Dragojlović Joko*
https://orcid.org/0000-0002-4713-1855
Petrović Maja**
https://orcid.org/0000-0003-2342-196x

UDC: 343.9.02:004.738.5
Review article
DOI: 10.5937/ptp2404134D
Received on: October 8, 2024
Approved for publication on:
October 29, 2024
Pages: 134–151

REFERENCE TO THE COMPETENCE AND SPECIALIZATION OF AUTHORITIES FOR THE PROSECUTION OF PERPETRATORS OF HIGH-TECH CRIMINAL OFFENSES

ABSTRACT: With the development of technology, especially the emergence and expansion of the internet over the past two decades, many traditional crimes have acquired new methods and means of execution, such as the use of computers, mobile phones, or other devices. In response to these new ways of committing crimes, the international community, within the framework of the Council of Europe, adopted the Budapest Convention in 2001, specifically addressing cybercrime. After ratifying the convention, the domestic legislator passed the Law on the Organization and Competencies of State Bodies for the Fight against High-Tech Crime, incorporating legal provisions from the convention. This law has not been significantly changed or amended since its adoption. However, the provisions in this law, especially in terms of jurisdiction, have proven to be inadequate and overly broad. The wide range of criminal offenses covered by this law has made it relatively ineffective and has overburdened the prosecutor's office responsible for prosecuting high-tech criminals. Moreover, the approach taken by the legislator in 2005, which concentrated

* LLD, Associate Professor, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary in Novi Sad, Novi Sad, Serbia, e-mail: jdragojlovic@pravni-fakultet.info
** LLD, Assistant Professor, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary in Novi Sad, Novi Sad, Serbia, e-mail: maja.subotin@pravni-fakultet.info

jurisdiction in the High Public Prosecutor's Office and the High Court in Belgrade, is no longer justifiable in today's age of widespread technology, internet access, and social networks. This paper aims to provide a brief overview of the Budapest Convention, which served as the foundation for the adoption of national regulations, and to highlight the shortcomings and unsustainability of the legal solutions proposed by the domestic legislator when national regulations in this field were established in 2005.

Keywords: *high-tech crime, criminal law, jurisdiction, specialization.*

1. Introduction

As in many other spheres of social life, technology has significantly changed the way crimes are committed today, not only facilitating new methods of committing traditional crimes, but also creating new forms of criminal activity. Technological progress has enabled the development of unique means of committing criminal acts, be it classic or completely new forms of crime. In the modern world, technology and the Internet have become almost ubiquitous, accessible to every part of the planet. Computers, smartphones, the Internet and personal accounts on social networks have become an integral part of everyday life, opening up space for abuse.

With the expansion of the use of these technologies, a new social phenomenon appeared – high-tech crime, also known as cybercrime. This form of crime encompasses a wide range of illegal activities that use computers, networks and the Internet as the primary means of execution. Cybercrime can include hacking, identity theft, distribution of malicious software, online fraud and other similar activities, which pose a serious challenge to justice systems and law enforcement institutions.

This specific form of crime is becoming increasingly relevant in the context of global digitalization, as criminals use advanced technological resources to avoid the justice system and international borders, thereby further complicating the process of their detection and prosecution. Precisely because of this, the fight against high-tech crime requires the establishment of modern technological tools, as well as international cooperation, in order to effectively respond to the challenges brought by the rapid development of technology. This type of criminality also has specific perpetrators of criminal acts, the criminal acts themselves are committed very quickly, and the specific criminal acts of computer crime imply that they are committed through

computers, that is, computers are used as a means of execution or as an object against which a criminal act is committed (Vidić, 2016, p. 94).

In terms of defining this emergent type of crime, from the broadest point of view, it can be stated that high-tech crime implies both active and passive use of computers, and even keeping evidence of the committed crime in a computer or in electronic form, while the victims and possible victims are all physical and legal entities that use computers and databases or depend on their use (Rome Memorandum, 2008).[1]

As this phenomenon caused the concern of the international community, states undertook normative activities, both at the international and national level. Following international standards, and in the first place the convention of the Council of Europe from Budapest, the domestic legislator passed a special law – the Law on the Organization and Competence of State Bodies for the Fight against High-Tech Crime (hereinafter the Law on VTK) which regulated the issue of high-tech crime in our country – regulated the issue (concentration) of subject matter and territorial jurisdiction of judicial bodies, units of the Ministry of Internal Affairs, specialization of bodies and other issues. However, the approach that the legislator (justifiably) applied back in 2005 when he passed this legal text cannot be accepted today – at a time when, for example, the Special Prosecutor's Office for High-Tech Crime processes over 6,000 cases a year.

This paper seeks to provide a brief overview of the Budapest Convention, which served as a basis for the adoption of positive regulations in this area, and then to point out the shortcomings and unsustainability of the legal solutions that the domestic legislator envisioned when, in 2005, he adopted national regulations from this area.

2. Convention on high-tech crime (the so-called "Budapest Convention")

Bearing in mind the seriousness and potential danger that technology has brought with it, the international community has, to a certain extent, normatively intervened in this area as well. This normative intervention was not of a universal character, so the convention was not adopted at the level

[1] Vidić (2016) notes that there are many names used for this same phenomenon, both at the international and national levels. The legislator opted for the term "high-tech crime"; bearing in mind the availability of this technology nowadays, the question can reasonably be raised as to how high technology it really is, and bearing in mind the widespread use of the term "computer crime", the legislator would be justified in changing the name of the law (pp. 95–96).

of the United Nations. In the absence of a universal convention that would regulate the issue of suppressing high-tech crime, and reluctant to wait for the wider international community, the member states of the Council of Europe adopted a convention related to high-tech crime within the framework of that organization.

Today, that Convention no. 185 appears as the most significant international legal act in the field of criminalization of computer crimes, which was adopted within the Council of Europe in 2001, after several years of work on harmonizing the integral text of this convention (Dragojlović, 2023, p. 66). The convention became known by the city where it was finally adopted – Budapest.

Council of Europe Convention on Cybercrime 185 from 2001, Additional Protocol to the Convention, 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 related to enhanced cooperation and the discovery of electronic evidence[2] are the first international documents that comprehensively 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 provisions of the Convention are systematized in four chapters: "the first chapter defines terms, 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 in the framework of mutual assistance in the fight against computer crime and the fourth refers to the final provisions of signing and entry into force" (Dragojlović, 2023, p. 70).

The domestic legislator acted entirely in accordance with the provisions of this Convention, and criminalized all the acts listed in the substantive part of

[2] The second additional protocol to the Convention on Cybercrime was adopted, after several years of negotiations on the text of this Protocol, in November 2021, and was opened for signature in May 2022; This Protocol has been signed by 24 countries (18 members of the Council of Europe and 6 non-member states, including the USA). The entry into force of the Protocol is subject to ratification by five countries. The Republic of Serbia has signed and ratified this Protocol.

this Convention (Articles 2-13).[3] Articles 14 and 15 of the Convention, which refer to procedural aspects, i.e. the rules for prosecuting persons prosecuted for criminal offenses incriminated by this Convention, are abstract in nature and do not require concrete measures by states – on the contrary, contracting states should "*adopt legislative and other measures necessary to prescribe the powers and procedures provided for in this section, for the purpose of certain criminal investigations or proceedings*" (Budapest Convention, 2001, Article 14, paragraph 1). Characteristic of many obligations contained in international conventions, these obligations are "obligations of the goal" and not "obligations of the means", so a general goal is set for the contracting states that they must fulfill, while the choice of specific means to achieve that goal is left to each contracting country.

In the above sense, the domestic legislator decided to regulate the procedural and organizational aspects by establishing a special prosecutor's office that will prosecute acts with an element of high-tech crime (VTK), the concentration of subject matter and territorial jurisdiction is determined in favor of the Special Department of the Higher Public Prosecutor's Office in Belgrade (designated in the Law on VTK as: Special Prosecutor's Office), but also the High Court in Belgrade and the Court of Appeal in Belgrade. Today, these solutions are subject to considerable criticism, because they appear insufficient and inadequate, and there are special practical problems in their application.

3. Application of the law on high-tech crime – Ratione Materiae –

As is characteristic of the legal texts of our special and secondary criminal legislation (corruption, organized crime), the Law on the Organization and Competence of State Bodies for Fight against High-Tech Crime defines the scope of its application. Certainly, determining the scope of application of the law that falls under secondary (and special) criminal legislation is a common thing, so the limited scope of the law, along with the special measures it carries with it, is what makes it special criminal legislation. However, bearing that in mind, the legislator must be careful when defining the scope and area of

[3] It is interesting to note that the Budapest Convention was adopted in 2001, that our country signed it in 2005, and that it was ratified only in 2009. However, regardless of that, the Law on the Organization and Competence of State Authorities for the Fight against High-Tech Crime was adopted in 2005, which almost completely reflected the rules contained in the Budapest Convention, so it is not clear why the legislature did not immediately ratify this convention.

application of a special law so as not to set it too broadly, because in this way the justification of the special nature of the law is lost, but also the work of special bodies or organizational units that are competent to act is made more difficult.

Defining the definition of high-tech crime, the law, at the same time, defines the subject matter jurisdiction of special bodies and organizational units that are competent to prosecute these criminal acts. Consequently, the Law on VTK determines, in the first place, in Article 2, paragraph 1, its scope, stipulating that "*High-tech crime in the sense of this law is the commission of criminal acts in which computers, computer systems, computer networks appear as the object or means of committing criminal acts, computer data, as well as their products in material or electronic form.*"[4] The definition of VTK set in this way is so broad that nowadays almost any criminal offense regulated by the Special Part of the Criminal Code could be a criminal offense of VTK. In the case of this type of regulation of the scope of application of the law and the subject matter competence of special authorities, the prosecution of these crimes would be almost impossible under the conditions and in the manner provided by the Law on VTK, because due to the extensive number of cases, the competent authorities would be paralyzed. However, in addition to this general provision contained in Article 2, paragraph 1, the legislator additionally determined and limited the scope of application of the law by prescribing Article 3 of the Law on VTK. Namely, the provisions of this article determine that this law is applied for the purpose of discovery, criminal prosecution and trial for:

1) *"criminal acts against the security of computer data determined by the Criminal Code;*
2) *criminal offenses against intellectual property, property, commercial and legal traffic, in which computers, computer systems, computer networks and computer data, as well as their products in material or electronic form, are the object or means of committing criminal acts, if the number of copies author's works exceeds 2,000 or the resulting material damage exceeds the amount of 1,000,000 dinars;*
3) *criminal acts against the freedoms and rights of man and citizen, sexual freedom, public order and peace and the constitutional order*

[4] Paragraphs 2 and 3 of the same article stipulate that products in electronic form specifically mean computer programs and author's works that can be used in electronic form, as well as the following expressions: computer, computer data, computer program, computer virus, computer system and computer network are used in this law and have the meaning in terms of the provisions of the Criminal Code.

> *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, in accordance with Article 2, paragraph 1. of this law."*

Article 2, paragraph 1 and article 3 of the Law on VTK definitively determine *the ratione materiae* of this law.

Bearing in mind the aforementioned provisions of the Law on VTK, high-tech criminal offenses prescribed in the Criminal Code can be conditionally divided into two groups of criminal offenses – those that relate only to high-tech crime and those that have elements of high-tech crime, but are not exclusively within the jurisdiction authorities specialized in combating high-tech crime (Pavlović, 2022, p. 3).

The first group includes eight criminal offenses against the security of computer data, while the second group of criminal offenses is more diverse and includes criminal offenses against intellectual property (Articles 198, 199, 202 of the Criminal Code), but also criminal offenses, such as endangering security, most often through social network (Article 138 Criminal Code); unauthorized publication and display of other people's writings, portraits and recordings (Article 145 Criminal Code); unauthorized collection of personal data (Article 146 Criminal Code); showing, obtaining and possessing pornographic material and exploiting a minor for pornography (Article 185 Criminal Code); using a computer network or communication by other technical means to commit a criminal offense against sexual freedom against a minor (Article 185b Criminal Code), as well as all other criminal offenses if computers or computer networks are used as a means or method of execution.

We see, therefore, that the corpus of criminal acts that constitute the subject matter jurisdiction of special judicial bodies is very rich and diverse. In these cases, the Special Prosecutor's Office will always act first. What's more, the explicit provision of Article 6, paragraph 2 of the Law on VTK stipulates that if the Special Public Prosecutor learns that a criminal case involves the cases prescribed in Article 3 of this Law, he addresses the Supreme Public Prosecutor in writing, requesting from him to entrust or transfer jurisdiction to him. Therefore, as soon as a criminal offense, which is the subject of any phase of criminal proceedings, anywhere in Serbia, has the characteristics of high tech, it, by the very force of the law and automatically, falls under the jurisdiction of the Special Prosecutor's Office and, consequently, the Law on VTK. Neither Article 3 nor Article 6 of the Law on VTK leaves any space for the Special Prosecutor's Office for a discretionary assessment, so it is obliged to act in every case with an element of high-tech crime, regardless

of the seriousness of the act and its consequences. Only the criminal acts referred to in point 2 of article 3 foresee a qualifier – damage that exceeds 1,000,000 dinars or the number of copies of the author's work exceeds 2,000. The setting of this qualifying condition for terminating the jurisdiction of the Special Prosecutor's Office and the application of the Law on VTK can hardly be accepted. Conditioning the application of the Law on VTK and the jurisdiction of the Special Prosecutor's Office on the factor of the damage caused is without criminological and criminal legal justification. Namely, the legislator "elevated" a certain criminal offense to the level of the Special Prosecutor's Office because that crime, due to the object or method of execution, is particularly socially dangerous and because the use of high technology during the execution of the criminal offense makes it difficult to prove and prosecute, so a certain specialization is required and the competence of the prosecuting authorities. Bearing that in mind, it is completely unacceptable to decide that in the case of the criminal offense of extortion (Article 214 of the CC), when the amount of extorted and obtained material benefit amounts to 990,000 dinars, the basic court and the basic public prosecutor's office will be competent, and that in the same circumstances not only High Prosecutor's Office will have jurisdiction but rather the Special Prosecutor's Office, if the value of the stolen is 1,000,001 dinars, where the threat was made through use of high tech, i.e. computer, internet or social networks. The same is the case with frauds that take place via the Internet (e-mail, social networks), when injured persons pay amounts for assistance to a person who does not exist or purchase goods that they do not receive – if the property test is met, it will be under the jurisdiction of the Special Prosecutor's office.

The manner of committing the crime, the means and methods are not different, the difficulties in proving it are the same, so there is no room for making a difference. It is clear that the legislator anticipated the problem of overloading the work of the Special Prosecutor's Office, but, we believe, he tried to narrow the scope of the Law on VTK and the jurisdiction of judicial authorities with a wrong approach.

Furthermore, it is difficult to accept making a distinction in relation to a single criminal offense just because a specific action was taken via the Internet or social networks. For example, the criminal offense of endangering security (Article 138 of the Criminal Code) or stalking (Article 138a of the Criminal Code) will, according to the regular course of things, fall under the jurisdiction of the basic court and the basic public prosecutor's office. If, therefore, the perpetrator directly sends a serious and realistic threat to another person that he will attack his life or body, then it would be an act of endangering security

from Article 138 of the Criminal Code, and the basic public prosecution would act. However, if such threats were not made directly, "face to face", but the threats were made, for example, via the social network Facebook or some other, it would also be a criminal offense under Article 138 of the Criminal Code, but due to the method of execution, it will be a high-tech crime. What's more, in 2023, the Special Prosecutor's Office had the largest number of cases precisely for the criminal offense under Article 138 of the Criminal Code – a total of 186 (Supreme Public Prosecutor's Office, 2024, p. 26). At the same time, it should be kept in mind that it is usually the basic form of this part, from paragraph 1 of Article 138 of the Criminal Code, where a monetary fine or a prison sentence of up to one year is threatened. Simply put, bearing in mind the importance of this crime and its social danger, it is unreasonable for the Special Prosecutor's Office to deal with this crime. Jurisdiction would be justified only in those cases when regular Public Prosecutor Offices, with the usual and regular methods of discovering and proving the crime, would not be able to successfully end the procedure, i.e. only in those cases, when the special circumstances of the crime or its execution require specialization and competence of the Special Prosecutor's office.

There is no doubt that at the time of the adoption of the Law on VTK, prescribing the jurisdiction of the Special Prosecutor's Office in the way it was done was acceptable and meaningful, given that the very concept of high-tech crime was relatively new. In addition, "high" technology was not as common and widespread as it is today. Consequently, the number of criminal offenses that fell under the "umbrella" of this Law, as well as the jurisdiction of specialized judicial authorities, was insignificant. In the first year after the adoption of the Law on VTK and the formation of these bodies, the Special Prosecutor's Office had a total of 19 cases, and in 2007, 154, while the number of cases in 2008 was 184 (Supreme Public Prosecutor's Office, 2024, p. 24). In 2023, the number of criminal cases received by the Special Prosecutor's Office was 6,456 cases (Supreme Public Prosecutor's Office, 2024, p. 24), which compared to 2007 (we will not take 2006 and 19 cases as reference) represents an increase of 3500%. That statistical data alone clearly indicates that the solutions adopted at the beginning of the 21st century are unsustainable in 2024 and that they need to be revised. In addition, statistical data (Supreme Public Prosecutor's Office, 2024, p. 24) clearly indicate that the number of cases under the jurisdiction of the Special Prosecutor's Office, with the exception of 2016, is constantly increasing, which was regularly expressed in double-digit percentages. Therefore, the increase in the number of cases is a decades-long trend, so the workload of the Special Prosecutor's

Office is not a phenomenon that happened suddenly, but was predictable in the first three years of the Special Prosecutor's Office, and especially after 2010, when the number of cases exceeds 550 and continues to grow radically, reaching almost 6,500 cases in 2023.

The trend of a constant increase in criminal charges under the jurisdiction of the Special Prosecutor's Office significantly complicates the work of this Prosecutor's Office, that is, the Special Prosecutor's Office does not have enough capacity to successfully deal with such an influx of cases. Certainly, part of the solution lies in expanding these capacities, but a far more necessary and effective solution is to redefine the rules of application of the law *ratione materiae* and the actual competence of the judicial authorities that are in charge of prosecuting the perpetrators of these crimes. The redefinition of jurisdiction can be carried out in several directions; the first implies a significant narrowing of the range of criminal offenses handled by the Special Prosecutor's Office, which can be done either by listing the offenses handled by this Prosecutor's Office – as was done, for example, with the prosecution of criminal offenses of organized crime. This would avoid situations in which the Special Prosecutor's Office prosecutes for the criminal offense of endangering security under Article 138 of the Criminal Code. The second approach would involve foreseeing the possibility that the Special Prosecutor decides (or recommends to the Supreme Public Prosecutor) to hand over the prosecution of a specific case to another public prosecutor's office with subject matter and territorial jurisdiction, when the circumstances of the case do not require special knowledge, skills and competencies of the Special Prosecutor's Office. For example, when a threat is sent via social networks, in the sense of Article 138 of the Criminal Code, and there are no disputed facts and evidentiary actions, it would be justified for such a case to be prosecuted by the (regular) public prosecutor's office, which would have otherwise prosecuted for that crime, had it not been done via social networks.

From a realistic point of view, it is not to be expected that any reasonable legislator would provide such wide discretion to the public prosecutor to choose the cases to prosecute, which would be contrary to the principle of legal certainty. On the other hand, *a numerus clausus* enumeration of all criminal offenses that would represent *the ratione materiae* of the Law would also be unreasonable, because it would be too strictly constructed and would leave the possibility that a particular criminal offense that should fall under the jurisdiction of the Special Prosecutor's Office would not be. However, in this sense, the wording of Article 6, paragraph 2 of the Law on VTK should be retained, with certain changes, which allows the Special Prosecutor to request

from the Supreme Public Prosecutor the assignment or transfer of jurisdiction for handling a specific case. The correct balance between the two approaches – *numerus clausus* and the discretionary power of the Special Prosecutor to decide on the transfer of the case to another prosecutor's office with subject matter and territorial jurisdiction – must be found.

The Budapest Convention provides that national authorities must take legislative measures to ensure effective prosecution mechanisms for criminal offenses covered by that Convention. The legislator may have thought that by creating a special prosecutor's office for high-tech crime, he would fullfil its obligations under Budapest Convention. However, by prescribing broad subject matter jurisdiction of the Special Prosecutor's Office, concentrating territorial jurisdiction, not providing enough resources for the work of that prosecutor's office, the legislator effectively did everything contrary to the assumed international obligation. In this sense, the mechanism that is in place today for the implementation of this Convention is ineffective, so the obligation of the goal set by the provisions of the Budapest Convention has not been realized.

4. Specialization of State Bodies Competent for Prosecuting High-Tech Criminal Offenses

In addition to the legal regulation of actions aimed at discovering and proving high-tech crime, their effective and efficient application depends on knowing the technical specifics related to the facts surrounding the proceedings. Therefore, it is essential that the authorities, such as the police and prosecutor's office, possess an appropriate level of knowledge in the field of information technology. The "high-tech" aspect of criminal acts, which are directed against or are carried out using computer data, systems or networks, creates special challenges when detecting and proving them (Pisarić, 2016, p. 73). Without specialized knowledge and skills necessary for the application of appropriate technical and tactical rules, the process of investigation and proof can be significantly more difficult.

In this context, it can be considered that the formation of specialized organizational units within the police and prosecution structures is one of the key factors in effectively combating high-tech crime (Pisarić, 2016, p. 74). These units would be composed of experts who have advanced knowledge in the field of information technology and who are trained to deal with the complexity this type of crime. Their action would enable the application of specialized methods and tools in the investigation, which would improve the

ability to detect, collect and process digital evidence, as well as the monitoring and capture of perpetrators who use technology to commit criminal acts.

Also, the cooperation of these units with international organizations and experts in the field of cyber security can contribute to the development of a comprehensive approach to the fight against high-tech crime, which transcends national borders and responds to the global challenges posed by this form of crime.

In connection with the determination of the role of specialized bodies, three functions can be observed that are realized within the work of those bodies: 1. Investigation of criminal offenses committed against computer data/systems and prosecution of the perpetrators of those offenses (in the sense of Articles 2-6 of the Budapest Convention); 2. Investigation of criminal offenses committed through (use of) computer data/systems and prosecution of the perpetrators of those offenses (in terms of Articles 6-10 of the Convention); and 3. Proceeding according to technical and tactical rules in relation to computer data that are stored, processed or transmitted through computer systems/networks, and which can be evidence in criminal proceedings for all criminal offenses (Specialized cybercrime units, 2011).

Our legislator adopted a special legal solution. Namely, the Law on the Organization and Competence of State Authorities for the Fight against High-Technological Crime provided for the formation of specialized organizational units within the police, public prosecutor's office and the corresponding court responsible for dealing with high-technological crimes (Matijašević & Dragojlović, 2021).

As we have seen, the Higher Public Prosecutor's Office in Belgrade is responsible for dealing with cases of crimes that have been determined as high-tech crime for the entire territory of the Republic of Serbia (Act on VTK, 2005, Article 4, Paragraph 1), within which a special department for combating against high-tech crime (Act on VTK, 2005, Article 4, Paragraph 2).[5] The

[5] It should be pointed out at this point that it is not understandable why the special department of the Higher Public Prosecutor's Office in Belgrade is responsible for the prosecution of criminal offenses of the VTK, i.e. why, as in the case of organized crime and corruption, a special prosecutor's office was not created as an independent one, but a special department was created within the VJT in Belgrade. Although it is not a legal imperative that there be a separate prosecution office, it seems to us that no reasonable basis for differentiation can be found, which made the prosecution of VTK crimes, despite extensive jurisdiction, "special", but of a lower class compared to organized crime and corruption. A similar approach, i.e. the initiative to establish the Prosecutor's Office for High-Tech Crime, as an independent prosecutor's office, was submitted by the Special Prosecutor's Office to the Government of the Republic of Serbia (Supreme Public Prosecutor's Office, 2024, p. 30-31).

work of the Special Prosecutor's Office is managed by the Special Prosecutor for High-Tech Crime, who is appointed for a period of 6 years by the Supreme Public Prosecutor (and cannot be reappointed) from among the public prosecutors of the Higher Public Prosecutor's Office, the Appellate Public Prosecutor's Office, the Public Prosecutor's Office of Special Jurisdiction or the Supreme Public Prosecutor's Office (with the written consent of the person being appointed and the adoption of a decision on the referral of that person to the Special Prosecutor's Office), whereby priority is given to deputy public prosecutors who possess special knowledge in the field of information technology (Act on VTK, 2005, Article 5). Upon learning that a case involves cases provided for in Article 3 of the Law, the Special Prosecutor addresses the Supreme Public Prosecutor of the Republic requesting him to entrust or transfer jurisdiction (Law on VTK, 2005, Article 6, Paragraph 2).

What appears to be particularly problematic, and which contributes to the large number of cases, is the concentration of jurisdiction provided for in Article 4, paragraph 1 of the Law on VTK, which stipulates that the prosecution of high-tech crimes shall be carried out by the Special Prosecutor's Office, as a special department of the Higher Public Prosecutor's Office in Belgrade. In 2015, the then Special Prosecutor was of the opinion that such a solution was "*an adequate solution, because partial jurisdiction would lead to problems in the form of communication and data exchange between prosecutors, as well as inequality between prosecutors practices*" (quoted from Pisarić, 2016, p. 82). This approach cannot be accepted. The concentration of jurisdiction can be accepted as a transitional or temporary solution, but it is unacceptable that nowadays there is only one prosecutor's office in the entire country that is competent enough to detect and prosecute high-tech crimes. The possibility of different prosecution practice is not a sufficient basis or reason for such a strict concentration of jurisdiction, because it could serve as an argument for any other prosecution. We believe that from the aspect of relieving the work of the Special Prosecutor's Office, but also of developing the capacity of judicial authorities, it would be desirable to carry out a partial deconcentration of jurisdiction, so that special departments are formed in the higher public prosecutor's offices in Novi Sad, Kragujevac and Niš, just as it was done in the case of prosecutions for the fight against corruption.

Regardless of the above, a special problem is the fact that there are not enough human resources in the Special Prosecutor's Office – currently six prosecutors are assigned to the Special Prosecutor's Office, including the Special Prosecutor, as well as five public prosecutor's assistants. This would

mean that, in 2023, assuming that the Special Prosecutor carried the same case load as other prosecutors, each prosecutor had almost 1,300 cases.

From the aspect of professional training, it can be concluded, based on the Report of the Supreme Public Prosecutor's Office (2024, p. 32), that prosecutors and associates of the Special Prosecutor attended and visited over 20 conferences, seminars and other activities, both in the country and abroad, which certainly required additional time and effort, considering the number of cases that each of them handles. In this sense, it can be assumed that the Republic of Serbia invests and encourages professional training and further specialization of the resources it has, even though these personnel are not sufficient.

On the other hand, there is a special issue of specialization and expertise of the judicial part of the judicial authorities that are responsible for prosecuting and judging high-tech crime cases. Although the formation of a special department for the fight against high-tech crime was prescribed by an express legal provision (Law on VTK, 2005, Article 11), it ceased to exist in 2009, and it does not exist today (High Court in Belgrade, 2024, p. 3). Due to the abolition of a special department within the High Court in Belgrade, as a consequence of judicial reforms, since then high-tech crime cases have been handled by judges without the necessary IT knowledge, who do not understand the matter and who are reluctant to engage in understanding the specifics of proof acts of high-tech crime (Pisarić, 2016, p. 84). Accordingly, it would be desirable, if not imperative, to use the legal possibility to form a Special Department for high-tech crime, within which there would be enough judges with the necessary IT knowledge, both judges for preliminary proceedings and judges which would be functionally competent for conducting the main trial, in order to ensure the full application of the Law on VTK in practice.

5. Conclusion

Computers and information technologies have largely become part of the everyday life of a large number of individuals and are no longer an abstraction, and given the ubiquity of information technologies in the everyday environment, it is inevitable that the future actions of an increasing number of criminals offenses have a "high-tech" element, which means that the number of cases that would fall under the jurisdiction of specialized judicial authorities will also increase, increasing the already large number of these criminal offenses.

The fact is that the overloading of the Special Prosecutor's Office with cases with elements of high-tech crime is already evident today, and with six prosecutors and five assistants, it objectively cannot respond to such an influx of work. The biggest contribution to this problem is the concentration of subject matter and territorial jurisdiction in the hands of the Special Prosecutor's Office. As a solution to this problem, a partial deconcentration of jurisdiction from the Special Prosecutor's Office should be carried out, by creating special departments for high-tech crime in the corresponding higher public prosecutor's offices in Novi Sad, Kragujevac and Niš.

As a special question arises *ratione materiae* of the Law on VTK, i.e. whether its scope is too broad, which must be answered in the affirmative, which is certainly evidenced by the drastic number of cases in the Special Prosecutor's Office. The use of computers as a means of execution or a means of execution may have been a rarity in 2005 at the time of the adoption of the Law on VTK, but today this is not the case. Therefore, the wide network that was justifiably set up at the time is now excessive and unnecessarily burdens the work of special authorities.

From the point of view of the court, basic technical knowledge is needed in order to understand the essence of the substantive legal provisions that contain the incrimination of high-tech crime, and especially with regard to the procedural provisions that refer to the specifics of evidentiary acts that only the court can will determine (e.g. search of computers), as well as free assessments of electronic evidence that arise as a result of those actions. However, it cannot reasonably be expected that every judge of the "general" criminal department will be familiar with the peculiarities of high-tech crime, that is, the detection and prosecution of these crimes. That is why it is imperative that the domestic legal system implements (again) the provisions of the Law on VTK, which establishes a special department within the High Court in Belgrade for the fight against high-tech crime, and whose judges will be especially specialized in substantive and procedural issues related to high-tech crime.

Consequently, it would first be necessary to fully implement all 12 provisions of the Law on VTK, as it reads today. In the second place, *de lege ferenda*, the legislator should provide for the formation of special departments of judicial authorities in regional centers, and in particular to define more precisely the criminal acts that would fall under the scope of the Law on VTK, while foreseeing the possibility of the acting special prosecutor to transfer the case to the prosecution, which would otherwise, it was actually and locally competent, if there was no high-tech element of the crime, if such a crime

does not require special knowledge and competence of a special prosecutor's office.

ACKNOWLEDGEMENT

The paper is the result of the research project "*Progressive Development of Law in the Modern Digital Society*" ["*Progresivni razvoj prava u savremenom digitalnom društvu*"], funded by the Provincial Secretariat for Higher Education and Scientific Research (decision no. 142-451-3484/2023-02, dated November 21, 2023).

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

Petrović Maja
Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

OSVRT NA NADLEŽNOST I SPECIJALIZACIJU ORGANA ZA GONJENJE UČINILACA KRIVIČNIH DELA VISOKOTEHNOLOŠKOG KRIMINALA

APSTRAKT: Razvojem tehnologija, a naročito pojavom interneta i njegovom ekspanzijom u prethodne dve decenije, mnoga krivična dela (klasična krivična dela) dobila su nova sredstva i modalitete izvršenja – upotrebom računara, mobilnog telefona ili drugog uređaja. Na pojavu novih načina i sredstava izvršenja krivičnih dela međunarodna zajednica je u okvirima Saveta Evrope 2001. godine, usvojila tzv. Budimpeštansku konvenciju, naglašavajući posebno pitanja sajber kriminala. Domaći zakonodavac je nakon ratifikacije ove konvencije, doneo Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, preuzimajući pravna rešenja iz konvencije, pri čemu ovaj zakonski tekst nije značajnije menjan niti dopunjavan od

njegovog donošenja. Rešenja koja su sadržana u ovom zakonskom tekstu, a pogotovo u pogledu stvarne nadležnosti, pokazuju se kao neadekvatna i kao preširoko postavljena. Širokim obuhvatom krivičnih dela koja potpadaju pod „kišobran" ovog zakona učinili su ga relativno nedelotvornim, te su preopteretili rad tužilaštva nadležnog za gonjenje učinilaca krivičnih dela visokotehnološkog kriminala. Pored toga, pristup zakonodavca iz 2005. godine, kada je ovaj zakon donet, a koji se odnosi na potrebu i opravdanost koncentracije nadležnosti Višeg javnog tužilaštva i Višeg suda u Beogradu, u današnje vreme rasprostranjenosti tehnologije, pristupa interneta i društvenim mrežama, ne može se prihvatiti niti opravdati. Ovaj rad nastoji da pruži kraći pregled konvencije iz Budimpešte, koja je poslužila kao osnova za donošenje pozitivnih propisa u ovoj oblasti, a zatim da ukaže na manjkavost i neodrživost zakonskih rešenja koja je domaći zakonodavac predvideo kada je 2005. godine, donosio nacionalne propise iz ove oblasti.

Ključne reči: *visokotehnološki kriminal, krivično pravo, nadležnost, specijalizacija.*

References

1. Dragojlović J., & Krstinić D. (2015). Evropski standardi u borbi protiv visokotehnološkog kriminaliteta i njihova implementacija u zakonodavstvu Republike Srbije [European standards in combat against high-tech criminality and theirs implementation in legislation Republic Serbia]. *Evropsko zakonodavstvo*, *14*(51), pp. 92–103
2. Dragojlović, J. (2023). Jurisdiction for criminal offenses of cybercrime – international and national standards. *Pravo – teorija i praksa*, *40*(1), pp. 63–83. DOI: 10.5937/ptp2300063D
3. Konvencija Saveta Evrope o visokotehnološkom kriminalu br. 185 [Convention on Cybercrime CETS No. 185]. 23. 11. 2001.
4. 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
5. 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
6. Pavlović, M. (2022). *Borba protiv visokotehnološkog kriminala u Srbiji – dostignuća i izazovi* [*Fight against Cybercrime in Serbia – achievements and challenges*]. Beograd: Beogradski centar za bezbednosnu politiku

7. Pisarić, M. (2016). *Posebnosti dokazivanja dela visokotehnološkog kriminala – doktorska disertacija* [*Specifities of proving Cyber Crime – doctoral thesis*]. Beograd: Pravni fakultet
8. Report and Guidance on Privacy in Social Network Services – "Rome Memorandum" – 43rd meeting, 3-4 March 2008, Rome (Italy). Downloaded 2024, September 8 from https://www.gpdp.it/documents/10160/10704/1531476
9. Specialised cybercrime units – Good practice study. 2011, p. 4. Downloaded 2024 September 10 from https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33
10. Vidić V. (2016). *Povreda prava na privatnost zloupotrebom društvenih mreža kao oblik kompjuterskog kriminaliteta – doktorska disertacija* [*An injury rights on privacy abuse social network like shape computer of criminality – doctoral thesis*]. Niš: Pravni fakultet Univerziteta u Nišu
11. Viši sud u Beogradu. (2024). *Informator o radu za 2023. godinu* [*Work Informant for 2023*]. Beograd: Downloaded 2024, September 10 from https://www.bg.vi.sud.rs/sekcija/95/informator-o-radu.php
12. Vrhovno javno tužilaštvo (2024). *Rad javnih tužilaštava na suzbijanju kriminaliteta i zaštitu ustavnosti i zakonitosti u 2023. godini* [*Work of Public Prosecutor Offices on combating crime and protection of constitutionality and legality in 2023*]. Beograd. Downloaded 2024, September 8 from http://www.parlament.gov.rs/upload/archive/files/cir/pdf/izvestaji/14_saziv/Izvestaj%20o%20radu%20javnih%20tuzilastava%202023.pdf
13. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala [*Law on Organization and Competencies State Organs for fight against High-Tech Crime*]. *Službeni glasnik RS*, br. 61/05, 104/09 i 10/23
14. Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu [*Law on Confirmation of Convention on Cybercrime*]. *Službeni glasnik RS,* br. 19/09