Jurisdictional Challenges of Cybercrime

***Dávid Tóth**[*] **– Zsolt Gáspár**[**]*

Abstract

As a result of the development of technology, the appearance of cybercrime set up new challenges for almost all fields of criminal law. New crimes appear in the criminal substantive law, like information system fraud, or criminal offenses related to non-cash payment instruments. The detection or seizure of electronic evidence can cause difficulties for the criminal procedure law, too (see the appearance of virtual currencies, e.g. bitcoin). According to the starting hypothesis of the study, the traditional principles used in international criminal law are not, or not sufficiently able to give adequate answers to the difficulties created by cybercrime.

The research aims to demonstrate and examine the practical and theoretical challenges revealed by cybercrimes. The first part of our research deals with the traditional principles of jurisdiction, and the theoretical and practical problems that can come up in the field of cybercrime. Relating to international cybercrime, positive jurisdictional collisions can be observed frequently, for which we devise suggestions. In the second part of our study, we investigate the difficulties and the institutional regards of the criminal cooperation connected to cybercrime. In the third part, we analyze The Convention on Cybercrime of the Council of Europe, whether if it provides suitable answers for jurisdictional challenges. In the closing part of our study, we summarize the conclusions and devise suggestions.

***Keywords**: cybercrime, jurisdiction, EU law, international law, Cooperation in criminal matters*

I. Introduction

In history, there have been several difficulties for the states in the cooperation in criminal matters. A traditional problem was, for example, the harm of sovereignty, the slow processes of extradition, the conflicts between the states. Despite these difficulties, some principles have been evolved, which can solve many questions (e.g. jurisdiction, extradition, legal aid).

With the development of society, the legal regulations became more and more complex in international criminal law[1]. Until the 20-21. century criminality was a local

[*] PhD, adjunct, Univesity of Pécs, Faculty of Law, Criminology and Penal Executional Law Chair

[**] PhD student, Univesity of Pécs, Faculty of Law, Criminology and Penal Executional Law Chair

[1] „The international criminal law is a segment of the international law and the national criminal law, which involves the institutions of the cooperation in criminal matters and the regulations of international crimes." Citing: László, Kőhalmi, 'A nemzetközi bűnügyi együttműködés [The international cooperation in criminal matters] ' in Ágnes, Balogh – Mihály, Tóth (eds), *Magyar büntetőjog Általános rész [Hungarian criminal law General part]* (Osiris 2010) 375.

phenomenon. The principles regulating the criminal jurisdiction were built to the basic axioms, that the dictum is a phenomenon bound to a determined geographical area. As a result of technological development, the appearance of cybercrime set up new challenges for almost every field of criminal law. New crimes appear in the criminal substantive criminal law, like the crimes conducted with information systems or the crimes related to the non-cash payment instruments. The investigation or seizure of electronic evidence can cause difficulties for the criminal procedure law also (see the virtual currencies, like the appearance of Bitcoin). Even before the appearance of cybercrimes, there were a rising number of delicts, which were able to harm or endanger two or more states' legal system due to the citizenship of the perpetrator, or the circumstances of the crime[2].

Cybercrime multiplies this phenomenon and changes the image of criminality in its basis, making it an international phenomenon that knows no borders. In the virtual space, for example, the crime of money laundering[3] has become more widespread. Cybercrime also provides a new financing area for the terrorists[4].

According to the initial hypothesis of the study, the traditional principles used in international criminal law cannot give adequate answers to the difficulties set up by cybercrime. In the first part of our study, we are dealing with the international sources of law and the jurisdictional principles in general. After that, in correspondence with the aim of the research, we are presenting and observing the practical and theoretical challenges connected to cybercrimes. In the third part of the study, we are presenting the regional efforts of the European Union against cybercrime.

II. Jurisdictional principles

The jurisdiction is a legal term used in international law. Under this institution a state has the right to legislate, apply and enforce the law. The jurisdiction creates the possibility of the application of the law and it is also it's requisite. We can talk about the criminal jurisdiction in a wider and a narrower sense. Criminal jurisdiction in a wider sense means that the state has the right to create a criminal law regulation. The narrower sense of criminal jurisdiction consists of the applicability of the national criminal regulation and the range of the competence of the authorities proceeding in criminal cases[5]. The Permanent Court of International Justice stated in the Lotus-case in 1927, that international law does not limit the criminal jurisdiction of the state, it

[2] Péter, M. Nyitrai, *Nemzetközi és Európai Büntetőjog [International and European Criminal Law]* (Osiris 2006) 208.

[3] István László, Gál, 'The Techniques of Money Laundering.' in István László, Gál – László, Kőhalmi (eds.), *Emlékkönyv Losonczy István professzor halálának 25. évfordulójára*. (Pécsi Tudományegyetem, Állam- és Jogtudományi Kar 2005) 129-138.

István László, Gál, 'A pénzmosás szabályozásának régi és új irányai a nemzetközi jogban és az EU-jogban [The old and new tendencies in the regulation of money laundering in the international and EU Law]' Európai Jog. [2007] 12-23.

[4] See further about the financing of terrorism: István László, GÁL, 'Új biztonságpolitikai kihívás a XXI. században: a terrorizmus finanszírozása. [New challenges of security policy in the 21st century: the financing of terrorism] ' Szakmai Szemle [2012] 5-15.

GÁL István László, *A terrorizmus finanszírozása: Die Terrorismusfinanzierung, [The financing of terrorism]* (PTE Állam- és Jogtudományi Kar Gazdasági Büntetőjogi Kutatóintézet 2010)

[5] cf Nyitrai (n 2) 209.

can enforce it if it has an effective possibility to do so[6]. An exception of the main rule is that during the practice of its penitentiary power, a state cannot intervene in another state's internal affairs, because that is its exclusive right. Under the decision of the Lotus-case, the territorial principle is not sole, therefore the jurisdiction of the states can be extended to the crimes committed by foreign citizens abroad[7]. If a state decides to extend its jurisdiction to the territory over its borders, then international only requires that's some kind of connection exists between the punishable conduct and the sovereignty of the country.

Several principles deal with this connection and are generally accepted in international law like the territorial, the personal, the protective and the universality principle. In these cases the state exercises its original sovereignty and are called original jurisdictional cases. Occasionally derivative jurisdiction can also occur in a few cases, where the state with the primary jurisdiction hands over its jurisdiction to another state while using the so-called aut dedere aut judicare or in other words representation principle[8]. The latter one serves to fill a regulatory gap. This supplements the criminal jurisdiction of other countries.

In legal cases containing international elements, conflicts can appear on deciding which country has jurisdiction. The Anglo-Saxon literature lists the following jurisdictional principles:

- *jurisdiction to prescribe*: the establishment of the future assertion of the state's punitive power. This answers the question, if there is any jurisdictional principle (e.g.: the territorial principle), according to which, an act can be subsumed under the inner criminal law. The actual practice of punitive power can emerge after this. In the continental legal systems, as well as in the Hungarian, we can find the jurisdictional regulations in the territorial and personal scope of the law. Another legal source of this area are the conventions on international legal aids in criminal matters[9].
- *jurisdiction to adjudicate*: the second term means the jurisdiction of the sentencing, based on which the sovereign power can subsume people or organizations under the procedure of the state court to decide whether an infringement has happened or not.
- *jurisdiction to enforce*: the third term means the possibility and limits of the actual practice of jurisdiction. The executive jurisdiction also involves the extradition after the decision[10].

---

[6] The essence the case is the following: the French ship, named Lotus crashed with a Turkish ship on the Sea of Marmora. After the accident the ships came to anchor in Istanbul. The two states got into a debate in front of the International Court of Justice due to the case. The question was if Turkey had jurisdiction over the French citizens who were involved in the case. According to the decision of the International Court of Justice, there is no regulation in the international law, which states that only the country has jurisdiction whose flag the ship wears. That means Turkey can assert its jurisdiction based on the presumption of sovereignty. See further: János, Bruhács, *Nemzetközi Jog I. Általános rész. [International Law I. General part.]* (Dialóg Campus Kiadó 2009) 21.

[7] Péter, Polt, 'A magyar büntető joghatóság. [The Hungarian criminal jurisdiction.]' in Polt et. al. (eds.) A Büntető Törvénykönyvről szóló 2012. évi C. törvény nagykommentárja. (Opten 2016) 26.

[8] Katalin, Ligeti, *Büntetőjog és bűnügyi együttműködés az Európai Unióban [Criminal law and Cooperation in criminal matters in the European Union]* (Közgazdasági és Jogi Könyvkiadó 2004) 43.

[9] ibid 43-44

[10] Henry Jr. H. Perritt, 'Jurisdiction in Cyberspace' Villanova Law Review [1996] 3.

The jurisdiction to prescribe can be decided based on various principles. Based on the territorial principle, the criminal law of the sovereign state has to be applied to every crime committed within the territory of the country, irrespectively to every other circumstance (e.g. the citizenship of the perpetrator or the victim)[11].

The quasi territorial principle extends this jurisdiction to ships and aircraft that sail or fly under the flag of the state[12]. This principle is often called the flag principle as well[13].

Under the nationality principle, the state can impeach its citizens, no matter whether they committed the crime in the country or abroad. This principle is called the active nationality (personality) principle. The other form of the principle is the passive nationality principle (which is also contained in the Hungarian Criminal Code). Based on this principle, the state can expand its jurisdiction for the crimes committed against its citizens abroad[14].

According to the self-defense of the state principle *(principium reale),* the state can sanction the people whose act harms the values or subjects protected by the criminal law system of the country, irrespectively to the citizenship of the perpetrator or the location of the act[15].

Based on the universality principle, the crimes harming the recognized subjects of law can be penalized and subsumed under the jurisdiction of the state, irrespectively to the location of the act or the citizenship of the victim or the perpetrator. It is also called the absolute punitive power, which usually appears in international conventions and expresses the sovereignty of the states. It is disputed though, which crimes can be subsumed under the principle of universality principle[16]. According to the fifth article of the International Criminal Court Statute approved on 17th July 1998 in Rome, the crimes that are under the Court's jurisdiction are the followings:

- the crime of genocide;
- crimes against humanity;
- war crimes;
- and the crime of aggression[17].

During the development of international law, the nationality jurisdiction has appeared earlier than the territorial but nowadays the territorial jurisdiction is applied more preferably by the states. The nationality principle did not disappear from the practice, it only has been reversed compared to by the application of the territorial principle, as a principle of jurisdiction[18].

---

[11] István László, Gál, 'Jogszabálytan. [Legal dogmatics]' in Balogh Ágnes – Tóth Mihály, *Magyar Büntetőjog Általános Rész.* (Osiris 2015) 75-76.

[12] cf Ligeti (n 8) 44.

[13] Helmut Satzger, *International and European Criminal law* (C.H. Beck, 2012) 17.

[14] Krisztina, Karsai, 'A magyar büntető joghatóság [The Hungarian criminal law jurisdiction]' in Krisztina, Karsai (eds.) *Nagykommentár a Büntető Törvénykönyvhöz: Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez,* (Wolters Kluwer 2019) 39-40.

[15] cf Gál (n 11) 75-76.

[16] cf Ligeti (n 8) 47.

[17] See further: Ferenc, Sántha, 'A Nemzetközi Büntetőbíróság joghatóságába tartozó nemzetközi bűncselekmények vázlata [Outline of international crimes within the jurisdiction of the International Criminal CourtOutline of international crimes within the jurisdiction of the International Criminal Court]' In Bragyova, András (eds.) *Tanulmányok a bűnügyi tudományok köréből.* (Gazdász Elasztik 2013) 170-197.

[18] A. Imre Wiener, 'A Nemzetközi Büntetőbíróság joghatóságáról' [About the jurisdiction of the International Criminal Court] Magyar Jog [2001] 457.

III. The regulation of the jurisdiction in the field of international cybercrime

Several international sources of law deal with the question of jurisdiction in connection with cybercrime. We would highlight the followings without the intention of being exhaustive:

- The Convention on Cybercrime accepted on 23rd November 2001 in Budapest by the Council of Europe deals with the question of jurisdiction;
- Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.1.2003, ETS No. 189, Article 4. (1);
- Arab Convention on Combating Information Technology Offences, Cairo, 21.12.2001, Article 30. (1)(a).

What is common in the above-listed conventions, that they all consider the territorial principle as a primary jurisdictional rule. In our study, we are focusing on the Budapest Convention on Cybercrime, due to its Hungarian relations.

Until September 2020, the international convention was ratified by 65 countries, inter alia, by Hungary, too.

Our country promulgated the convention with the Act LXXIX of 2004.

The jurisdictional regulations of the convention can be found in Article 22 of Section 3. Based on this regulation, states can establish jurisdiction over any offense committed in its territory; or onboard a ship flying the flag of that state; or onboard an aircraft registered under the laws of the state; or committed by one of its nationals. The signing parties can present their reservations or conditions against the regulations of the convention.

The convention also gives solutions to jurisdictional conflicts. When more than one Party claims jurisdiction over an alleged offense established following this Convention, the Parties involved shall, where appropriate, consult to determine the most appropriate jurisdiction for prosecution[19].

The question of extradition is tightly connected to the jurisdiction, which is also regulated by the cybercrime convention. According to Article 24: *"This article applies to extradition between Parties for the criminal offenses established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty."*

Where different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply[20].

The criminal offenses described in paragraph 1 of this article shall be deemed to be included as extraditable offenses in any extradition treaty existing between or among the Parties. The Parties undertake to include such offenses as extraditable offenses in any extradition treaty to be concluded between or among them[21]. It is an important rule, that the extradition should meet the requirements set up in the

[19] Budapest Cybercrime Convention, Article 22. 5.
[20] Budapest Cybercrime Convention, Article 24. 1.
[21] Budapest Cybercrime Convention, Article 24. 2.

requested country's national law or the extradition treaties in force, without that, the extradition request can be denied.

If extradition for a criminal offense referred to in the Budapest Cybercrime Convention is refused solely on the basis of the nationality of the person sought, or because the requested state deems that it has jurisdiction over the offense, the requested state shall submit the case at the request of the requesting state to its competent authorities for prosecution and shall report the outcome to the requesting state in due course[22].

Similarily to the convention, the fifth point of Article 15 of the United Nations Convention against Transnational Organized Crime[23] also declares that if a State Party *"has been notified, or has otherwise learned, that one or more other States Parties are conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another to coordinate their actions."*[24]

In a summary, the presence of the Budapest Cybercrime Convention is positive, because it laid down the basis of cooperation for the states involved. From the other side – according to our point of view – the regulations of the convention should be renewed because it still does not solve several questions and problems, that cannot be dealt with under the territorial principle. The consultation is a necessary precondition, but it does not give a concrete answer or at least a guideline to the problems. Until today, international law did not set up a priority order between the jurisdictional principles[25]. As these types of crimes are getting more frequent, the slow and difficult consultation procedures will not be sufficient in the fight against cybercrimes. It might enlarge the problem, that a lot of times these negotiations does not lead to successful result between the states.

IV. Theoretical problems in cybercrime cases

4.1. Which cybercrimes can set up jurisdictional problems?

In this chapter, we would like to present through hypothetic examples, which jurisdictional problems can appear in the cases of crimes realized in cyberspace. Various types of cybercrimes can be differentiated. According to a theoretical division, we can make a difference between cybercrimes crossing local and international barriers. In the former case, there is usually no territorial jurisdictional problem. At most, the nationality of the perpetrator, or the victim, can bring an international element to the case, which is relatively easier to resolve through the traditional principles of international criminal jurisdiction (territorial principle, nationality principle etc.). However, inner jurisdictional disputes can be caused by local cybercrime where in some cases it is difficult to decide which court has competence of the case[26].

---

[22] Budapest Cybercrime Convention, Article 24. 6.

[23] About organized crime see further: Mihály, Tóth – László, Kőhalmi, 'A szervezett bűnözés [The organized crime]' in Borbíró et. al. (eds.) *Kriminológia.* (Wolters Kluwer 2016) 603-625.

[24] <https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf> accessed 19 September 2020.

[25] Susan W. Brenner, 'Cybercrime jurisdiction.' Crime, law and social change. [2006] 189-206.

[26] See further: Tibor, Ibolya, *A számítástechnikai jellegű bűncselekmények nyomozása [The investigation of IT crimes]* (Patrocinium Kiadó 2012)

The other case is the so-called international or transnational cybercrime, where the perpetrator and the victim are located in different states.

Working in cross-border cyberspace grants even more benefits for the perpetrators, they can stay hidden and they can hide their identity, they can focus on more victims, causing even bigger damages in a short time. The perpetrator can aim at hundreds or even thousands of victims, for example with a so-called distributed denial-of-service (abbreviated DDoS) attack.

Jurisdictional conflicts can appear when more states have the right and the intention to proceed in a criminal case containing international elements (positive jurisdictional collision). The negative jurisdictional conflict is when no state has the right or the intention to proceed in a criminal case. This case is also called *vacuum iuris* in latin[27].

4.2. Hypothetical example for jurisdictional conflict

The following hypothetic case can be an example of a positive jurisdictional collision. A perpetrator from Congo commits a so-called "419 fraud" (which stands for the 419th paragraph of the Nigerian Criminal Code) to deceive English, Brazilian and Chilean victims. If all three countries start a criminal procedure at the same time against the perpetrator, it will lead to a positive jurisdictional conflict. All the countries valuate the case differently in consonance with their criminal codes (e.g. fraud, computer fraud, online abuse). Also, there are differences between the countries in the number of victims and on the scale of the caused damages. The question is given, that in the case of positive jurisdictional collision, which state has the priority against the other states, to proceed in the case.

Pursuant to Susan Brenner, the following factors should be taken into consideration while solving a positive jurisdictional conflict:

- procedural and practical processes, which were used to solve similar conflicts,
- standards, which were used to solve other kinds of jurisdictional conflicts,
- the special characteristics of cybercrimes[28].

However, Brenner highlights that alongside the mentioned ones, other aspects can also be taken into consideration with different emphasis. In the next subsection, we are examining how efficiently can the different jurisdictional principles solve the hypothetical case.

According to Zoltán Nagy, in addition to the above, the following aspects should be taken into account in jurisdictional issues:

- the interests of the defendant,
- the interests of victims and witnesses,
- the admissibility of the evidence, or
- delays in the case[29].

4.3. Which jurisdictional claim has priority?

4.3.1. The place of commission

Current international law most generally accepts the principle of territoriality as a principle of jurisdiction. Based on our hypothetical case, pursuant to the territorial

---

[27] cf Ligeti (n 8) 50.

[28] cf Brenner (n 25) 198.

[29] Zoltán András, Nagy, 'A joghatóság problémája a kiberbűncselekmények nyomozásában [The problems in the investigation of cybercrimes]' in Homoki-Nagy et. al. (eds.): *Ünnepi kötet dr. Nagy Ferenc egyetemi tanár 70. születésnapjára.* (Szegedi Tudományegyetem Állam- és Jogtudományi Kar 2018) 761

principle, the Congolese perpetrator should be held liable in Congo, because he continued his activity there. On the other hand, there was no victim of the crime in Congo, so there was no question of instituting criminal proceedings in that country. The victims report the crime in their own country and criminal proceedings are initiated there. All three countries represented by the victims (England, Brazil and Chile) cannot invoke the territorial principle because the perpetrator did not commit a criminal offense in their country. Another problem can be if the place of the offense and the IP address (see chapter 5.1 for more details) point to an unknown location. With the use of the so-called VPN services, the authorities would discover a location where the perpetrator has never been (points to a false place of commission).

Based on these facts, the territorial principle is not a solution for the hypothetical example.

4.3.2. The location of the arrest of the perpetrator

It could be a logical solution if the arresting state had the priority to proceed against the presumed offender. In traditional crimes this is a frequently used solution, but international cybercrime makes this field more complicated.

It is possible, that the perpetrator in the arresting state has caused damages only to a few victims, but to hundreds in another state, so this solution of the jurisdictional conflicts may seem unfair.

Let us assume that the Congolese perpetrator committed a terrorist act in England, instead of cyber-frauds. The perpetrator exploded a bus, in which citizens of Brazil and Chile died. England is detaining the perpetrator for committing a terrorist act. All states want to prosecute him. The relevant factor in the case is that the offense was committed in England, which gave the English authorities priority to institute criminal proceedings. If England successfully prosecutes, the other countries may decide not to continue the proceedings and are content with the English sentence.

In the case of cyber-fraud, the location where he committed the crime is completely irrelevant, just like the place of the victims. The legitimacy of the proceedings requires some other decisive argument or reason for the English State to prosecute the Congolese perpetrator. Such an expediency argument may be that the evidence is found in the country where the perpetrator committed the crime.

The place of detention may, in our view, provide a more effective solution in such cases than the application of the territoriality principle.

4.3.3. The location of the occurrence of the harm

In jurisdictional disputes, guiding factors can be the damage caused by the perpetrator and the number of victims. However, these should not be decisive either, because it can be problematic if the same amount of damage has occurred or the number of victims is the same in each country. It is also possible that the offender has caused millions in damage to a victim in England and, also caused small amounts of damage to hundreds of Brazilian citizens. Quantifying industrial espionage or identity theft can cause even greater difficulties in establishing a jurisdictional sequence[30].

Notwithstanding the above, it is important to take the magnitude of the damage into account in such matters, but it cannot in itself be a decisive argument for deciding jurisdiction.

[30] cf Brenner (n 25). 200-201.

4.3.4. The citizenship of the victim (passive personality)

The nationality of the victims has traditionally been of great importance in jurisdictional matters. Of course, this may be an important consideration in deciding the case, but it is still not certain to be decisive. All three states have victims, so the jurisdictional dispute can't resolved by this factor alone[31].

The principle of passive personality may be a more appropriate solution than the territorial principle, as in a significant number of cases victims report the crime and the criminal proceedings will presumably be initiated in these countries. On the other hand, this can also cause logistical difficulties, if the perpetrator is in a very distant country.

4.3.5. The citizenship of the perpetrator

Based on the nationality of the perpetrator, Congo would have the right and duty to proceed in the case. The application of the principle of nationality implies that a State is responsible for the actions of its own nationals, so that it will be responsible for prosecuting and bearing the costs of crime.

As Geoffrey R. Watson wrote, "*If disturbance of the legal order within a State's territory is considered the most persuasive reason for penal jurisdiction, such disturbance may be found in the presence unpunished of an offender who has committed crime elsewhere"*[32].

The application of the principle of nationality can be strengthened by the application of the principle of "*aut dedere, aut judicare"* ((Latin for "either extradite or prosecute"). This principle refers to the legal obligation of states under public international law to prosecute persons who commit serious crimes with international element where no other state has requested extradition. This presupposes that the "A" citizen offender flees to country "B" from the investigating authorities, and in this case, they are obliged to extradite the perpetrator or at least initiate criminal proceedings[33].

V. Practical difficulties

5.1. Technical background

The Internet Protocol (or shortly IP) is a unique set of identification numbers assigned to computer devices to be able to recognize each other and send data to each other through the Internet[34]. IP addresses are maintained by an international non-profit company called Internet Corporation for Assigned Names and Numbers (ICANN for short), which was founded in 1988, and which also performs coordination tasks[35]. IP addresses can also be linked to geographical locations, which as a result could determine the origin of a particular cybercrime based on the attacker's IP address. However, the problem is rooted in the fact that no competent perpetrator

[31] Ibid 202-204.

[32] Geoffrey R. Watson, 'The Passive Personality Principle.' in Texas International Law journal [1993] 17.

[33] BRENNER, Op.Cit. p. 198.

[34] Da-Yu Kao – Shiuh-Jeng Wang, 'The IP Address and Time in Cyber-Crime Investigation.' Policing: An International Journal of Police Strategies & Management 32, [2009] 195.

[35] <www.icann.org/history> accessed 19 September 2020

uses their IP address for an attack, also, there is a huge variety of techniques available to them to maintain their anonymity[36]. On one hand, the IP address of the device used by the attacker can be easily exchanged for the IP address of another device, making the attack appear to come from a different location than where it originates[37].

Besides, changing the IP address is a very easy-to-learn technique, so it is used by many users, and there are also several guides on online interfaces that describe in detail how to use this method[38]. Another preferred solution is the use of private or public proxy servers, which act as a kind of intermediary tool between the attacker's computer system and the victim's system so that the attacker can remain anonymous[39]. Public servers are more accessible. On the other hand, because they are used by many, they are slower, less reliable than private servers. Nowadays, such services can be accessed relatively cheaply and easily, as countless companies lease them[40]. In addition to the formerly mentioned ones, the most commonly used and most effective technique is when they remotely take control over a device in a foreign country, and using that device they launch an attack on a third party. This so-called "victim-computer" is usually the last piece in a long chain that is composed of several devices and states[41].

5.2. The Ivanov and Gorshkov-case

The US government claims that Aleksey Vladimirovich Ivanov in 2000 hacked into the computer system of the Online Information Bureau, Inc. (OIB) and took the key passwords, with which he could take over control of the entire system of the OIB. According to the indictment, Ivanov then began to threaten to destroy the company's entire computer system and demanded roughly $ 10,000 in exchange for not doing so. When he was rejected, he sent another threatening e-mail to an OIB-employee working in Vernon, Connecticut, using the system of Lightrealm (an internet provider from Kirkland, Washington) remotely from Russia[42].

The FBI agents caught the perpetrators in a very unusual way, as part of which, disguised as a businessman, they lured the two Russian hackers to Seattle for a job interview. During the interview, they had to show their IT skills on a computer on which the FBI had previously installed spyware programs. With the help of these programs, the FBI agents obtained those passwords from the hackers, which gave them access to their computers, from which federal agents later backed up the data and then used it as evidence in the criminal proceedings[43].

Aleksey Vladimirovich Ivanov and Vasiliy Gorshkov have been indicted in the United States for conspiracy, computer fraud, and related activity, extortion, and

---

[36] Jean-Baptiste Maillart, 'The limits of subjective territorial jurisdiction in the context of cybercrime' ERA Forum [2019] 378-379

[37] ibid 379.

[38] See e.g.: <https://www.safervpn.com/blog/how-to-change-ip-address> accessed 19 September 2020

[39] cf Maillart (n 36) 379.

[40] <https://medium.com/@ProxiesAPI.com/public-proxy-servers-vs-private-proxy-servers-for-web-scraping 1c5b27549cca> accessed 19 September 2020

[41] cf Maillart (n 36) 379.

[42] <https://law.justia.com/cases/federal/district-courts/FSupp2/175/367/2419190/> accessed 19 September 2020

[43] Önder Kutay Seker, *International Regulation of National Cybercrime Jurisdiction.* (Tilburg University 2012) 10.

unauthorized access to assets. Ivanov argued, that because he was in Russia at the time when the crimes were committed, he could not be charged with the violation of the law of United States[44]. However, the court found that it has jurisdiction over the case, on one hand, because the intentional and actual harmful effects of Ivanov's acts (committed in Russia) developed in the United States, on the other hand. After all, all the substantive legal facts realized by Ivanov are applicable regardless of the territory, according to Congress[45].

The Russian authorities, on the other hand, had a different view about the case, arguing that the decision violated the traditional principles of jurisdiction, besides, they were criticizing the events of the investigation and the obtainment of the evidence, giving voice to their disagreement with the accusation of the FBI agents in Russia of hacking, which in itself raises another issue of jurisdiction[46].

5.3. The Gary McKinnon-case

Gary McKinnon was an unemployed computer administrator from the UK who gained unauthorized access to 97 U.S. government computers from his home in London. Among other things, he has been proven to erase data from their operating systems, and as a result, the U.S. Army had to shut down more than 2,000 from its computers in Washington for 24 hours. In November 2002, the states of New Jersey and Virginia also raised charges against McKinnon. The U.S. government wanted to make a bargain with McKinnon's lawyers, as part of which McKinnon would plead guilty and give consent to his extradition, in exchange for spending 37-46 months in prison, of which he could return home after serving 6-12 months in the US. to serve his remaining sentence in the United Kingdom. Then, he could have been released under English law, as a result of which he would only have to spend between 18 and 24 months in prison, but if he did not cooperate, he would have had to face 8-10 years (of which max. 15% could have been waived) in a high-security prison without the possibility of returning home[47]. In August and September 2004, after McKinnon refused the deal, the states of Virginia and New Jersey also sought an arrest warrant against McKinnon, and they also requested his extradition from the Secretary of State. After accepting the applications, McKinnon was arrested on June 7, 2005, and after hearings in 2006, the Secretary of State informed him that he had issued an order for his extradition. In 2008, the House of Lords dismissed his appeal against his extradition[48]. However, in 2012, Home Secretary Theresa May revoked the extradition warrant against McKinnon because he had been diagnosed with Asperger's Syndrome and, according to experts, he would be at risk of suicide if he was extradited[49].

---

[44] Ibid 10.

45 <https://law.justia.com/cases/federal/district-courts/FSupp2/175/367/2419190/> accessed 19 September 2020

[46] cf Seker (n 43) 10.

[47] Nicola Padfield, 'Shining the Torch on Plea-Bargaining.' The Cambridge Law Journal [2009] 11-14.

[48] <https://publications.parliament.uk/pa/ld200708/ldjudgmt/jd080730/mckinn-1.htm> accessed 19 September 2020

[49] <https://www.gov.uk/government/news/theresa-may-statement-on-gary-mckinnon-extradition> accessed 19 September 2020

VI. The European Union's institutional and regulatory solutions

6.1. Regulations connected to cybercrime

The first EU regulation dealing with cybercrime jurisdiction was the Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, in the Article 17. According to this article, the State has jurisdiction and shall take the necessary measures, if the offense was entirely or in part committed within its territory or the offender is one of their nationals. If a State establishes its jurisdiction over an offense regardless of the above-mentioned cases, the State shall inform the Commission. This can happen in the following cases:

- if the offense is committed against a national of that Member State or a person who has his or her habitual residence in the territory of that Member State; or
- the offense is committed for the benefit of a legal person established in the territory of that Member State; or
- the offender is habitually resident in the territory of that Member State[50].

The second significant source, the Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA brought only minor charges in connection with jurisdiction. According to Article 12 of the Directive, a State can establish jurisdiction if the crime was committed in whole or in part within their territory, or by one of their nationals, at least in cases where the act is an offense where it was committed.

Regarding the territoriality principle, the directive also stipulates that if the offender is physically present in the territory of a State at the time when the offense is committed, it shall have jurisdiction, regardless of whether the offense was against an information system within its territory, and also if the offender is not in the territory of that State but the offense is against an information system located within its territory. Similarly to the Directive 2011/92/EU, the State shall inform the Commission in the following cases:

- the offender has his or her habitual residence in its territory, or
- the offense is committed for the benefit of a legal person established in its territory[51].

The Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA applies the same logic as the before-mentioned directives. The jurisdictional regulations can be found in Article 12, according to which a State can establish jurisdiction if the offense was entirely or in part committed within its territory or the offender is one of their nationals. The

[50] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, Article 17.

[51] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Article 12.

Commission should be informed if a Member State establishes its jurisdiction over an offense that was committed outside of its territory and:

- the offender has his or her habitual residence in its territory,
- the offense is committed for the benefit of a legal person established in its territory,
- the offense is committed against one of its nationals or a person who is a habitual resident in its territory[52].

6.2. The institutional side of the fight against cybercrime: the Europol

The judicial and police cooperation has developed in parallel with the strengthening of economic ties between the Member States of the European Union. The abolition of controls has led to an increase in cross-border crime, so there has been an urgent need to institutionalize the cooperation between the Member States in these areas[53].

Criminal judicial cooperation between the Member States and the establishment of the European Police Office (Europol for short) was already an objective set out in the 1992 Maastricht Treaty, with the idea of establishing police cooperation between the Member States to strengthen the fight against terrorism, drug trafficking and other forms of international crime, based on Europol by ensuring the flow of information. In 1995, the Europol Drugs Unit (EDU) was set up temporarily with the main task of curbing drug trafficking and money laundering[54].

However, in the following year, the Council of Ministers extended its powers and Europol became generally accepted among the Member States[55].

The main objective of Europol is to facilitate the work of Member States' investigative authorities and increase their effectiveness in the fight against terrorism and international crime.

Its main tasks include (among others):

- the facilitation of the flow of information among the Member States,
- the provision of assistance to the operations of the investigative authorities of the Member States,
- collecting, organizing, and investigating information on crime,
- the development and maintenance of the computerized IT systems for data analysis,
- providing practical and technical assistance to the investigations processed by the Member States' investigative authorities[56].

---

[52] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, Article 12.

[53] Željko Nikač, The European Arrest Warrant-Europol.International Journal of Economics and Law [2014] 91-92.

[54] Eszter, Karoliny, 'Igazságügyi együttműködés büntetőügyekben; a kölcsönös elismerés elve. A ne bis in idem elve az Európai Unió Bíróságának ítélkezési gyakorlatában. [Cooperation in criminal matters, the mutual recognition and the principle of ne bis in idem in The practice of the European Court of Justice]' in Mohay Ágoston – Szalayné Sándor Erzsébet (eds*.): Az Európai Unió Joga.* (Dialóg Campus Kiadó 2015) 206-217.

[55] <https://www.policija.si/eng/areas-of-work/other-areas/international-cooperation/europol> accessed 19 September 2020

[56] cf Nikač (n 53) 92.

The organization's competencies have been expanded during the years, which now deals with the prevention and the combat of the following crimes: trafficking in human beings, illicit car trafficking, human smuggling, child pornography, trafficking in nuclear and radioactive materials, money laundering[57]. In 2013, Europol set up the European Cybercrime Center to support strengthened EU legislation on cybercrime and to protect EU citizens, governments, and businesses. The ECC publishes an annual report on the Internet Organized Crime Threat Assessment (IOCTA for short), which also gives proposals for strengthening the legislation in this area and provides key information for Member State governments and EU citizens and businesses. Since 2014, the ECC has a cybercrime task force (the so-called Joint Cybercrime Action Taskforce or shortly J-CAT), which, as an action group, inter alia, coordinates the cross-border cybercrime investigations and operations. The establishment of the mentioned institutions has led to several successes, including:

- the coordination of a joint operation, including private-sector partners to target a botnet called Ramnit, that had infected millions of computers around the world,
- coordination with Eurojust in an operation targeting large-scale malware attacks that originated in Ukraine and that were being investigated by several agencies – an operation that led to tens of arrests and continues to supply evidence that supports other cybercrime investigations,
- an operation targeting a major cybercriminal forum engaged in trading hacking expertise, malware and botnets, Zero Day Exploits, access to compromised servers, and matching partners for spam campaigns and malware attacks[58].

6.3. The European Arrest Warrant

The European arrest warrant is a decision issued by a judicial authority issued in a Member State of the European Union to have the person apprehended by another Member State and hand it over to the issuing judicial authority[59]. The primary purpose of the EAW is the conduction of the criminal proceedings and, also, the arrest and handover of the requested person to enforce a custodial measure and/or a custodial sentence[60]. In Hungary, the regulation was implemented with the Act CLXXX. of 2012 on the Cooperation in Criminal matters with Member States of the European Union.

It applies to offenses punishable by at least 12 months' imprisonment and penalties involving deprivation of liberty of at least four months. The arrest warrant only sets aside from double criminalization only in the case of cataloged offenses, but in those cases only, if the maximum sentence under the law of the issuing State reaches a term of imprisonment of at least three years[61]. Groups of cataloged crimes without the need for completeness: participation in a criminal organization, terrorism, trafficking in human beings, sexual exploitation of children and child pornography, illicit trafficking in arms,

---

[57] Péter, Fejes, 'Az Európai Unió, mint büntető joghatóság? [The European Union as a criminal jurisdiction?]' in Európai Jog [2005] 5.

[58] <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime> accessed 19 September 2020

[59] László, Kőhalmi, 'Az európai bűnügyi együttműködés. [The European cooperation in criminal matters]' In: Ágnes Balogh – Mihály Tóth (eds.)*Magyar büntetőjog Általános rész.* (Osiris 2010) 390.

[60] Petra Bárd, '*Az európai elfogatóparancs Magyarországon. [The European arrest warrant in Hungary]*' (Országos Kriminológiai Intézet 2015) 26.

[61] Act CLXXX. of 2012, 3.§ (3)

munitions, and explosives, illicit trafficking in narcotic drugs and psychotropic substances, corruption, money laundering, intentional homicide, and cybercrime, but also the Council of European Union can extend the scope of cataloged criminal offenses[62]. Regarding the extradition, there are certain types of exceptions to the rules of the European Arrest Warrant, based on which the Metropolitan Court refuses (for mandatory reasons) or may refuse extradition (for optional reasons).

The mandatory grounds for refusal are set out in the 3rd subchapter of the Act CLXXX. of 2012, for example, if the requested person is not punishable due to childhood, or according to Hungarian law the punishability is expired, if the offense on which the European arrest warrant is based falls within Hungarian jurisdiction etc.[63]. Extradition shall also be refused if it was issued to enforce a decision rendered in the absence of the requested person, unless:

- the requested person has been duly notified,
- an authorized or seconded lawyer acted at the hearing on behalf of the requested person,
- the decision has been served, the person concerned has been duly informed about the remedies but has not exercised it or the decision has not been served to the requested person, but after the handover, it shall be served and the requested person shall be informed about the ordinary and extraordinary remedies and the deadline[64].

Besides, extradition should also be refused if the European arrest warrant has been issued to serve a custodial sentence or measure involving deprivation of liberty and the requested person is a Hungarian citizen who resides in the territory of Hungary. In this case, the Minister of Justice shall initiate (at the Member State) the taking over of the execution of the sentence or custodial measure of the sentenced person[65]. The act also summarizes in the same subchapter the optional grounds for refusal, in which cases the Metropolitan Court may decide on the execution or refusal of the European Arrest Warrant:

- if the arrest warrant relates to a criminal offense committed in whole or in part in the territory of Hungary[66], or
- if two or more Member States have issued a European arrest warrant against the same person, the Metropolitan Court shall decide, considering all the circumstances, which European arrest warrant should enjoy priority[67].
- If there are no grounds for refusal, a European Arrest Warrant can be requested. The application must include:
- the personal data and nationality of the requested person,
- name, address, telephone number, the e-mail address of the requesting authority,
- the arrest warrant, the evidence of the proceedings to be enforced, or any other judicial decision which they intend to enforce,
- the nature and legal assessment of the act committed,
- a description of the circumstances of the offense, including the time, place, and degree of guilt, and

---

62 cf Bárd. (n 60) 25-27.
63 Act CLXXX. of 2012, 5.§
64 Act CLXXX. of 2012, 6.§
65 Act CLXXX. of 2012, 8.§ (1)
66 Act CLXXX. of 2012, 7.§
67 Act CLXXX. of 2012, 9.§ (1)

- the penalty imposed, if there is already a final decision in the case, or, if not, the penalty which may be imposed in the Member State[68].

An application for a European Arrest Warrant may arise for several reasons, in particular for the investigation of a criminal offense, to enforce a final judgment or for pre-trial detention, providing an opportunity to fight transnational crime and other forms of crime more effectively.

VII. Conclusion

International cybercrime poses new challenges for states. In many cases, it can lead to the positive and negative collision of jurisdiction. While some jurisdictions have adopted cybercrime-specific jurisdiction rules, the principles underlying fair enforcement of criminal jurisdiction may also justify the enforcement of jurisdiction against internal and external criminals.

A clear set of rules at the EU level could serve as a compass for the Member States in matters of jurisdiction, but directives in this area do not make it entirely clear which state is entitled to act in a particular case. From an institutional point of view, however, Europol's coordinating work across national jurisdictions and its growing role in the European area can be seen as a positive outcome. In addition to Europol, the role of the European Arrest Warrant should also be emphasized in the fight against cybercrime, which is the basis for international criminal cooperation and the recognition of other Member States' jurisdictions.

The principles of jurisdiction are difficult to rank. In many cases, it may be case-specific to decide which principle of jurisdiction may be the best solution. It would be necessary to renew existing international legislation or to adopt the new convention that emphasizes the principle of citizenship or passive personality. Also, it is appropriate for the states to lay down specific rules. Adopting special laws for cybercrime, (as in the United States,) can also be a solution to jurisdictional issues[69].

References

1. Bárd P, *Az európai elfogatóparancs Magyarországon. [The European arrest warrant in Hungary]* (Országos Kriminológiai Intézet 2015)

2. Brenner S.W, 'Cybercrime jurisdiction.' Crime, law and social change. [2006]

3. Bruhács J, *Nemzetközi Jog I. Általános rész. [International Law I. General part.]* (Dialóg Campus Kiadó 2009)

4. Da-Yu K – Shiuh-Jeng W, 'The IP Address and Time in Cyber-Crime Investigation.' iPolicing: An International Journal of Police Strategies & Management 32, [2009]

5. Fejes P, 'Az Európai Unió, mint büntető joghatóság? [The European Union as a criminal jurisdiction?]' Európai Jog [2005]

6. Gál I. L, 'A pénzmosás szabályozásának régi és új irányai a nemzetközi jogban és az EU-jogban [The old and new tendencies in the regulation of money laundering in the international and EU Law]' Európai Jog. [2007]

[68] cf Nikač (n 53). 96.

[69] Réka Eszter, Gyaraki, *'A számítógépes bűnözés nyomozásának problémái. [The problems around the IT crimes investigation]'* (PTE-ÁJK 2019) 80.

7. Gál I. L, 'Jogszabálytan. [Legal dogmatics]' in Balogh Ágnes – Tóth Mihály, *Magyar Büntetőjog Általános Rész*. (Osiris 2015) 75-76.

8. Gál I. L, 'The Techniques of Money Laundering.' in István László, Gál – László, Kőhalmi (eds.), *Emlékkönyv Losonczy István professzor halálának 25. évfordulójára*. (Pécsi Tudományegyetem, Állam- és Jogtudományi Kar 2005) 129-138.

9. Gál I. L, 'Új biztonságpolitikai kihívás a XXI. században: a terrorizmus finanszírozása. [New challenges of security policy in the 21st century: the financing of terrorism]' Szakmai Szemle [2012] 5-15.

10. Gál István László, *A terrorizmus finanszírozása: Die Terrorismusfinanzierung, [The financing of terrorism]* (PTE Állam- és Jogtudományi Kar Gazdasági Büntetőjogi Kutatóintézet 2010)

11. Gyaraki R.E, *A számítógépes bűnözés nyomozásának problémái. [The problems around the IT crimes investigation]* (PTE-ÁJK 2019) 80.

12. Ibolya T, *A számítástechnikai jellegű bűncselekmények nyomozása [The investigation of IT crimes]* (Patrocinium Kiadó 2012)

13. Karoliny E, 'Igazságügyi együttműködés büntetőügyekben; a kölcsönös elismerés elve. A ne bis in idem elve az Európai Unió Bíróságának ítélkezési gyakorlatában. [Cooperation in criminal matters, the mutual recognition and the principle of ne bis in idem in The practice of the European Court of Justice]' in Mohay Ágoston – Szalayné Sándor Erzsébet (eds.): *Az Európai Unió Joga*. (Dialóg Campus Kiadó 2015)

14. Karsai K, 'A magyar büntető joghatóság [The Hungarian criminal law jurisdiction]' in Krisztina, Karsai (eds.) *Nagykommentár a Büntető Törvénykönyvhöz: Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez*, (Wolters Kluwer 2019)

15. Kőhalmi L, 'A nemzetközi bűnügyi együttműködés [The international cooperation in criminal matters]' in Ágnes, Balogh – Mihály, Tóth (eds), *Magyar büntetőjog Általános rész* (Osiris 2010)

16. Kőhalmi, L 'Az európai bűnügyi együttműködés. [The European cooperation in criminal matters]' In: Ágnes Balogh – Mihály Tóth (eds.) *Magyar büntetőjog Általános rész.* (Osiris 2010)

17. Ligeti K, *Büntetőjog és bűnügyi együttműködés az Európai Unióban [Criminal law and Cooperation in criminal matters in the European Union]* (Közgazdasági és Jogi Könyvkiadó 2004) 43.

18. M. Nyitrai P, *Nemzetközi és Európai Büntetőjog [International and European Criminal Law]* (Osiris 2006)

19. Maillart J, 'The limits of subjective territorial jurisdiction in the context of cybercrime' ERA Forum [2019]

20. Padfield N, 'Shining the Torch on Plea-Bargaining.' The Cambridge Law Journal [2009]

21. Perritt H, 'Jurisdiction in Cyberspace' Villanova Law Review [1996]

22. Polt P, 'A magyar büntető joghatóság. [The Hungarian criminal jurisdiction.]' in Polt et. al. (eds.) *A Büntető Törvénykönyvről szóló 2012. évi C. törvény nagykommentárja.* (Opten 2016)

23. Sántha F, 'A Nemzetközi Büntetőbíróság joghatóságába tartozó nemzetközi bűncselekmények vázlata [Outline of international crimes within the jurisdiction of the International Criminal Court Outline of international crimes within the jurisdiction of the International Criminal Court]' In Bragyova, András (eds.) *Tanulmányok a bűnügyi tudományok köréből.* (Gazdász Elasztik 2013)

24. Satzger H, *International and European Criminal law* (C.H. Beck, 2012)

25. Seker Ö. K, *International Regulation of National Cybercrime Jurisdiction*. (Tilburg University 2012)

26. Tóth M – Kőhalmi L, 'A szervezett bűnözés [The organized crime]' in Borbíró et. al. (eds.) *Kriminológia*. (Wolters Kluwer 2016)

27. Watson G.R, 'The Passive Personality Principle.' in Texas International Law journal [1993]

28. Wiener A. I,, 'A Nemzetközi Büntetőbíróság joghatóságáról' [About the jurisdiction of the International Criminal Court] Magyar Jog [2001]