Dragojlović Joko[*]
http://orcid.org/0000-0002-4713-1855

UDK: 343.533::004
Review article
DOI: 10.5937/ptp2300063D
Received: 31.12.2022.
Approved on: 21.02.2023.
Pages: 63–83

JURISDICTION FOR CRIMINAL OFFENSES OF CYBERCRIME – INTERNATIONAL AND NATIONAL STANDARDS

ABSTRACT: Criminal acts of a computer crime are no longer a new social and legal phenomenon. In addition to the execution of criminal acts that fall within the domain of a computer crime, computers have found their application in the execution of the so-called classic criminal acts, giving them a different modus operandi. A spatial distance between the action taken and the resulting consequences during the execution of criminal acts of a computer crime, led to the strengthening of the transnational crime. Initially, the international community tried to intervene in this area, with the idea of regulating the criminal prosecution of the perpetrators of the cross-border criminal acts of a computer crime. However, to date, there has been adopted no normative framework regulating the issue of prosecuting the perpetrators of these criminal acts at the universal level. In this sense, the paper analyzes the existing international standards with regard to the normative arrangement of jurisdiction for the prosecution of perpetrators of transnational computer crimes. In addition, the paper contains a presentation of the normative arrangement of this issue in domestic legislation.

Keywords: *computer crime, transnational crimes, jurisdiction, international standards, The Convention from Budapest.*

[*] LLD, Associate professor, Faculty of Law for Economy and Justice in Novi Sad, University of the Academy of Economics in Novi Sad, Serbia, e-mail: jdragojlovic@pravni-fakultet.info

1. Introductory considerations

The immeasurably great opportunities in all spheres of social life that have appeared to man with the development of information technologies have undoubtedly entailed certain risks and social dangers that are reflected in various types of misuse of computers, computer systems and computer networks, above all the Internet.

As a consequence of the marked expansion of the use of computers and computer technologies, a new social phenomenon appeared – computer crime. It is a special type of criminality that has a very wide phenomenological dimension, bearing in mind that criminal acts are committed through computers, that is, computers are used as a means of execution, or, alternatively, as an object against which a criminal act is committed (Matijašević & Dragojlović, 2021, p. 54). Also, this type of crime has specific perpetrators, crimes are committed very quickly (in a fraction of a second), there is a large dark figure present (often the victims do not realize that they have been deceived and that one of the crimes from the area has been committed against them computer crime). In addition, with computer crime, the area of criminal activity is expanded, that is, the perpetrator can undertake an action in one country, and the consequences can occur in another, which gives this type of crime a transnational character.

Respecting all the specifics of computer crime, and especially its transnational character, the international community has a strong motive to establish a general normative framework for regulating the issue of defining computer crime and determining the rules of jurisdiction for prosecuting these crimes. However, reasons of sovereignty, political independence, interest in conducting criminal proceedings and the like prevent the international community from establishing uniform rules at the universal level, while the rules set at the regional level are not sufficiently up-to-date, not binding or not sufficiently widely set.

2. General remarks on computer crime and the question of jurisdiction in combating computer crime

Regarding the definition of computer crime, in general, it can be stated that computer crime includes both active and passive use of a computer, and even the storage of evidence of a committed criminal act in a computer or in electronic form, while the victims and possible victims are all natural and legal persons. that use or depend on computers and databases (Rome Memorandum, 2008). In this sense, the computer, as a characteristic feature of computer crime, appears in different functions: **1) the object of the execution of the**

criminal act ; **2) the subject of the criminal act** ; **3) means of committing the crime** ; **4) "weapon" or means** (Vidić, 2016, p. 94).

When it comes to the definition of computer crime itself, there is no single and generally accepted definition of computer crime in the literature. The first and most general definition was given in 1979 by the US National Law Institute in The Criminal Justice Resource Manual of computer Crime (Parker, 1989), according to which computer crime is understood as "any illegal act for which successful criminal prosecution requires good knowledge of computer technology." Such a broad definition will serve as a starting point for the international legal definition of the concept of computer crime.

From the point of view of criminal law theory, computer crime, as a general form of manifestation of various forms of criminal activity, is crime directed against the security of information (computer) systems as a whole or in its individual parts, which, in different ways and by different means, is intended to to gain some benefit for oneself or another or to cause some harm to another (Jovašević & Hašimbegović, 2004; Gordon & Ford, 2006, pp. 13-20). In this sense, Petrović and Jovašević correctly note that the key determinant of computer crime is the close connection of the criminal act with technology, from which its dynamism and variety of appearances derive (Petrović & Jovašević, 2006, pp. 211-216). We will see in the later chapter of this paper, the domestic legislator, deciding on the definition of high-tech criminality, was guided by some, but not all, of the presented theoretical legal elements of this form of criminality.

It is a generally accepted definition that the jurisdiction of an authority, in terms of criminal proceedings, implies the right and obligation of that authority to conduct and conclude one proceeding in one criminal case depending on the severity of the criminal offense, expressed in the prescribed sentence and the characteristics of the perpetrator of the criminal offense.

However, jurisdiction includes several distinct concepts, including jurisdiction to prescribe legal rules, jurisdiction to adjudicate disputes, and jurisdiction to enforce laws and decisions (Restatement, 1987, para. 401). In this sense, jurisdiction to prescribe legal rules is the authority of a sovereign entity to make its law applicable to a person's activities, relationships or status, or a person's interests in legal matters. Jurisdiction is the authority of a sovereign entity "to subject persons or subjects to the proceedings of its courts or administrative bodies" to determine whether a prescribed legal rule has been violated (Brenner & Koops, 2004, p. 5). According to the Restatement (1987, para. 401b), the power to enforce laws and decisions is the power of a sovereign entity "to encourage or compel compliance with or to punish the

violation of its laws or other regulations, whether by judicial means or by the use of executive, administrative, police or other extrajudicial measures."

Traditionally, all three manifestations of the concepts of sovereignty and jurisdiction, i.e. the three types of jurisdiction mentioned, are primarily based on the element of territoriality. Thus, from the very beginning, the state had the authority to prescribe the rules of conduct of its subjects within its physical territory, and it had the authority to enforce the prescribed rules of conduct against any individual whose illegal behavior took place on the territory of that state (Vukadinović & Avramović, 2014, pp. 38-42). This concept of jurisdiction derives from the basic principle that a sovereign entity has the legal authority to exercise control and authority over "its territory, generally to the exclusion of other states" and that it has "the power to govern its territory and the power to enforce the laws." (Restatement, 1987, para. 206b). In this sense, the US Supreme Court correctly stated that the nature of the act as a legal or illegal action must be determined entirely by the law of the country where the act itself was committed (American Banana Company v. United Fruit Company). From the foregoing, therefore, it follows that no state and no sovereign entity can apply its criminal laws to behaviors that occur on the physical territory of another nation.[1]

However, the constant development and expansion in the use of information and telecommunication technology significantly undermines certain assumptions that gave birth to the traditional model of jurisdiction, as an expression of sovereignty (Goodman & Brenner, 2002, pp. 4-24). The development of technology has made it much easier to commit a criminal offense in one country, while the victim, i.e. the injured person, is physically located in another country, which all creates new and unique challenges in the area of jurisdiction for prescribing and prosecuting criminal offenses of computer crime, but also raised the question of the need to revise the regulations on extradition. In this sense, the existing concept of requiring double criminality of the act for legal extradition, as well as the position that states have sovereign power over those within their borders, still retain their

[1] True, this principle is deviated from in the criminal legislation in certain cases. Likewise, the provisions on the territorial validity of the Criminal Code of the Republic of Serbia (Articles 7–9 of the Criminal Code) provide for the validity of this criminal regulation for acts committed abroad. However, Article 10 of the CC provides for relatively strict conditions for the application of the previous provisions on territorial validity. Therefore, these narrowly constructed exceptions, as well as the rules on universal jurisdiction for the prosecution of certain criminal acts incriminated at the international level (e.g. genocide, war crimes, etc.), should not be understood as violating the general principle of the limited validity of the criminal legislation of a country only on the territory of that country, without affecting, at the same time, the legal rules on extraterritorial areas.

importance, but in the past few decades there has been a need to review and relativize these attitudes regarding the exercise of criminal jurisdiction.[2]

Jurisdiction, therefore, no longer depends only on the physical presence of a person on the territory of a country. However, even under this expanded view of jurisdiction, a state cannot "exercise jurisdiction to prescribe rules of conduct in relation to a person or activity connected with another state when the exercise of such jurisdiction would be unreasonable (Restatemen 1987, para 403(1)).[3]

So, as can be concluded, the appearance of computers, computer systems and computer networks, as well as their development and the expansion of the use of these novelties, caused changes in the previous approaches to jurisdiction for trial in criminal matters, because the previous concepts, mostly based on the principle of territoriality, they could no longer maintain as absolute.

3. International standards regarding jurisdiction for prosecuting criminal offenses of computer crimes

Bearing in mind the fact of the spread of information technologies and, consequently, computer crime, as well as the importance of suppressing this phenomenon and the consequences it causes, it is not surprising that the

[2] Namely, in order for extradition to be legal and possible, as a rule, it is required that extradition can only be carried out if there is a so-called "dual criminality" which means that one and the same act is criminalized in both countries as a criminal offense. If, on the other hand, this is not the case, but only one country incriminates the act, then the other country, which does not incriminate the act, will not, as a rule, be able to carry out a legal extradition. On the problem of extradition on the example of the computer virus Love bug from 2000, see in detail: (Brenner & Koops, 2004, pp. 7-8).

[3] Whether the exercise of the power to prescribe is unreasonable is determined by taking into account various factors, including the following: (a) the connection of the activity with the territory of the regulating state, that is, the extent to which the activity takes place within the territory, or has a significant, direct and foreseeable effect on or in the territory; (b) links, such as nationality, residence or economic activities, between the regulating State and the person principally responsible for the activity to be regulated or between that State and the one the regulation is designed to protect; (c) the character of the activity being regulated, the significance of the regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which the desirability of such regulation is generally accepted. (d) the existence of legitimate expectations that could be protected or harmed by the regulation; (e) the importance of the regulation for the international political, legal, or economic system; (f) the extent to which the regulation is in accordance with the traditions of the international system; (g) the extent to which another state may have an interest in regulating the activity; and (h) the likelihood of conflict with the regulations of another state (Restatement 1987, para 403(2)) The standard of reasonableness is, in paragraphs 3 and 4 of the same article of the Restatement, used to determine jurisdiction to try and enforce judicial and extrajudicial decisions. This standard, however, is not without problems.

international community, both at the universal level, within the United Nations, and at regional levels (Council of Europe, European Union), intervened in the field of computer crime. Consequently certain international documents in the field of high-tech crime, which foresee criminal acts and mechanisms by which these acts can be prevented, also determine the rules on jurisdiction for the prosecution of these criminal acts. The most detailed and relevant, certainly, is the Convention on High-tech Crime.

It can be stated that significant progress has been achieved on the international level with regard to the normative regulation of computer crime, but that there are still significant problems related to international cooperation and global efforts to combat computer crime.[4]

4. International standards contained in United Nations documents

As part of the work of the General Assembly, the United Nations adopted several resolutions dedicated to computer crime.[5]

Work in the field of legal regulation of computer crime The United Nations began in 1990, when the Resolution on legislation in the field of computer crime was adopted at the VIII UN Congress on the Prevention of Crime and the Treatment of Offenders (8th UN Congress on the Prevention of Crime and the Treatment of Offenders) held in Havana. After the adoption of this Resolution, in 1994, the OUN Manual on the prevention and control of computer crime was adopted, and then in May 1998, the Geneva Resolution on the abuse of the Internet for the purpose of sexual exploitation. The Geneva resolution stated that the Internet is currently the most unregulated communication network in the world with new technologies that represent a major challenge for national and international regulation and application, and warned that various forms of sexual exploitation are being promoted on the Internet for the purpose of sexual entertainment. In order to reduce these phenomena, the Resolution contains

[4] The most important problems are: different legal definitions of the actions of computer crime; insufficient training of police officers, prosecutors and judges who act in cases of computer crime; inconsistency of procedural rules in criminal laws when it comes to the investigation and prosecution of computer crimes; non-functioning or absence of international legal assistance. See more: (Bejatović, 2012, p. 22).

[5] These resolutions, it is true, do not have binding force for the member states and are mostly declarative in nature, but they should be mentioned because they contain a call to all states to harmonize legislation in this area as soon as possible in order to eliminate the so-called "safe states" for computer crime in which harmful behaviors related to misuse of computers, information and communication technologies are not criminalized and sanctioned (Vidić, 2016, p. 256).

recommendations to influence the reduction of human trafficking, prostitution and sexual exploitation on the Internet. [6]In 2000, the General Assembly of the United Nations adopted the Resolution on the fight against misuse of information technologies. This Resolution highlights the importance of certain measures in the fight against misuse of information technologies.[7]

At the 10th Congress of the United Nations in 2005, which was dedicated to crime prevention, a working group of experts defined computer crime as a general term that includes criminal acts committed through computer systems or networks. This means that this term includes any criminal offense committed in the electronic environment (Matijašević & Ignjatijević, 2010, p. 853). In the plenary part of the session dedicated to computer crime, it was stated that it is possible to recognize two types of computer crime (Nikić, 2010): (1) computer crime in the narrower sense, which includes any illegal behavior aimed at the electronic security operations of computer systems and the data processed in them (which includes acts related to unauthorized access to a computer system or network by violating security measures; damage to computer data or programs; computer sabotage; unauthorized interception of communications from and in computer systems and networks; computer espionage), (2) computer crime in the wider sense, which includes any illegal behavior related to or in relation to a computer system and network, including such criminality as the illegal possession, offering and distribution of information through computer systems and networks (such as computer forgery; computer theft; technical manipulation of devices or electronic skim components of the device; abuse of

[6] In the recommendations, the governments of the signatory countries and non-governmental organizations are suggested to, as a priority, consider amendments and implementation of existing laws or pass new laws in order to prevent the abuse of the Internet for trafficking, prostitution and sexual exploitation of women and children; classes investigation related to the misuse of the Internet for the purposes of promoting and/or conducting trade, prostitution and sexual exploitation of women and children; undertake more vigorous measures in order to eliminate human trafficking, exploitation of prostitution and sexual exploitation on the Internet; develop educational programs, policies and laws regarding the use of the Internet by users of prostitution; conduct an investigation and use as a record of criminal acts and acts of discrimination advertising, correspondence and other forms of communication over the Internet that are used to promote sex trade, prostitution, sex tourism, bride trafficking and rape; develop good cooperation at the level of national and regional bodies of criminal services in the fight against the escalation of trafficking and prostitution of women and children, the globalization of this industry and the abuse of the Internet to promote and implement acts of sex trafficking, sexual tourism, sexual violence and sexual exploitation.

[7] Two measures are listed as the most important measures: the first is that states must provide such laws and practices that will eliminate any possible "sanctuary" for those who misuse information technologies in the criminal sense; and secondly, that the legal system must protect and respect the confidentiality, integrity and availability of electronic data and computer systems, so that their abuse and unauthorized use do not occur and that every perpetrator of such a crime is sanctioned.

payment systems such as manipulation and theft of electronic credit cards or use of false codes in illegal financial activities).

As can be concluded from this brief overview, it is clear that there is still no universal convention or any other act that comprehensively regulates the issue of cyber and computer crime, but the regulation is limited to recommendations, manuals and the like. On the other hand, efforts within the UN are mainly focused on substantive criminal law, that is, prescribing a unique definition of certain forms of computer crime, while defining jurisdiction for prosecuting these crimes is, for now, on the back burner.

However, with the increasingly widespread occurrence of computer crime, and attacks directed at the computer systems and databases of various governments and international organizations, while the perpetrators of these acts are as a rule outside the jurisdiction of the injured states or international organizations, namely the United Nations, therefore, announced the imminent adoption of the text of the universal convention on cybercrime.

In our opinion, when regulating this issue, the United Nations should, as a starting point, take the Convention of the Council of Europe on high-tech crime no. 185 from 2001, and the concept of obligation and rules to preserve national sovereignty should be regulated according to the model of the UN Convention on Combating Transnational Organized Crime.

5. Standards contained in the documents of the Council of Europe – Budapest Convention

Convention no. 185 adopted within the framework of the Council of Europe in 2001, after several years of work on harmonizing the integral text of this convention.

Council of Europe Convention on High-Technological Crime 185 from 2001, Additional Protocol to the Convention on High-Technological Crime, which refers to the criminalization of acts of a racist and xenophobic nature committed via computer systems (Strasbourg, 28.01.2005), as well as the Second Additional Protocol to the Convention on High-Technological Crime to crime related to enhanced cooperation and the discovery of electronic evidence [8]are the

[8] The second additional protocol to the Convention on High-tech Crime was adopted, after several years of negotiations on the text of this Protocol, in November 2021, and was opened for signature in May 2022; For now, this Protocol has been signed by 24 countries (18 members of the Council of Europe and 6 non-member states, including the USA), but no country has yet ratified this Protocol. The entry into force of the Protocol is subject to ratification by five countries. The Republic of Serbia has signed, but not yet ratified, this Protocol.

first international documents which, on a broad level, regulate the substantive, organizational, procedural and international framework of criminal offenses committed via the Internet and other computer networks. The adoption of these documents is the result of a Council of Europe initiative formally launched in 1996 with the establishment of the Committee of Experts on Cybercrime. The convention is an international legal instrument that for the first time regulates problems related to high-tech crime and modern media (Dragojlović & Krstinić, 2015, p. 95).

The convention has as its goal, first of all, the harmonization of domestic substantive criminal law provisions in the field of computer crime, enabling the domestic criminal procedural legal framework to provide competent state authorities with the powers necessary for the effective detection and prosecution of perpetrators of these crimes, as well as the establishment of a quick and effective framework of international cooperation in this area. The provisions of the Convention are systematized in four chapters: the first chapter defines the concepts, the second, foresees the measures that need to be taken at the level of individual states within the framework of criminal substantive and procedural legislation, the third chapter refers to international cooperation within the framework of mutual assistance in the fight against computer crime and the fourth relates to the final provisions of signing and entry into force (accession, territorial application, declarations, reservations, settlement of disputes, cancellation, etc.). The importance of the Convention lies primarily in the fact that its adoption enabled national legislations to develop their own network of combating computer crime based on the provisions of the Convention (Vidić, 2016, p. 265).

When, on the other hand, we talk about the rules on jurisdiction for prosecuting computer crimes, the Convention devotes only one article to this issue: Article 22 of the Convention.

According to the provision of this article, paragraph 1, each "Contracting Party should adopt legislative and other measures necessary to establish jurisdiction for each act prescribed in accordance with articles 2–11 of this Convention, when the act is committed:

a) on its territory; or
b) on a ship under the flag of that contracting party; or
c) in an aircraft registered in accordance with the laws of that contracting party;
d) by its citizen, if the act is punishable under the criminal law of the country where it was committed or if the act was committed in a place outside the jurisdiction of any country."

From the above, it can be clearly determined that, in this paragraph, the Convention sets as a general rule, and insists on it, jurisdiction according to the traditional principle of territoriality[9] – the contracting state will have jurisdiction when the act was committed on its territory, accepting, at the same time, the rules on extraterritorial places and jurisdictions of the state. This approach, although theoretically and legally correct, which stems from the concept of sovereignty, can no longer be accepted in modern conditions.

It is true that point g) of this paragraph allows the contracting state to prosecute its citizen for an incriminated offense that he committed abroad, but only if that offense is double incriminated – that it is prescribed as a criminal offense both in the country that wants to undertake the criminal prosecution of his citizen, as well as in the state where the act itself was committed. Also, the state will have jurisdiction to prosecute even if the crime was committed in an area that does not fall under the jurisdiction of any other state.[10] However, these rules on criminal jurisdiction are, in our view, part of the generally accepted legal principle regarding criminal jurisdiction and the interest of each state, and represent the usual "expansion" of the criminal jurisdiction of a country, and not specific rules on the jurisdiction of this Convention.

Thus, adapting and more extensively understanding the concept of territoriality, the Report (para. 233) points out that, according to Article 22, paragraph 1a, the contracting state could establish territorial jurisdiction if both the perpetrator (attacker of the computer system) and the attacked system are located within the territory of that country (which is the

[9] The report should not be understood as an authentic interpretation of the Convention. However, it is de facto an authoritative source of law. This is because in practice preparatory reports, notes and drafts from sessions where the text of any international agreement (fr. Travaux preparatoires) was prepared are regularly used as a means of interpreting the agreement or determining the intention of the contracting parties. In this sense, Article 32 of the Vienna Convention on the Law of Treaties foresees preparatory works as a way of interpreting an international treaty.

[10] It is interesting to point out that, according to the Report (para. 235), "the area that does not fall under the jurisdiction of any other country" should primarily be understood as the area that is outside the borders of the planet Earth – that is, space and, analogously, space bodies. As, according to customary international law, as well as the corresponding documents of the United Nations, no country can establish jurisdiction in space, and it is the good of all humanity, in the event that a cyber attack is carried out outside the space of the planet Earth, the jurisdiction to prosecute that act would every country had. This solution, as well as the far-reaching view that its authors had, can only be criticized in terms of resolving conflicts of jurisdiction in the event that when the act is possible to be done in outer space, and it is done, what will happen if several states establish your jurisdiction? This is because this Convention does not establish a clear mechanism for resolving conflicts of jurisdiction, except for the provision of paragraph 5 of the same article, according to which the contracting parties will "consult" regarding the determination of the most suitable jurisdiction for prosecution.

application of the classical principle of territoriality), but the state will have the authority to prosecute even when only the attacked computer system is located within the territory, regardless of whether the perpetrator of the act (according to the Report – the "attacker") is not located on the territory of that country. This approach can be justified from two aspects. First, the very nature of computer crime, which often has an international element, dictates the expansion of the traditional concept of territorial jurisdiction. Especially in modern times, it is relatively common for attacks on computer systems in one country to come from the territory of another country. If the requirement that both the attacked system and the attacker should be located on the territory of the same country, in order for it to have jurisdiction, would remain, the efforts of the international community to combat transnational computer crime would be significantly obstructed. In addition, such type of criminal activity would not need to be regulated at the international level – it would be the domain of exclusive national jurisdiction. In addition, the general interest of the international community, embodied through various international and regional organizations, is not to intervene and regulate the internal issues of each country, but to normatively regulate those issues that are of international importance, that have an international element, that is, that concern several countries. On the other hand, it is a theoretically legally acceptable position regarding extended territorial jurisdiction if the moment of the committed act is taken into account. Namely, criminal acts of computer crime, as a rule, are not consequential crimes. Therefore, it is not required that the damage actually occurred, or that the data was actually changed. For the existence of a crime, it is sufficient that a breach in the computer system (hacking) has occurred. Even the penetration of the computer system represents damage in itself, and the deed is completed.[11] Therefore, although the opposite could be argued, we believe that, bearing in mind the peculiarity of computer crime, it can be considered that the consequence of the action – hacking – occurred on the territory of the country where the specific computer system is located. In addition, the

[11] This does not mean that there are no other criminal acts that incriminate different behavior and that contain additional or broader elements of the criminal act. Thus, there are also those criminal acts that require a special element of intent – for example, Article 300 of the Serbian Criminal Code provides for the act of creating and introducing computer viruses, and where the existence of the criminal act is conditioned by the existence of intent – the act of creating a computer virus with intent is criminalized its entry into someone else's computer or computer network. However, it is not necessary that the introduction of the virus actually occurred, nor that it was attempted. For the existence of a criminal offense, it is sufficient to prove that the virus was created and that the intention to introduce it existed.

country in whose territory the computer system that is attacked has the strongest interest in prosecuting the attackers of that computer system. For all the reasons stated, this determination of the authors of the Convention is completely acceptable, reasonable and justified.

When it comes to the rules on extraterritorial places and jurisdiction, paragraph 2 of Article 22 of the Convention stipulates that each Contracting Party may retain the right not to apply, or to apply only in certain cases or under certain circumstances, the rules on jurisdiction specified in paragraphs 1b) to 1g) of this article or in another part of that article. The linguistic interpretation alone easily leads to the conclusion that this provision allows the contracting states to express reservations in relation to the rules of jurisdiction in these cases, in such a way as to completely exclude the application of these rules, or to partially exclude them, or to bind their application to occurrence of any additional condition (Report, para. 238). However, the contracting states cannot exclude, limit or condition the application of the rule of territorial jurisdiction from point a) of this paragraph, considering that the exclusion of that basis of jurisdiction would completely defeat the purpose of international regulation of this issue.

Each Contracting Party should adopt the measures necessary to establish its jurisdiction over the acts listed in Article 24, paragraph 1 of this Convention, after submitting a request for extradition, in cases where the suspect is on its territory and the Contracting Party only of his or her citizenship, shall not be extradited to the other contracting party (Article 22, paragraph 3 of the Convention). This provision embodies the general legal principle of public international law *aut dedere aut judicare* (extradite or prosecute). In the case when the contracting party refused to extradite the alleged perpetrator of the crime prescribed by the Convention on the basis of his nationality, and the perpetrator is present on its territory, it was necessary to prescribe the jurisdictional rule from paragraph 3, to ensure that those states that refuse to extradite citizens have the legal possibility to, instead of extradition, undertake investigation and prosecution, if requested by the contracting state that requested extradition in accordance with the rules of "Extradition", from Article 24, paragraph 6 of this Convention (Report, para. 238). This rule, therefore, preserves the basic principle of international law – deliver or judge. In addition, if one member state could refuse both extradition and trial for the offense provided for in the Convention, then neither the Convention itself nor the international regulation of the fight against international computer crime would have any meaning or purpose. That is why the obligation provided for in this provision is, by its very nature, an objective obligation – states

are obliged to adopt the measures necessary to preserve the *extradite or try principle.*

According to paragraph 4 of Article 22, this Convention does not exclude jurisdiction for any criminal prosecution undertaken in accordance with domestic law. As already pointed out, this Convention was adopted after several years of consultation and harmonization of the draft of its text. In addition, it represents a compromise of different countries, different systems and political interests. In addition, this Convention aimed to establish a minimum of uniform rules in this area. That is why, in this position, it has been established that the rules on the bases of jurisdiction set forth in this article are not *numerus clausus,* that is, they are not of an exclusive nature, and the contracting parties are essentially free to, in accordance with their internal criminal legislation, establish other bases and types of criminal jurisdiction (Report , para. 238).

When several Contracting Parties assert jurisdiction over an alleged act prescribed in accordance with the Convention, those Contracting Parties shall consult each other, when appropriate, regarding the determination of the most appropriate jurisdiction for prosecution (Article 22, paragraph 5 of the Convention). Therefore, as it was pointed out earlier, this Convention, taking into account all the circumstances in which it was adopted, does not contain a concrete mechanism for resolving conflicts of jurisdiction. That is, there are no clear rules according to which the dispute will be resolved if two or more states simultaneously establish jurisdiction in relation to the same offense and the same perpetrator. According to the explanation from the Report (para. 239), it can be concluded that the idea was that, in the case when several of them establish jurisdiction, they will agree on where to prosecute and for which offense, all guided by the rational interests of easier enforcement investigations, prosecutions, evidence, etc. However, this explanation seems more like an effort to justify the prescribed rule as completely reasonable and logical, and not as a result of the impossibility of political compromise. It is completely clear that no country wants to give up its jurisdiction, as an expression of its sovereignty. Each state will therefore have an interest and a desire to prosecute the perpetrator of an act directed against it, its order and its subjects. However, it is also a reality that at a given moment it was necessary to first make a step forward in the fight against computer crime at the international level, and during the adoption of this Convention a compromise was made regarding the rules on jurisdiction. This is all the more so since even the consultations prescribed by paragraph 5 of Article 22 are not mandatory in every case of jurisdictional disputes, but will only take place “when it is

appropriate." This, further, means that if State A considers that consultations are expedient, and State B considers that they are not, consultations will not take place (Report, para. 239).

In truth, with the special and extensive rules on international cooperation contained in the Convention (Articles 23-35 of the Convention), the authors of the Convention tried to replace the relatively loose rules on jurisdiction with extensive rules and obligations on international cooperation. This effort is further embodied in the 2021 Second Additional Protocol on Enhanced Cooperation and Discovery of Electronic Evidence.

The Budapest Convention certainly represented the first and important step in the right direction towards universal regulation of the issue of combating and suppressing international computer crime, which is more relevant today than ever. In addition, this Convention laid the foundations for individual national legislations to more precisely determine the features and characteristics of individual computer crimes, their basic, easier or more serious forms, and to prescribe criminal sanctions for their perpetrators (natural or legal entities) (Jovašević, 2014, p. 41).

6. National standards regarding competence for prosecuting criminal offenses of computer crimes

When it comes to domestic legislation, it is necessary to look at the issue of computer crime from the aspect of assumed international obligations and from the aspect of the internal regulation of normative and institutional regulation of the issue of jurisdiction for the prosecution of criminal acts of computer crime.

Regarding the aspect of assumed international obligations, the Republic of Serbia signed the Council of Europe Convention on High-tech Crime and the Additional Protocol back in 2005, and finally ratified them in 2009, without reservations or declarations. In addition, the Republic of Serbia signed the Second Additional Protocol to this Convention in May 2022, but it has not yet been ratified. The Republic of Serbia hereby undertakes to prescribe and establish normative and institutional prerequisites for successfully combating computer crime.

To that end, several regulations (laws and by-laws) were adopted in which certain provisions of the Convention were implemented and on the basis of which an institutional framework was created for their implementation. The most important among them are the following laws: the Law on the Organization and Competence of State Bodies for Combating High-Tech

Crime[12], the Criminal Code of the Republic of Serbia and the Criminal Procedure Code of the Republic of Serbia.

The Law on the Organization and Competence of State Bodies for Combating High-Tech Crime is undeniably the most important legal document in the fight against this type of crime in Serbia (Dragojlović & Krstinić, 2015, p. 98). This Law determines the institutional framework for the implementation of the provisions of the law related to high-tech crime, and it foresees special organizational units of existing state bodies, whose actions contribute to better protection against computer crime and the implementation of preventive and repressive measures. The specialization of state authorities to fight against computer crime is necessary due to the complexity and special characteristics of computer crime, the necessity of special knowledge in this area (Dragojlović & Krstinić, 2015, p. 98) as well as due to the constant monitoring of the development of modern computer technologies.

Special rules on jurisdiction refer to special state bodies that are responsible for detecting, prosecuting and adjudicating high-tech crimes. This primarily refers to special units within the Ministry of Internal Affairs, the Special Prosecutor's Office for High-Tech Crime, as well as the rules on jurisdiction. Thus, the Law on the Organization and Competence of State Bodies for Combating High-Tech Crime, Article 4, Paragraph 1 prescribes that the Higher Public Prosecutor's Office in Belgrade is responsible for handling cases of criminal offenses from this law for the territory of the Republic of Serbia, while Paragraph 2 of the same Article prescribes that a special department for the fight against high-tech crime be formed in the High Public Prosecutor's Office in Belgrade (hereinafter: Special Prosecutor's Office). According to Article 5, the work of this Special Prosecutor's Office is managed by the High-Tech Crime Prosecutor, who is appointed for a period of four years by the Public Prosecutor of the Republic, with the consent of the appointed person. This Prosecutor has all the rights and obligations of a public prosecutor (according to the latest amendments to the Constitution of the RS,

[12] According to Article 3, this Law is applied for the purpose of detection, prosecution and trial of criminal offenses against the security of computer data specified in the Criminal Code and – criminal offenses against intellectual property, property, economy and legal traffic in which the object or means of execution of criminal offenses occur computers, computer systems, computer networks and computer data, as well as their products in material or electronic form, if the number of copies of copyrighted works exceeds 2,000 or the resulting material damage exceeds the amount of 1,000,000 dinars, as well as criminal offenses against human freedoms and rights and citizen, sexual freedom, public order and peace and constitutional order and security of the Republic of Serbia, which due to the method of execution or the means used can be considered criminal acts of high-tech crime.

he is the Chief Prosecutor). On the other hand, the provisions of Article 10 and 11 of the Law define the jurisdiction and organization of courts in terms of trials for criminal offenses within the scope of this Law. Thus, Article 10, Paragraph 1 stipulates that the High Court in Belgrade is competent for dealing with cases of criminal offenses from this law, for the territory of the Republic of Serbia, while Paragraph 2 determines that the Court of Appeal in Belgrade is competent for decision-making in the second instance. [13]Article 11, on the other hand, stipulates that the High Court in Belgrade shall establish a (special) Department for the fight against high-tech crime in the High Court in Belgrade to deal with cases of criminal offenses from this Law, which will consist of judges appointed by the President of the High Court in Belgrade from among the judges of that court , for a period of 2 years, and with their consent.

With regard to the organization and competence of the internal affairs body, as an investigative body, in Article 9 of the Law on the Organization and Competence of State Bodies for Combating High-Tech Crime, the Office for the Fight against High-Tech Crime is established for the work of the internal affairs body in cases related to these crimes which is located within the Ministry of Internal Affairs, and which acts according to the requests of the Special Prosecutor.

So, as we can see, with this Law, the concentration of jurisdiction was carried out both in terms of the actions of the prosecution, as well as in terms of the actions and trials of the court, by this regulation deviating from the general rules of local jurisdiction contained in the Code of Criminal Procedure by jurisdiction is concentrated in the High Public Prosecutor's Office in Belgrade and the High Court in Belgrade, with their special departments. In practice, there are no major problems in determining the competence for the actions of special departments. In addition, although it is not explicitly determined by this Law, the High Court in Belgrade is the only one competent to provide international legal assistance in criminal acts of high-tech crime, in the sense of the Budapest Convention. This approach, according to the author, could be initially accepted, taking into account the fact that high-tech crime was not so widespread at the time of the adoption of the first law in this area (2005). However, in modern times, the prevalence of computer crime, which our

[13] It was completely unnecessary, in our opinion, to determine that the appellate jurisdiction belongs to the Court of Appeal in Belgrade. Since the High Court in Belgrade (in a special department) judges in the first instance, it is quite logical that the Court of Appeal in Belgrade will also have jurisdiction over the appeal, which is also a general rule contained in the Law on the Organization of Courts. Therefore, the inclusion of this provision in a separate law cannot be justified.

legislator defined even more widely than the international standard, is so great that it would be completely justified, if not necessary, to establish appropriate special departments of the prosecution and courts in Novi Sad, Kragujevac and Nan, and in that sense, a partial deconcentration of jurisdiction should be implemented, and as it was done also with regard to organized crime.

7. Conclusion

Computer crime certainly represents one of the biggest security challenges of the twenty-first century, both for developed and less developed countries. Effective prevention, detection and initiation of proceedings against perpetrators of criminal offenses is further hampered by its transnational character.

The international community, due to different interests, which mostly rest on the sovereignty of each state, has not yet established minimal uniform rules on a universal level that would regulate some issues in the field of cybercrime. The Council of Europe, as a regional organization, has, we have seen, intervened and adopted the Convention on High-Tech Crime, with two additional protocols. However, even within these documents, the question of jurisdiction is loosely regulated, precisely because of the absence of the will of the contracting states to renounce their jurisdiction for criminal acts of computer crime. There, as the biggest problem, the issue of resolving conflicts of jurisdiction may arise when one of the states claiming jurisdiction does not consider it expedient to participate in the consultations. Protection of the national interest, the principle of sovereignty and jurisdiction for criminal prosecution as an expression of the same, are certainly high values that the state should protect. However, the danger of transnational cybercrime is immediate and high, and this circumstance must have an impact on the attitude of countries regarding the prosecution of these acts prescribed by the Convention. The idea of establishing a European tribunal for high-tech crime, with complementary jurisdiction, does not seem completely unacceptable either – if the states fail to agree, through consultation, on which of them will exercise jurisdiction. Certainly, it is necessary for the international community to settle this issue in the shortest possible time in the most comprehensive way.

When it comes to our country, Serbia, by ratifying the Convention and the Additional Protocol and incorporating its provisions into the national legislation, has shown a clear will and readiness to fight against high-tech crime, and the normative solutions in Serbia in this area represent a good basis for leading a successful fight against this type of crime. criminality. Also, the existing

normative solutions are harmonized to a significant extent with European standards, i.e. with the Convention and the Additional Protocol. However, in the future, we should work on strengthening the technical-technological and personnel conditions for detecting and prosecuting these crimes. In addition, *de lege ferenda,* our legislator should carry out a partial deconcentration of jurisdiction from Belgrade to Novi Sad, Kragujevac and Niš.

Dragojlović Joko
Pravni fakultet za privredu i pravosuđe u Novom Sadu, Univerzitet Privredna akademija u Novom Sadu, Srbija

NADLEŽNOST ZA KRIVIČNA DELA RAČUNARSKOG KRIMINALITETA – MEĐUNARODNI I NACIONALNI STANDARDI

REZIME: Krivična dela računarskog kriminaliteta ne predstavljaju više novu društvenu i pravnu pojavu. Pored izvršenja krivičnih dela koja spadaju u domen računarskog kriminaliteta, računari su svoju primenu našli i kod izvršenja tkz. klasičnih krivičnih dela, dajući im drugačiji modus operandi. Prostorna distanca između preduzete radnje i nastale posledice prilikom izvršenja krivičnih dela računarskog kriminaliteta, doveli su do jačanja transnacionalnog kriminala. Inicijalno, međunarodna zajednica je nastojala intervenisati u ovoj oblasti, sa idejom da uredi krivično gonjenje učinilaca prekograničnih krivičnih dela računarskog kriminaliteta. Međutim, do danas nije usvojen normativni okvir koji će na univerzalnom nivou urediti pitanje gonjenja učinilaca ovih krivičnih dela. U tom smislu, u radu je izvršena analiza postojećih međunarodnih standarda u pogledu normativnog uređivanja nadležnosti za gonjenje učinioca transnacionalnih računarskih krivičnih dela, a pored toga, dat je i prikaz normativnog uređenja ovog pitanja u domaćem zakonodavstvu. Cilj ovog rada je da ukaže na poteškoće koje nastaju prilikom regulisanja nadležnosti kod krivičnih dela računarskog kriminaliteta, kao i analiza postojećih nedostataka i ukazivanje na eventualne pravce budućeg regulisanja.

Ključne reči: *računarski kriminalitet, transnacionalna krivična dela, nadležnost, međunarodni standardi, Konvencija iz Budimpešte.*

References

1. Bejatović, S. (2012). Visokotehnološki kriminal i krivičnopravni instrumenti suprotstavljanja [High-tech crime and criminal legal instruments of opposition]. In: Šikman M. (ured.), *Suzbijanje kriminala i evropske integracije s osvrtom na viskotehnološki kriminal* [*Suppression of crime and European integration with reference to high-tech crime*]. (pp. 17-30), Banja Luka: Visoka škola unutrašnjih poslova
2. Brenner, S. W., Koops, B., J. (2004). Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law*, *4*(1), pp. 3-46
3. Dragojlović, J., & Krstinić, D. (2015). Evropski standardi u borbi protiv visokotehnološkog kriminaliteta i njihova implementacija u zakonodavstvu Republike Srbije [European standards in the fight against high-tech crime and their implementation in the legislation of the Republic of Serbia]. *Evropsko zakonodavstvo*, *14*(51), pp. 92-103
4. Goodman D., M., & Brenner W., S., (2002). The Emerging Consensus on Criminal Conduct in Cyberspace, *International Journal of Law & Technology*, *10*(2), pp. 139-223
5. Gordon, S., Ford, R. (2006). On the definition and classification of cybercrime, *Journal of computer virology*, *2*(1), pp. 13-20
6. Jovašević, D. (2014). Računarski kriminalitet u Srbiji i evropski standardi [Cybercrime in Serbia and European standards]. *Evropsko zakonodavstvo*, *13*(47-48), pp. 40-56
7. Jovašević, D., & Hašimbegović, T. (2004) Krivičnopravna zaštita bezbednosti računarskih podataka [Criminal Protection of Computer Data Security]. In: Petrović, R., (ured.), *Zloupotreba informacionih tehnologija i zaštita* [*Misuse of information technologies and protection*] (pp. 1-9). Beograd: Udruženje sudskih veštaka za informacione tehnologije
8. Konvencija Saveta Evrope o visokotehnološkom kriminalu br. 185 [Convention on Cybercrime CETS No. 185], 23. 11. 2001
9. Krivični zakonik [Criminal Code]. *Službeni glasnik RS*, br. 85/05, 88/05 – ispr., 107/05 – ispr., 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 i 35/19
10. Matijašević, J., & Ignjatijević, S., (2010). Kompjuterski kriminal u pravnoj teoriji, pojam, karakteristike, posledice [Cybercrime in legal theory, concept, characteristics, consequences], In: *Infoteh Jahorina*, (pp. 852-856), Istočno Sarajevo: Elektrotehnički fakultet u Istočnom Sarajevu

11. Matijašević, J., & Dragojlović, J., (2021). Metodika otkrivanja krivičnih dela računarskog kriminaliteta [Methodology of detection of computer crime offenses], *Kultura polisa*, 18 (posebno izdanje 2), pp. 51-63. DOI: 10.51738/Kpolisa2021.18.2p.1.04
12. Nikić, S., (2010). Najčešće metode napada cyber kriminalaca i kako se odbraniti [The most common methods of attack by cybercriminals and how to defend yourself]. In: Petrović, R., (ured.), *Zloupotreba informacionih tehnologija i zaštita* [*Misuse of information technologies and protection*]. (pp. 265-279). Beograd: Udruženje sudskih veštaka za informacione tehnologije
13. Parker, D., B., (1989). *The Cybercrime: Criminal Justice Resource Manual*, Washington: National Institute of Justice
14. Petrović, B., Jovašević, D. (2006). Izvršno krivično/kazneno pravo [Enforcement criminal/penal law]. Sarajevo: Pravni fakultet
15. Priručnik UN o sprečavanju i kontroli kompjuterskog kriminala [United Nations Manual on the Prevention and Control of Computer-related Crime], 1994. Downloaded 2022, September 15 from https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF
16. Report and Guidance on Privacy in Social Network Services – "Rome Memorandum" – 43rd meeting, 3-4 March 2008, Rome (Italy). Downloaded 2022, September 15 from https://www.gpdp.it/documents/10160/10704/1531476
17. Restatement (Third) Of Foreign Relations Law Of The United States (1987). Downloaded 2022, September 16 from https://www.ali.org/publications/show/foreign-relations-law-united-states-rest/
18. Rezolucija Ujedinjenih Nacija A/res/55/63 o borbi protiv zloupotrebe informacionih tehnologija [UN resolution A/res/55/63 on combating the criminal misuse of information technologies], 04. 12. 2000
19. Rezolucija Ujedinjenih Nacija o zakonodavstvu u oblasti kompjuterskog kriminaliteta [UN Resolution on computer crime legislation], 07. 09. 1990.
20. Vidić, V. (2016). *Povreda prava na privatnost zloupotrebom društvenih mreža kao oblik kompjuterskog kriminaliteta – doktorska disertacija* [*Violation of the right to privacy by abuse of social networks as a form of cybercrime – doctoral dissertation*]. Niš: Pravni fakultet
21. Vukadinović, G., & Avramović, D. (2014). *Uvod u pravo* [*Introduction to Law*]. Novi Sad, Pravni fakultet

22. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala [Law on Ratification of the Convention on High-Tech Crime]. *Službeni glasnik* RS, br. 61/05 i 104/09
23. Zakonik o krivičnom postupku [Code on Criminal Procedure]. *Službeni glasnik RS*, br. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14, 35/19, 27/21 – odluka US i 62/21 – odluka US