DR. FERENC SÁNTHA, EGYETEMI DOCENS
University of Miskolc | DOI: 10.32041/9788367149761/5

Chapter 5. Problems of Jurisdiction in Cybercrimes Cases

5.1. Introduction

Until the mid-20th century, crime was largely a local matter. The principles governing the exercise of criminal jurisdiction were based on the axiom that a crime was a phenomenon tied to a specific geographic area.[1] Consequently, the dominant principle among the grounds of jurisdiction was the application of the territorial principle, since it was obvious that jurisdiction should be exercised by the State in whose territory the offence was committed. However, even before the appearance of cybercrimes, there was an increasing number of criminal offences which, due to the place of commission, the nationality of the perpetrator or the nature of the act, violated or threatened the legal order of two or more states at the same time.[2] Cybercrime has multiplied this trend and has fundamentally changed the nature of crime, making it transnational and borderless.[3] The development of cyberspace and info-communication is an important dimension of the dynamic changes of the 21st century.[4] In this context, cyberspace almost epitomises the phenomenon

[1] D. Tóth, Zs. Gáspár, *Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés terén*, "Belügyi Szemle" 2020, No. 2, p. 140.

[2] P.M. Nyitrai, *Nemzetközi és európai büntetőjog*, Budapest 2006, p. 207.

[3] D. Tóth, Zs. Gáspár, *Nemzetközi…*, *op. cit*., p. 140.

[4] Á.Farkas, *A kibertér műveleti képességek kialakításának és fejlesztésének egyes szabályozási és államszervezési alapjai*, "Jog-Állam-Politika" 2019, No. 2, p. 63.

of deterritorialisation, as it allows for the rapid transfer of digital data between users and devices around the world.[5] Deterritorialisation, as the globalisation of social processes and the move away from individual and isolated locations, is a major challenge for the current jurisdictional system, which is still based on the primacy of the territorial principle.[6] The communication space of the web operates on the principle of non-locality. The communication universe is a linguistic, social and political space to which the jurisdiction and sovereignty of individual states cannot easily be extended. States, however, do not want to accept the restriction or even the erosion of their territorial jurisdiction and sovereignty in cyberspace, and therefore try to prevent it in various ways.[7] Since the countries exercising criminal jurisdiction coexist, the permeability of borders, which is also a feature of criminality, raises jurisdictional problems.[8]

In this paper, I define the concept of jurisdiction and then analyse the principles underlying criminal jurisdiction in the first and in the second chapter. In doing so, I draw on the legal literature, the rules of the Budapest Convention,[9] and the provisions of the Hungarian Criminal Code (HCC) and Polish Criminal Code (PCC) on jurisdiction. The latter aspect is also important because one of the questions to be answered is: In which cases do the HCC and the PCC apply to the commission of a cybercrime? The third chapter is devoted to jurisdictional conflicts, and finally I outline three hypothetical practical cases in which jurisdictional problems and institutions of international cooperation in criminal matters

[5] C. Ryngaert, *Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts*, "German Law Journal" 2023, Vol. 24, Issue 4, p. 537.

[6] D.B. Jakab, *Területiség és deterritorializáció. A terület mint a társadalomelmélet vezérfonala*, "Replika" 2009, No. 5, p. 164.

[7] L. Fekete, *Szabadság, jog és szabályozás a kibertérben*, "Replika" 2001, No. 9, p. 219. Clough also notes that "early scholarship postulated cyberspace as a distinct place, beyond traditional rules based on geographical location." However, states do not share this view, and consistently apply the principle of territoriality to cybercrime and refuse to treat the Internet as an area outside their jurisdiction. J. Clough, *Principles of cybercrime*, Cambridge 2010, p. 405.

[8] L.A. Wiener, *A büntető joghatóság és gyakorlása, kivált az Európai Unióban*, "Állam és Jogtudomány" 2002, No. 3–4, p. 177.

[9] The Council of Europe's Convention on Cybercrime, Budapest, 23 November 2001.

can be analysed. The aim of my research is to confirm or refute a hypothesis I have put forward, which is the following: Traditional jurisdictional principles in domestic and international criminal law are not able to respond to the challenges posed by cybercrime, in particular positive jurisdictional conflicts.

5.2. The Concept of Jurisdiction

Jurisdiction, in the most general sense, is the set of rules that make the law a functioning, accessible body of law, and the most important prerequisite for its application.[10] One aspect of the concept, criminal jurisdiction, refers to the right of the state to legislate and enforce criminal law. In a narrower sense, it has a twofold meaning: firstly, the applicability of the rules of national criminal law and, secondly, the scope of the authorities' competence in criminal matters.[11]

The three-level understanding of the concept of jurisdiction is an indispensable issue in the international and especially in the Anglo-Saxon literature, and this paper also refers to it. According to this concept, jurisdiction is the basis for the future exercise of the state's criminal claim (*jurisdiction to prescribe* or *legislative jurisdiction*), which means the state's power to regulate human behaviour: to require the exercise of certain conduct or, as is typical in criminal law, to prohibit certain acts. Another meaning of jurisdiction is the *jurisdiction to enforce*, which is the actual exercise of existing jurisdiction: the ability of a State to validly enforce its law through the exercise of executive and judicial power. Finally, the third level of interpretation of jurisdiction is the *jurisdiction to adjudicate*, which means the power of a state to try a criminal case and to determine whether the accused person has committed a crime.[12]

---

[10] Jurisdiction is essentially a term of international law that refers to the right of a state to make and enforce its law and to exercise justice. P.M. Nyitrai, *Nemzetközi és…*, *op. cit*., p. 208.

[11] P.M. Nyitrai, *Nemzetközi és…*, *op. cit*., p. 209.

[12] See in detail: S.W. Brenner, B.-J. Koops, *Approaches to Cybercrime Jurisdiction*, "Journal of High Technology Law" 2004, Vol. 4, No. 1, pp. 5–6; D. Tóth, Zs. Gáspár, *Nemzetközi…*, *op. cit*., p. 141.

Although several international legal instruments, including the Budapest Convention, contain provisions on jurisdiction, it is not a purely international legal category: the rules of jurisdiction and their content are given substance by domestic criminal law provisions. As a concept of domestic criminal law, *scope* defines the different aspects of the application of the criminal law of a given State (temporal, territorial and or personal scope). Therefore, in this paper, the concept of jurisdiction is used in the following sense: *jurisdiction means the power of the state to make and apply the rules of criminal law. The provisions on jurisdiction regulate when, where and to whom the criminal law (the Criminal Code) is to be applied when adjudicating a criminal offence.* Provisions on criminal jurisdiction can be found in the General Part of the Criminal Code in most countries – including Hungarian and Polish criminal law. The principles underlying criminal jurisdiction have been developed by jurisprudence, but these principles are always reflected in the provisions of the Criminal Code on jurisdiction.

5.3. The Principles of Jurisdiction

States traditionally base criminal jurisdiction on five aspects: territoriality, the active and passive aspects of citizenship (active and passive personality principle), state self-defence and the principle of universality.[13]

1. *The territoriality principle* is the most common basis for the exercise of criminal jurisdiction, according to which the criminal law of a State applies to all offences committed on its territory, irrespective of the nationality of the perpetrator. The Budapest Convention regulates the territoriality principle in the first place[14] and, unlike the other grounds

[13] P.M. Nyitrai, *Nemzetközi és…*, *op. cit.*, p. 213.

[14] See Art. 22(1) of the BC: "Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established under Articles 2 through 11 of this Convention, when the offence is committed: a) in its territory (…)".

of jurisdiction, its adoption and application in domestic law is binding on the States Parties.[15] The territoriality principle is also included in the Hungarian Criminal Code (HCC)[16] and in the Polish Criminal Code (PCC).[17] According to this rules, HCC applies in the case of cybercrime committed on the territory of Hungary and the PCC if the crime is committed on Polish territory. Here I mention the *quasi-territorial principle*, which extends the concept of domestic territory to offences committed on board a ship or registered aircraft flying the flag of a given country. The quasi-territoriality principle is included in the Budapest Convention[18] as well as in the HCC[19] and PCC.[20]

2. The second most frequent basis of jurisdiction is the *personality principle* (nationality principle or *active personality principle*), according to which the jurisdiction of the state extends to the offence committed by its citizen abroad. The active personality principle is also regulated both by the Budapest Convention and by the HCC and the PCC.

---

[15] See Art. 22(2) of the BC: "Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down paragraphs 1 b) through 1 d) of this article or any part thereof."

[16] See Art. 3(1) of the HCC: "Hungarian criminal law shall apply: a) to criminal offenses committed in Hungary (…)".

[17] See Art. 5 of the PCC: "Polish criminal law shall be applied to the perpetrator who committed a prohibited act within the territory of the Republic of Poland (…)".

[18] See Art. 22(1)(b)(c) of the BC: "Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established under Articles 2 through 11 of this Convention, when the offence is committed: (…) (b) on board a ship flying the flag of that Party; or (c) on board an aircraft registered under the laws of that Party".

[19] See Art. 3(1) of the HCC: "(1) Hungarian criminal law shall apply: (…) (b) to criminal offenses committed on commercial ships or watercraft sailing, or aircraft flying under Hungarian flag outside the territory of Hungary."

[20] See Art. 5 of the PCC: "Polish criminal law shall be applied to the perpetrator who committed a prohibited act (…) on a Polish vessel or aircraft, unless an international agreement to which the Republic of Poland is a party stipulates otherwise."

It is important to note that, according to the Convention[21] and the PCC,[22] a further condition for the application of the principle is that the act is also considered a criminal offence and punishable under the law of the place where it is committed. This is called the *double incrimination requirement* or the principle of *double criminality*. In contrast, the active personality principle plays a much broader role in Hungarian criminal law: the additional condition is not that the act should be a criminal offence under the law of the place of the commission, but only that it should be a criminal offence under the Hungarian Criminal Code.[23] Here I mention that whereas the Convention does not, the Hungarian[24] and Polish Criminal Codes[25] do also regulate the *passive personality principle*, which is also one of the grounds for extraterritorial jurisdiction. The principle protects the state's own citizen (or its own legal person or other organisation) in the event of an offence committed abroad by a foreigner.[26]

[21] See Art. 22(1)(d) of the BC: "Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established under Articles 2 through 11 of this Convention, when the offence is committed: (…) (d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State."

[22] See Art. 109 of the PCC: "Polish criminal law shall be applied to Polish citizens who have committed an offence abroad". See also the Art. 111 § (1): "The liability for an act committed abroad is, however, subject to the condition that the liability for such an act is likewise recognised as an offence, by a law in force in the place of its commission."

[23] See Art. 3(1) of the HCC: "Hungarian criminal law shall apply: (…) (c) to any act of Hungarian citizens committed abroad, which is punishable by Hungarian law."

[24] See Art. 3(2)(d) of the HCC: "Hungarian criminal law shall apply: (…) (b) to any act committed by non-Hungarian citizens abroad against a Hungarian national or against a legal person or unincorporated business association established under Hungarian law, which is punishable under Hungarian law."

[25] See Art. 110(1) of the PCC: "Polish criminal law shall be applied to foreigners who have committed abroad an offence against the interests of the Republic of Poland, a Polish citizen, a Polish legal person or a Polish organisational unit not having the status of a legal person".

[26] T. Horváth, M. Lévay, *Magyar büntetőjog általános rész*, Budapest 2014, p. 102.

The following jurisdictional principles already apply in cases where the offence is committed *abroad* by a person who is *not a national* of the State (foreign national or stateless person). It should be noted that the Convention does not contain such principles but allows States Parties to regulate and apply them.[27]

3. Under the *principle of state self-defence* or the *protective principle,* a State has jurisdiction to criminalise extra-territorial conduct, regardless of the nationality of the offender, where that conduct is against the fundamental interest of the state, for example crimes against the security, territorial integrity or political independence of the state. The protective principle is included in both the PCC[28] and the HCC.[29] It should be noted that in Polish criminal law, the double incrimination requirement is not necessary in this case and the scope of the relevant offences is quite broad. Double incrimination is not a precondition in Hungarian criminal law either, but the relevant criminal offences are narrower, namely the offences against the state regulated by the Criminal Code. Based on this provision, a cyber-attack launched against Hungary from abroad with the aim of obtaining data that can be used to the detriment of the country ("conducting intelligence activities" against Hungary) may

[27] According to the Art. 22(4) of the BC: "This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law."

[28] See Art. 112 of the PCC: "Regardless of the provisions in force in the place of the commission of the offence, Polish criminal law shall be applied to a Polish national, or to a foreigner in case of the commission of:
1) an offence against the internal or external security of the Republic of Poland,
2) an offence against Polish offices or public officials,
3) an offence against essential economic interests of Poland,
4) an offence of false deposition made before a Polish office,
5) from which a material benefit was gained, even if indirectly, in the Republic of Poland".

[29] See Art. 3(2)(b) of the HCC: "Hungarian criminal law shall apply (a) to any act committed by non-Hungarian citizens abroad, if it is recognized as an offense against the State (…) regardless of whether or not it is punishable in accordance with the law of the country where committed."

constitute the crime of espionage (Art. 261 of the HCC), in which case the Hungarian Criminal Code applies.

4. The *principle of universality* requires a State to prosecute certain crimes, regardless of the place it was committed or the nationality of the perpetrator. These are typically the so-called crimes under international law (genocide, crimes against humanity, war crimes and crime of aggression) and the so-called transnational crimes, namely crimes punishable under an international treaty. Both the HCC[30] and the PCC[31] regulate the principle of universality, and it is important that double incrimination is not a condition here, either.
5. Until now, Polish and Hungarian rules on criminal jurisdiction have been very similar, but there is a difference about *offences committed abroad by foreigners*. In addition to the cases mentioned above, the Polish legislator provides for the application of the PCC for offences punishable by imprisonment for more than 2 years if the perpetrator is in Poland, and for terrorist offences.[32] The HCC also contains an additional provision on the offence committed by a non-Hungarian citizen abroad. Under *the representational principle* (the vicarious administration of justice), it is possible to prosecute and hold liable a non-Hungarian perpetrator

[30] See Art. 3(2)(b) of the HCC: "Hungarian criminal law shall apply (a) to any act committed by non-Hungarian citizens abroad, if it constitutes a criminal act under Chapter XIII or XIV (crimes against humanity and war crimes), or any other criminal offenses which are to be prosecuted under an international treaty ratified by an act of Parliament."

[31] See Art. 113 of the PCC: "Regardless of regulations in force in the place of commission of the offence, Polish criminal law shall be applied to a Polish national, or to a foreigner, concerning to whom no decision on extradition has been taken, in the case of the commission abroad of an offence which the Republic of Poland is obligated to prosecute under international agreements, or in case of offences prescribed in the Rome Statute of the ICC."

[32] See Art. 110(2)(3) of the PCC: "1. Polish criminal law shall be applied to foreigners in the case of the commission abroad of an offence other than listed in § 1, if, 2. under Polish criminal law, such an offence is subject to a penalty exceeding 2 years of deprivation of liberty, and the perpetrator remains within the territory of the Republic of Poland and where no decision on his extradition has been taken. 3. an act must be considered terrorism".

> not only for the aforementioned serious international crimes but also for other offences committed abroad, if the double incrimination requirement is met.[33]

Based on the principles and rules of jurisdiction in Polish and Hungarian criminal law, it can be concluded that, in addition to the primary application of the territorial principle, the relevant regulations extend the traditional territorial jurisdiction and provide for almost unlimited extraterritorial jurisdiction. Consequently, *when a cybercrime is committed, Hungarian and Polish criminal law apply in almost every possible situation, regardless of the place of the commission and the nationality of the perpetrator*. The only limitation[34] appears to be the double incrimination requirement, but since cybercrimes are punishable under international treaties, the principle of universality applies in theory, and there is no obstacle to applying Hungarian and Polish criminal law to cybercrimes committed by non-citizens abroad. However, such a *broad and almost catch-all regulation of jurisdictional provisions inevitably generates conflicts of jurisdiction*.

5.4. Conflicts of Jurisdictions

There are two types of jurisdictional conflicts, negative and positive. In the first case, either no state has potential jurisdiction over the case (this is almost impossible in practice), or no state intends to exercise its actual jurisdiction. The latter situation is very rare, but it can happen. An example from the literature maintains that when there occurs cybercrime concerning viruses, or Web sites showing hate speech, single countries may feel they are insufficiently harmed for

[33] See Art. 3(2)(aa) of the HCC: "Hungarian criminal law shall apply to any act committed by non-Hungarian citizens abroad, if it is punishable as a criminal offence under Hungarian law and in accordance with the laws of the country where committed."

[34] However, it should be stressed that in the case of offences committed abroad by non-Hungarians, the provision requiring the decision of the Prosecutor General to initiate criminal proceedings constitutes a (self-)limitation on the exercise of Hungarian criminal jurisdiction.

them to claim jurisdiction, perhaps also because they may think that some other country will surely claim jurisdiction.[35]

Much more common is the positive conflict of jurisdiction, where two or more states claim and intend to exercise jurisdiction in the same criminal case. For instance, if a Hungarian national uses a computer in Poland to hack into a computer in Austria, at the very least, Hungary, Poland, and Austria will be able to claim jurisdiction.[36]

Since cybercrime in many cases falls within the scope of transnational criminality, it can often be difficult to determine in which country the crime has been committed; the perpetrator and the victim may be in different countries, and the information asset or data involved in the crime may be located in a third country. Consequently, *in cybercrime cases, it is a very realistic and almost necessarily occurring situation that numerous countries have jurisdiction to prosecute*. In this situation, problems may arise in making decisions about which state should prosecute.[37]

Resolving conflicts of jurisdiction is a fundamental interest to avoid duplication of proceedings and to ensure efficient, timely and cost-effective prosecution.[38] Two basic methods for resolving positive conflicts of jurisdiction are the hierarchy of jurisdictional principles and the consultation between the States concerned.

The hierarchy of jurisdictional principles is exemplified by the Council of Europe Recommendation 420 (1965) on the Settlements of conflicts of jurisdiction in criminal matters, according to which the State in whose territory the offence was committed shall have the primary right to exercise jurisdiction. The primacy

[35] S.W. Brenner, B.-J. Koops, *Approaches…*, *op. cit*., p. 41.

[36] Similar examples are mentioned by Mezei and Brenner, Koops. See K. Mezei, *A kiberbűnözés egyes büntetőjogi szabályozási kérdései*, Pécs 2019, p. 195 and S.W. Brenner, B.-J. Koops, *Approaches…*, *op. cit*., p. 41.

[37] L. Dornfeld, *Az elektronikus bizonyítékszerzés aktuális kérdései*, "Kriminológiai Közlemények" 2017, No. 77, p. 243.

[38] Further risks of jurisdictional conflicts are the duplication of effort, unnecessary inconvenience for witnesses, or competition among law enforcement officials of the states concerned. See point 239 of the Explanatory Report to the Convention on Cybercrime, https://rm.coe.int/16800cce5b (accessed on: 15.07.2023).

of the territorial principle can only be overridden by the protection principle, because if the act threatens the security or credit of the state, the threatened state has the primary criminal claim. The territorial principle is followed by the active personality principle, and finally the jurisdiction of the state in whose territory the perpetrator is found.[39] Furthermore, Article 10 of Council Framework Decision 2005/222/JHA[40] on attacks against information systems established the grounds of jurisdiction for the offences it covers. Proceedings may therefore be initiated if the offence has been committed in whole or in part within its territory, or by one of its nationals or the benefit of a legal person that has its head office in the territory of that member state. Based on paragraph 4, this ranking also constitutes a hierarchy in deciding which State should prosecute if two or more states have and intend to exercise jurisdiction in the same criminal case. However, Directive 2013/40/EU on attacks against information systems and replacing the Framework Decision no longer establishes a hierarchy between these jurisdictional grounds.[41] Ideas on the jurisdictional hierarchy have also been formulated in the relevant literature. Bassiouni, the famous international criminal lawyer, argued that the primacy of the territorial principle must prevail, followed by the active and passive personality principles, and only then can jurisdiction be exercised based on other principles, provided that the accused is in the territory of the state claiming jurisdiction.[42]

At first sight, the primacy of the territorial principle seems acceptable. For example, in principle, territoriality better guarantees due process and compliance with the principle of legality, which

[39] Recommendation 420 on the settlement of conflicts of jurisdiction in criminal matters adopted by the Consultative Assembly of the Council of Europe on 29 January 1965.

[40] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[41] L. Dornfeld, *Az elektronikus…*, *op. cit.*, p. 244.

[42] M.C. Bassiouni, *International Criminal Law. A Draft International Criminal Code and a Draft Statute for an International Criminal Tribunal*, Hingham 1987, p. 191.

requires individuals to be aware that a certain act is punishable.[43] Moreover, the majority of the evidence necessary for the investigation of a crime is usually located at the place where it was committed and there is reason to be optimistic about a quick and efficient completion of the criminal proceedings. However, it must be emphasised that currently there is *no international treaty that establishes a hierarchy of jurisdictional principles* and provides a general primacy of the territorial principle. Nor does customary international law allow such a conclusion to be drawn. On the other hand, in the case of cybercrime, *the place of commission is often uncertain*. Different countries have different rules on what should be considered the place of the commission in case of content-related cybercrimes, such as child pornography.[44] This can be the place where the data or content is uploaded or downloaded, or – as in Hungary[45] – the place where the server hosting the website is located. The identification of the perpetrator's location is further hampered by software and methods whose specific purpose is to hide the perpetrator's location (and identity) so that they cannot be identified geographically.[46]

Another way of solving the positive jurisdictional conflicts is *consultation* between states having and claiming jurisdiction. According to the Article 22(5) of the Budapest Convention, "When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution."

It can be seen that, under the Convention, consultation is only an "appropriate" option and not a real obligation,[47] and the laconic

[43] J.-B. Maillard, *The limits of subjective territorial jurisdiction in the context of cybercrime*, "ERA Forum" 2018, Vol. 19, Issue 3, p. 3.

[44] S.W. Brenner, B.-J. Koops, *Approaches…*, *op. cit*., pp. 15–16.

[45] See the Decision BH2022.65 of the Hungarian Supreme Court.

[46] These methods include IP address modification and hiding (spoofing) and the use of proxy servers, VPN (Virtual Private Networks) or botnet infrastructure (zombie machines). See in details: J.-B. Maillard, *The limits…*, *op. cit*., pp. 4–6, and K. Mezei, *A kiberbűnözés…*, *op. cit*., pp. 195–196.

[47] According to the Explanatory Report of the Convention, "(…) the obligation to consult is not absolute, but is to take place „where appropriate". "Thus, for example, if one of the Parties knows that consultation is not necessary (e.g., it

provision does not provide guidance on the ranking of jurisdictional claims. Moreover, the Convention does not regulate the criteria[48] which, considered together, can be used to decide which country is clearly most closely linked to the crime committed. Finally, the Convention does not provide an answer to the question of what to do if the consultation fails.[49]

5.5. Conflicts of Jurisdiction and the Institutions of International Cooperation in Criminal Matters[50]

In the following, I outline three hypothetical cases with a common characteristic: a *cybercrime* – a cyberattack – *is committed against a Hungarian victim* (a Hungarian citizen natural person or a Hungarian resident legal person, or other organisation). The three models were set up based on the place of the commission, giving importance to the perpetrator's nationality and the perpetrator's detected location after initiating the criminal proceedings. In

has received confirmation that the other Party is not planning to take action), or if a Party is of the view that consultation may impair its investigation or proceeding, it may delay or decline consultation." See point 239 of the Explanatory Report to the Convention on Cybercrime, https://rm.coe.int/16800cce5b (accessed on: 15.07.2023).

[48] The factors need to be examined and taken into account in the consultation to resolve the jurisdictional conflict may include the place of the commission of the crime; the nationality of the perpetrator; the location of the perpetrator and the victim(s); the place where the majority of the crime was committed or where most of the victims are located; the place where the damage is significant; the possibilities of transfer or extradition to other countries; the interests of the perpetrator, in particular his or her resocialisation, etc. See: Z.A. Nagy, *A joghatóság problémája a kiberbűncselekmények nyomozásában*, [in:] K. Karsai, Zs. Fantoly, Zs. Juhász, Zs. Szomora, A. Gál (eds.), *Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára*, Szeged 2018, p. 761.

[49] If the consultation is unsuccessful, recourse to an intergovernmental organisation or (arbitration) tribunal can be an option, but this would certainly lead to a prolongation of the procedure and call into question the timeliness of the subsequent criminal proceedings.

[50] This chapter is made by using the following source R. Bartkó, F. Sántha, *A kibertér műveletek büntetőjogi értelmezésének lehetőségei, különös tekintettel a nemzetközi bűnügyi együttműködésre*, (manuscript, under publication).

the first case, the detected location of the cyberattack is Hungary, in the second case the starting point of the attack is a member state of the European Union (EU), and in the third, the place of the commission is on the territory of a third state outside the EU.

5.5.1. THE DETECTED LOCATION OF THE CYBER-ATTACK IS HUNGARY

When the perpetrator – whether a Hungarian citizen or a foreigner – commits cybercrime on the territory of Hungary, there is no jurisdictional problem, as the Hungarian state, and therefore the competent Hungarian criminal authorities have clear jurisdiction based on the territorial principle. In this case, the perpetrator located in Hungary can, as a main rule, be prosecuted without any particular difficulty.

From the perspective of jurisdiction, the situation becomes more complex and the instruments of international cooperation in criminal matters will play a role when the detected offender has left Hungary and is staying in a member state of the EU at the time of the initiation of the criminal proceedings. In this situation, if the national arrest warrant is unsuccessful, the Hungarian criminal court will issue a *European arrest warrant*, which, if successful, will allow the perpetrator to be *surrendered* in accordance with the procedural rules laid down in the Act CLXXX of 2012 on the cooperation with the member states of the European union in criminal matters.[51]

Two scenarios are possible from this point. If the perpetrator is a Hungarian national who is residing in a member state of the EU,

[51] This Act is the implementing law of the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States. The European arrest warrant is a simplified cross-border judicial surrender procedure for the purpose of prosecuting or executing a prison sentence or detention order. A warrant issued by one EU country's judicial authority is valid in the entire territory of the EU. It has replaced the cumbersome in many cases lengthy extradition procedures that used to exist between EU countries. Here it should be noted that all cybercrimes in Hungary meet the condition that a European arrest warrant can only be issued if the crime is punishable by a minimum of 1 year imprisonment.

Hungary will have exclusive jurisdiction based on the territoriality principle and the suspect will most likely be surrendered to Hungary under the arrest warrant. By contrast, if the perpetrator is not a Hungarian, the EU member state of which he or she is a national may also establish jurisdiction based on the active personality principle which is included in the Budapest Convention, as analysed earlier.[52] However, in my view, if the cyberattack takes place in Hungary against a Hungarian victim, the aspects of the evidentiary procedure, and, consequently, the success of the procedure will shift the balance towards the territorial principle. In this case, the surrender based on the European arrest warrant ensures the presence of the Hungarian perpetrator in the domestic criminal proceedings.

The situation is even more complicated if the location of the suspect, based on the international arrest warrant issued by the Hungarian Court, is detected in a third country, namely outside the European Union. In this case, surrender based on the European arrest warrant cannot be invoked, but the provisions on *extradition* under Article 24 of the Budapest Convention and the Hungarian Act XXXVIII of 1996 on international mutual legal assistance in criminal matters will apply. According to Article 31 of the Hungarian Act, Hungary is entitled to submit a request for extradition for the purpose of prosecuting to the third state where the perpetrator is staying. The previously mentioned conflict of jurisdiction may of course arise in this case as well, but the spirit of the Budapest Convention justifies the preference for conducting criminal proceedings under Hungarian rules in this case as well, therefore extradition may be a viable legal institution.[53]

[52] If this state and Hungary reach an agreement in the consultation, this state may prosecute the perpetrator.

[53] If the perpetrator is located in a non-EU member state that has not ratified the Budapest Convention, the provisions of the European Convention on Extradition (1957) will apply. (All countries that are members of the Council of Europe are parties to the European Convention on Extradition.) In the case of a non-European country, the rules of the international treaty concluded with the state concerned, or, in the absence of a treaty, the rules of reciprocity, and the Hungarian Act XXXVIII of 1996 will apply.

5.5.2. THE DETECTED LOCATION OF THE CYBER-ATTACK IS A MEMBER STATE OF THE EUROPEAN UNION

The second case of my model analysis is when the cyberattack affects a Hungarian victim, but the location and starting point of the attack is not Hungary, but another member state of the EU.

In this situation, *one possible scenario* is if the perpetrator is a Hungarian national who is staying in another EU country.[54] As a result, there are essentially two competing grounds of jurisdiction. The first is the Hungarian nationality of the perpetrator, which is the factor underlying the active personality principle. The other is the territoriality principle, since the offence was committed from the territory of another member state. The fact in which state the criminal proceedings were initiated will be relevant to the solving of this jurisdictional problem.

a) *If the proceedings have been initiated only in Hungary*, the presence of the perpetrator in the domestic criminal proceedings can be provided along the previously mentioned forms of cooperation in criminal matters.
b) *If the offender perpetrator has been prosecuted only in the member state where the offence was committed*, that state, since the perpetrator is a Hungarian national, shall provide information to Hungary on the proceedings within the framework of the exchange of information,[55] resulting in two further possible cases: (i) member state where the offence was committed conducts its own criminal proceedings, and then, after taking into account the foreign judgment, the final decision can be enforced in Hungary; or (ii) the Hungarian authorities initiate the surrender of the Hungarian national for the purpose of prosecuting based on an European arrest warrant issued after the initiation of the criminal proceedings.

[54] If the Hungarian national perpetrator is staying in a non member state of the EU after the criminal proceedings have been initiated, the provisions on extradition previously mentioned may be applied.

[55] On the provisions on the exchange of information between Member States, see Articles 104–105 of the Act CLXXX of 2012.

c) In the third case, *criminal proceedings have been initiated both in Hungary and in the member state where the offence was committed*. In the case of *parallel proceedings*, namely where two member states are simultaneously conducting criminal proceedings against the same offender for the same cybercrime, the Act provides for a *consultation procedure,*[56] the outcome of which will determine which Member State will actually prosecute the offender.

The other possible scenario in my second model is when the cybercrime causing harm in Hungary is committed by a person of non-Hungarian nationality in another EU member state. In this case, apart from the passive personality principle, there is no other ground for conducting criminal proceedings in Hungary, and the jurisdiction of Hungary cannot be justified based on the interest of evidence and the nationality of the perpetrator. I think that, in such a scenario, the Hungarian authorities may provide procedural legal assistance for criminal proceedings conducted by a foreign state, but there is no reasonable justification either for conducting the proceedings domestically or for enforcing any criminal sanction in Hungary.

5.5.3. THE DETECTED LOCATION OF THE CYBER-ATTACK IS A THIRD COUNTRY OUTSIDE THE EUROPEAN UNION

In my third hypothetical situation, the cybercrime directed against the Hungarian victim is committed in the territory of a state that is not a member state of the EU. If the perpetrator is a Hungarian citizen and staying in Hungary, Hungary has jurisdiction on

[56] See Articles 106–107 of the Act CLXXX of 2012. According to the Act, the parties shall take into account all relevant factors to decide which member state will prosecute the case. Such relevant factors include the place of the commission of the crime, the nationality of accused and the victim(s), the place of detention of the accused, the state of the criminal proceedings in the member states, the fact in which member state more evidence is available, and whether the criminal proceedings in the member states are related to other criminal proceedings in that member state. If the consultation is unsuccessful, the Prosecutor General may refer the matter to Eurojust to decide.

the basis of the active personality principle and there is no particular problem in prosecuting the perpetrator. However, if the Hungarian perpetrator is located in a non-EU country, extradition under Article 24 of the Budapest Convention or, if the Convention cannot be invoked, extradition rules based on the European Convention on Extradition (1957)[57] may apply.[58] And if the Hungarian offender is staying in a country that is not party to the previously mentioned conventions, the rules of the international treaty concluded with the state concerned, or, in the absence of a treaty, the rules of reciprocity, and the Hungarian Act XXXVIII of 1996 will apply. Finally, the last possible scenario for my third situation is when the offender is not a Hungarian citizen. In this case, the jurisdiction of Hungary could only be established on the basis of the passive personality principle, which presupposes the principle of double criminality. However, based on the place where the offence was committed and the nationality of the perpetrator, the states concerned are much more likely to claim jurisdiction under the Budapest Convention. In this scenario – as we have also discussed in the second model – Hungarian authorities may only provide procedural legal assistance for criminal proceedings conducted by the foreign state.

5.6. Conclusion

The hypothesis I put forward at the beginning of this study has been proven to be true: traditional jurisdictional principles in domestic and international criminal law are not able to respond to the challenges posed by cybercrime, in particular positive jurisdictional

[57] Since the Budapest Convention, based on the purposes set out its preamble, is a lex specialis compared to the European Convention on Extradition, the applicability of the Convention should be examined first, and the European Convention on Extradition is secondary.

[58] It is not excluded, of course, that the state concerned, either on based on the Article 24(6) of the Budapest Convention or Articles 7 and 8 of the European Convention on Extradition, may refuse extradition because it has already initiated criminal proceedings under the territoriality principle. In this case, following the criminal proceedings, the foreign judgment can be enforced in Hungary.

conflicts. Possible solutions to the problems outlined could be the creation of a global international treaty[59] to regulate jurisdictional issues and the procedure to be followed in the event of a conflict of jurisdiction. Consultation between the States concerned is a necessary element, but it is advisable to set a reasonably short deadline for such consultation. And if the consultation fails, a mandatory hierarchy of jurisdictional principles need to be established, otherwise we risk the effective prosecuting the perpetrators of cybercrime. Finally, it should be emphasised that the successful determination of the state that has actual jurisdiction in the case is only the first step in holding the perpetrator accountable, since jurisdiction can only be effectively exercised and proceedings carried out if the perpetrator is available to the authorities of the state that has jurisdiction, for example if he or she is in the custody of that state. Otherwise, the institutions of international or European mutual legal assistance in criminal matters, such as extradition or surrender based on the European arrest warrant, should be used.

REFERENCES

Bartkó, R., Sántha, F., *A kibertér műveletek büntetőjogi értelmezésének lehetőségei, különös tekintettel a nemzetközi bűnügyi együttműködésre*, (manuscript, under publication).

Bassiouni, M.C., *International Criminal Law. A Draft International Criminal Code and a Draft Statute for an International Criminal Tribunal*, Hingham 1987.

Brenner, S.W., Koops B.-J., *Approaches to Cybercrime Jurisdiction*, "Journal of High Technology Law" 2004, Vol. 4, No. 1.

Clough, J., *Principles of cybercrime*, Cambridge 2010.

Dornfeld, L., *Az elektronikus bizonyítékszerzés aktuális kérdései*, "Kriminológiai Közlemények" 2017, No. 77.

[59] Note that a new convention on cybercrime – the Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes – is being drawn up within the framework of the United Nations.

Farkas, Á., *A kibertér műveleti képességek kialakításának és fejlesztésének egyes szabályozási és államszervezési alapjai*, "Jog-Állam-Politika" 2019, No. 2.

Fekete, L., *Szabadság, jog és szabályozás a kibertérben*, "Replika" 2001, No. 9.

Horváth, T., Lévay, M., *Magyar büntetőjog általános rész*, Budapest 2014.

Jakab, D.B., *Területiség és deterritorializáció. A terület mint a társadalomelmélet vezérfonala*, "Replika" 2009, No. 5.

Maillard, J.-B., *The limits of subjective territorial jurisdiction in the context of cybercrime*, "ERA Forum" 2018, Vol. 19, Issue 3.

Mezei, K., *A kiberbűnözés egyes büntetőjogi szabályozási kérdései*, Pécs 2019.

Nagy, Z.A., *A joghatóság problémája a kiberbűncselekmények nyomozásában*, [in:] Karsai, K., Fantoly, Zs., Juhász, Zs., Szomora, Zs., Gál, A. (eds.), *Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára*, Szeged 2018.

Nyitrai, P.M., *Nemzetközi* és *európai büntetőjog*, Budapest 2006.

Ryngaert, C., *Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts*, "German Law Journal" 2023, Vol. 24, Issue 4.

Tóth, D., Gáspár, Zs., *Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés terén*, "Belügyi Szemle" 2020, No. 2.

Wiener, I.A., *A büntető joghatóság és gyakorlása, kivált az Európai Unióban*, "Állam és Jogtudomány" 2002, No. 3–4.