border cooperation in cybercrime is caused by the fact that electronic evidence is held on servers owned by service providers who are often foreign, non-EU companies. Majority of service providers are USA legal entities (i.e. Google, Facebook, Microsoft, Apple). However, the location of servers could be in the third country which contributes to further complexity for law enforcement authorities. Also, territorially based mutual legal assistance instruments are not applicable on cloud-based services (Krishnamurthy, 2016, p. 1). Furthermore, the jurisprudence and interpretation of access to foreign searches differ among jurisdictions. Namely, USA Supreme Court judges are on the position that USA courts do not have competence to issue warrants for foreign searches (Daskal, 2015, p. 354). On contrary, the European Court of Justice recognised the right of European courts to order the search of service provider parent company in the USA (Google Spain SL and Google Inc. v. Agencia Española

de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, ECLI:EU:C:2014:317, para. 43). Despite the decision of the European Court of Justice, there is no mechanism to oblige services providers to respond on requests of law enforcement authorities. At the national level, the example of the court decision where the principle of territoriality was abandoned was delivered in Belgium (*Yahoo! Inc. v Belgium* case, Hof van Cassatie of Belgium, Case P.13.2082.N.). The first example is the case law of the Supreme Court of Belgium in case of Yahoo in 2011, 2012 and 2015 and latter in case against Facebook (De Hert, Parlan & Thumfart, 2018, p. 343). The court jurisprudence influenced on the legislation and as consequence national legislation of Belgium, Germany and Austria was amended to include provisions allowing remote evidence gathering through the internet. (Warken, 2018, p. 227)

4. EU Cross Border Cooperation in Evidence Gathering

To overcome problem in evidence gathering the EU authorities prepare proposals of the two legal instruments, Regulation and Directive (Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final 2018/0108 (COD); Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings COM/2018/226 final 2018/0107 (COD)), with the aim to establish legislative framework that will permit direct communication between law enforcement agencies and service providers from different EU Member States. Based on the proposals the law enforcement authorities will be equipped to directly request from service providers in another Member State to produce or preserve electronic data (Tosza, 2020, p. 162). Implementation of proposed acts in the EU member states would create new challenges for direct interconnection of investigating and prosecuting authorities and private companies (Carrera, Mitsilegas & Stefan, 2021, p. 26).

The European Production and Preservation Orders are designed to bring a new dimension in mutual recognition. In comparison to other EU mutual recognition instruments that ensure direct communication between state authorities, the proposed instruments are focussed to empowering law enforcement actors to request, access and share data held by service providers across borders. However, both legal acts have been criticized for violation of human rights standards (Matić Bošković, 2021, pp. 132-135).

As far as cross-border demands for electronic information involving EU member states which are not part to the European Investigation Order Directive (Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *OJ* L 130, 1 May 2014, pp. 1-36; Directive (EU) 2022/228 of the European Parliament and of the Council of 16 February 2022 amending Directive 2014/41/EU, as regards its alignment with Union rules on the protection of personal data, *OJ* L 39, 21 February 2022, pp. 1-3) such as Ireland or Denmark, or third countries (e.g., the USA or Japan), EU Mutual Legal Assistance Treaties present framework for communication and establish rules for requesting, gathering, and exchanging data for criminal investigations and prosecutions.

As for transatlantic cooperation, the Agreement on Mutual Legal Assistance (MLA) between the European Union and the United States of America (Agreement on mutual legal assistance between the European Union and the United States of America, *OJ* L 181, 19 July 2003. pp. 34-42) has set conditions relating to the provision of mutual legal assistance in criminal matters between the EU and the US and represents the framework agreement to their bilateral mutual legal assistance treaties (Stefan & Gonzalez Fuster, 2018, p. 18). The aim of the Agreement is to enhance cooperation between EU member states and the US as a complement to existing bilateral mutual legal cooperation treaties with particular EU member states and to amend some of their provisions, if they provide for less effective avenues of cooperation (Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America). In the absence of such a treaty, the EU member states and USA undertake to ensure that the agreement is applied and provides a suitable legal basis for cooperation.

The Agreement is setting framework that ensures compliance of the mutual legal assistance request on access to electronic information with the legal and procedural requirement of issuing and requested country (Carrera *et al*., 2015, pp. 7-8). Gathering of electronic evidence by law enforcement agencies in USA is regulated by the Electronic Communication Privacy Act (ECPA) and Stored Communication Act (SCA). Furthermore, the Fourth Amendment sets the default rule that any search and seizure without a warrant is unreasonable that could be obtained upon a showing standard of probable cause (Swire, Hemmings, Vergnolle, 2016, p. 110). The ECPA and the SCA set different rules for different type of electronic evidence,[5] which cause challenges for EU investigating

[5] The ECPA and the SCA make distinction between following categories of evidence: basic subscriber information; dialing, routing, addressing and signaling information; other metadata,

authorities. For certain categories of evidence, the EU member state authorities can submit request directly to the service provider, while other type of electronic evidence are subject to the MLA process. The EU–US Agreement ensures that rights of suspects and accused persons are protected in line with national legislation and data protection standards, including the need to provide a court order for qualifying categories of electronic evidence.

The EU investigating bodies may request stored non-content electronic information directly from USA service providers. However, the SCA has complex rules on voluntary disclosure of that type of electronic evidence. Basic subscriber information is type of electronic evidence that is not protected under the Fourth Amendment and service providers can voluntarily disclose this information to law enforcement upon request. However, this ability to provide evidence voluntarily has as a consequence lack of legal certainty, compared with mutual legal assistance request which has to be compulsory executed. Although the cross-border requests to access and gathered electronic data held by service providers have become a common investigative practice in the EU, the Commission is on the position that the high volume of request to access e-evidence under the MLA put whole system under the strain and has shown its weakness. The MLA processes with the US on average takes 10 months and is perceived too long for efficient investigation (European Commission, 2018; Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, 2018, p. 9). Having in mind mentioned limitations of the MLA system, it is evident that direct cooperation is not a fully satisfactory solution.

The transparency reports showed that number of EU Member States requests to the main service providers has increased by 70% over the four-year period (2013-2016). The two service providers were dominant, Google and Facebook received more that 70 percent of total number of requests from the EU Member States. However, the percentage of requests from the EU Member States answered by service providers is relatively low and range from 46% in 2013 to 58% in 2016. The limitation of transparency reports is that they include information on the number of requests answered, which is not same as fulfilled.[6]

such as location information; the stored content of electronic communications and the real-time content of electronic communications.

[6] According to the European Commission Impact Assessment, five main service providers are Google, Facebook, Apple, Microsoft and Twitter. The EU Commission estimated that up to 90% of current cross-border requests for non-content data are sent to these five providers, based on their market share, (European Commission, 2018, pp. 16-17).

While indicating that these requests "mostly" concern non-content data, the European Commission in the 2018 Impact Assessment also noted how these transparency reports suffered from important limitations. For example, the reports did not distinguish whether reported requests came directly from the member state in which they originated, or it came from the public authorities of member state that was asked to cooperate with the one in which the request originated (European Commission, 2018, pp 16-17). As such, based on the information provided by the transparency reports it is difficult to precisely quantify the number of requests executed based on voluntary procedures.

A specific challenge arises when data collection measures are requested directly from service providers subject to EU law but originating from non-EU countries. According to the SCA, the US investigative and prosecuting authorities can obtain a warrant requiring from US companies to produce data stored abroad. The competence to order disclosure of data stored abroad is explained that it is for the US company with control over the data to grant US authorities the competence to require its production (Kyriakides, 2019, p. 100).

The US Government adopted the CLOUD Act (Clarifying Lawful Overseas Use of Data (CLOUD Act), S. 2383, H.R. 4943) after the *Microsoft Ireland* case,[7] which challenged the competence of the US federal courts to issue warrants for the search and seizure of data located outside the territory of the United States. The aim of the CLOUD Act was to clarify that the SCA's scope application extends to data stored abroad.[8] The adoption of the CLOUD Act raised questions of compliance with EU acquis, especially articles 48 and 49 of the EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)).

To overcome challenges that could arise from different level of fundamental rights protection in the EU and the US legal system, the EU–US Umbrella Agreement was signed in 2016 (Agreement between the United States of America and the European Union on the protection of personal information relating to the

[7] The dispute questioned the lawfulness of extraterritorial assertion of US criminal jurisdiction in light of standing (i.e. pre-CLOUD Act) domestic legislation. The US Department of Justice argued that its warrant authority under the SCA required US-based companies to turn over the requested data, regardless of where the latter were stored.

[8] Part I of the Act (section 103) now formally grants USA authorities the power, under USA law, to order private companies to disclose the "content of a wire or electronic communication and any record of other information" about a person, regardless of either the nationality of the latter or the location of the data. Providers can also be ordered to preserve data in their possession for up to 180 days prior to the issuance of any compulsory process.

prevention, investigation, detection, and prosecution of criminal offences, *OJ* L 336/3, 10 December 2016). The Umbrella Agreement puts in place a data protection framework for EU – US law enforcement cooperation, which is confirmed in definition of its purpose in the Article 1 of the Agreement. The Agreement applies to all personal data exchanged between the EU and the US for purpose of prevention, investigation, detection and prosecution of criminal offences. The Agreement also covers transfer by private companies in the territory of one party to the competent authority of the other party (Stefan & Gonzales Fuster, 2019, p. 20). The Umbrella Agreement grants EU citizens the possibility to seek judicial remedies before US courts if US authorities mistreat their data.

According to the Review of the EU–US MLA Agreement implementation (Council of the European Union, 2016) the two problems are identified and affect the process of obtaining electronic evidence from the US. The first one relates to the non-enforcement of the requests due to the inadequacy and insufficient presentation of probable cause. The second one relates to the fact that majority of the service providers are located in the US, which has caused high volume of request for electronic evidence to be submitted to the US (Daskal, 2016, p. 358).

The EU and US authorities are assessing possibilities for improvement of cooperation under the existing MLA Agreement with the aim to strengthen fight against crime and especially cybercrime and cyber laundering. Over the time the EU and the US were introducing practical measures as specialised personnel including establishment of the European Judicial Cybercrime Network (EJCN) in 2016 to foster contacts between practitioners specialised in cybercrime and to increase the efficiency of investigations and prosecutions of cybercrime. The EJCN is the body with which US Department of Justice liaise. Additionally, national contact points and liaison officers are also practical solutions that could contribute to better results in combating cybercrime. Complexity of procedures could be overcome by simplification and streamlining of processes for requesting and providing assistance as well as allocation of sufficient financial and human resources for enforcement of received requests.

Exercising reciprocal judicial scrutiny over incoming law enforcement agencies requests for data emerges as an essential requirement under EU law. The reciprocal judicial scrutiny ensures the protection of the subject whose data are requested under the EU-US Agreement. Due to this protection the requests are being refused for the reason: the failure to demonstrate probable cause, the absence of dual criminality, the failure to demonstrate a connection between the evidence sought and the criminal conducted alleged, and on the basis of essential interests (Council of the European Union, 2016a, p.7). Additionally, judicial scrutiny has a purpose to guarantee the EU citizens' fundamental rights, both in the EU and US.

5. Conclusions

Development of information and communication technologies affected on development of cybercrime and specifically cybercrime laundering. The criminal justice systems developed new legal instruments to adapt to new circumstances and to the fact that majority of evidence are in the digital form. The Covid-19 pandemic and introduced social distancing measures, increased used of online tools and platforms worsened situation and increased risks of cybercrimes, and specifically cyber laundering.

The specific of the cyber laundering is cross-border element. Patchwork enforcement mechanisms across the jurisdiction continue to hamper efforts to control cybercrime. Within the EU, the member states could use the mutual recognition instruments to collect digital evidence. However, majority of service providers are US legal entities, so mutual recognition instruments are not applicable. Cyber laundering and use of cryptocurrencies require immediate response of law enforcement authorities, due to possibility to easily move assets and destroy evidence. Requirement for efficient investigation and prosecution of cybercrimes, including cyber laundering put authorities within the EU and US under the pressure to enable law enforcement smooth access to data at the international level.

Collection of digital evidence in cyber laundering cases is challenging since evidence is stored by service providers that might have headquarter in another EU member state, or very often in the US since there is a headquarter of five main service providers. Access to this electronic evidence and its gathering create difficulties for law enforcement agencies and criminal investigation authorities. The EU Commission Impact assessment has identified that traditional mutual legal assistance and mutual recognition instruments have limitations that affect effectiveness of investigations.

The recent EU and US legislative initiatives have focused on ensuring of the direct cross-border requests of the criminal justice authorities to service providers as private companies. The proposed Regulation on Production Order and Preservation Order within the EU is criticized since they are not in line with EU rule of law standards.

The analysis has shown that new cross-border data collection and evidence gathering instruments are useful in practice only if they are in line with the human rights protection standards.

References

Adams, R., Hobbs, V. & Mann, G. 2013. The Advanced Data Acquisition Model (Adam): a process model for digital forensic practice. *Journal of Digital Forensics, Security and Law,* 8 (4), pp. 25-48, https://doi.org/10.15394/jdfsl.2013.1154.

Braid, M. 2002. Collecting Electronic Evidence After a System Compromise, Global Information Assurance Certification Paper for SANS Institute. Available at: https://www.giac.org/paper/gsec/659/collecting-electronic-evidence-system-compromise/101519.

Carrera, S., González Fuster, G., Guild, E. & Mitsilegas, V. 2015. Access to Electronic Data by Third-Country Law Enforcement Authorities. *CEPS Paperback*. Brussels: CEPS.

Carrera, S., Mitsilegas, V. & Stefan, M. 2021. Criminal Justice, Fundamental Rights and the Rule of Law in the Digital Age. *Report of a CEPS and QMUL Task Force*, Brussels

Carrier B. & Spafford, E. 2004. *An Event-based Digital Forensic Investigation Framework*. Presented at the Digital Forensic Research Workshop, Baltimore.

Clough, J. 2014. A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation. *Monash University Law Review,* 40(3), pp. 698-736.

Craiger, P. 2006. Computer Forensics Procedures and Methods. In: Bidgoli, H. (ed.) *Handbook on Information Security,* Vol. 2. New Jersey: John Wiley & Sons. pp. 715-750.

Crisanto, J. C. & Prenio, J. 2020. Financial Crime in Times of COVID-19 / AML and Cyber Resilience Measures. Financial Stability Institute, *FSI Briefs*, 7.

De Hert, P., Parlan, C. & Thumfart, J. 2018. Legal Instruments Used in Courts Regarding Territoriality and Cross-border Production Orders: From Yahoo Belgium to Microsoft Ireland. *New Journal of European Criminal Law*, 9(3), pp. 326-352, https://doi.org/10.1177/2032284418801562.

Daskal, J. 2015. The Un-Territoriality of Data. *Yale Law Journal*, 125(2), pp. 326–398.

Doyle, S. 2018. *Quality Management in Forensic Science*. London: Elsevier.

Filipkowski, W. 2008. Cyber Laundering: An Analysis of Typology and Techniques. *International Journal of Criminal Justice Science*, 3(1), pp. 15-27.

Kyriakides, E., 2019. United States of America - The CLOUD Act, E-Evidence, and Individual Rights. *European Data Protection Law Review*, 5(1), pp. 99-106, https://doi.org/10.21552/edpl/2019/1/16.

Karagiannis, C. & Vergidis, K. 2021. Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal. *Information*, Vol. 12, pp. 181-197, https://doi.org/10.3390/info12050181.

Matić Bošković, M. 2021. Impact of Modern Technologies on Free Movement of Evidence in European Union. *Journal of Criminology and Criminal Law*, 59(3), pp. 123-140, https://doi.org/10.47152/rkkp.59.3.6.

Morgan, S. 2020. Cybercrime to Cost the World $10.5 Trillion Annually by 2025. *Cybercrime Magazine*. Cybersecurity Ventures. November 13, 2020. Available at: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

Pollitt, M., Casey, E., Jaquet-Chiffelle, D.O. & Gladyshev, P. 2019. *A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence*. National Institute of Standards and Technology – Organization of Scientific Area Committees for Forensics Science, Task Group on Digital/Multimedia Science, https://doi.org/10.29325/OSAC.TS.0002.

Savona, E. 2014. Organised crime numbers. *Global Crime*, 15(1-2), pp. 1-9, https://doi.org/10.1080/17440572.2014.886512.

Souto, A.M. 2013. Money Laundering, New Technologies, FATF and Spanish Penal Reform. *Journal of Money Laundering Control*, 16(3), pp. 266-284, https://doi.org/10.1108/JMLC-01-2013-0002.

Stefan, M. & Gonzalez Fuster, G. 2018. Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters – State of the Art and Latest Development in the EU and the US. *CEPS Paper in Liberty and Security in Europe*. Brussels: CPES.

Stoykova, R. 2021. Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence. *Computer Law and Security Review*, Vol. 42, https://doi.org/10.1016/j.clsr.2021.105575.

Swire, P., Hemmings, J. & Vergnolle, S. 2016. A Mutual Legal Assistance Case Study: The United States and France. *Wisconsin International Law Journal*, Vol. 34 (2), pp. 102-144, https://doi.org/10.2139/ssrn.2921289.

Tinoco-Pastrana, A. 2020. The Proposal on Electronic Evidence in the European Union. *Eucrim*, 1, pp. 46-50, https://doi.org/10.30709/eucrim-2020-004.

van Baar, R.B, van Beek, H.M.A. & van Eijk, E.J. 2014. Digital Forensics as a Service: A Game Changer. *Digital Investigation*, 11(S-1), pp. S54–S62, https://doi.org/10.1016/j.diin.2014.03.007.

van Wegberg, R., Oerlemans, J-J. & van Deventer, O. 2018. Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, 25(2), pp. 419-435, https://doi.org/10.1108/JFC-11-2016-0067.

Warken, C. 2018. Classification of Electronic Data for Criminal Law Purposes, *Eucrim*, pp. 226-234, https://doi.org/10.30709/eucrim-2018-023.

Marina M. Matić Bošković
Viši naučni saradnik, Institut za kriminološka i sociološka istraživanja, Beograd, Srbija
E-mail: *m.m.boskovic@roldevelopmentlab.com*

PRANJE NOVCA PUTEM VISOKOTEHNOLOŠKOG KRIMINALA I DIGITALNI DOKAZI

Sažetak

Široka zavisnost od digitalnih sistema i povećana vrednost digitalne trgovine u metaverzumu povećali su sajber ranjivost. Sajber-kriminal će biti profitabilniji od globalne trgovine svim glavnim ilegalnim drogama zajedno, dok *Cybersecurity Ventures* očekuje da će globalni troškovi sajber kriminala rasti za 15% godišnje do 2025. godine. Sajber kriminal je promenio tradicionalne metode pranja novca koje je teško otkriti jer se isti može počiniti bilo gde u svetu. Pretnja koju predstavljaju metodologije pranja novca sajber kriminala pogoršana je usled pandemije Covid-19.

Za istragu *cyber laundering-a* e-dokazi su ključni, što potvrđuje i procena Evropske komisije da 85% krivičnih istraga zahteva elektronske dokaze. Dodatni izazov za istražne organe za sprovođenje zakona predstavlja činjenica da organizovani sajber kriminal postaje sve organizovaniji i da se verovatnoća otkrivanja i krivičnog gonjenja procenjuje na 0,05% u SAD. Štaviše, digitalne dokaze često drže pružaoci usluga - privatne kompanije sa sedištem u drugoj zemlji, što uzrokuje mnoge prepreke pristupu tim podacima od strane istražnih organa.

U radu se identifikuje uticaj Covid-19 na sajber kriminal i povećani rizik od cyber laundering (sajber pranja novca). U vezi sa istragom i procesuiranjem sajber pranja novca, u radu se analiziraju izazovi istražnih organa da prikupe podatke i dokaze u slučajevima sajber pranja novca i napore vlasti EU i SAD da olakšaju pristup digitalnim dokazima i relevantnim podacima koje čuvaju pružaoci usluga. Rad ukazuje na moguće nedostatke predloženih instrumenata i potrebu efikasnog reagovanja i prilagođavanja promenama u sajber kriminalu.

Ključne reči: sajber pranje novca, međusobna pravna pomoć, digitalni dokazi, prikupljanje podataka, prekogranična saradnja.

Primljeno: 2. 11. 2022.
Prihvaćeno: 30. 12. 2022.