Srećković Jovan[*]

UDK: 343.222.2:004.738.5
Review article
DOI: 10.5937/ptp2303115S
Received: 09.06.2023.
Approved on: 11.09.2023.
Pages: 115–133

INTERNET FRAUD

ABSTRACT: Internet law represents one of the youngest branches of law, which emerged from the need to expand the existing and create a new regulatory framework that would regulate the internet and introduce the necessary legal security and protection for its users. Internet Law or Cyber Law is largely intertwined with the Law on Information and Communication Technology, as a legal field which encompasses the regulation of contractual relations established by means of information technology, the right to privacy and data protection, freedom of speech and intellectual property, internet security, copyright on computer program codes and databases, criminal offenses arising from actions on the internet, as well as the tax aspects of online goods and services exchange. In contrast to the broader scope of IT law, Internet law refers to a narrower segment of this legal field related to the internet, regulation of internet management at all levels, management of internet domain names and IP addresses, etc. Internet law (or Cyber law), in a broader sense, encompasses those parts of the legal system and legal domains that are related to the internet and provide protection to its users. To address the issue of domain name registrant liability and determining their identity, it is necessary first to explain the governance structure of the internet and the informational and legal nature of internet domains. Although the internet is often said to be free and belonging to everyone, this complex system does not operate entirely on its own, which means that it is not perfect to the extent that its structure is fully automated.

[*] LLM, PhD student at the Faculty of Law for Commerce and Judiciary in Novi Sad, University Business Academy in Novi Sad, Serbia, e-mail: jovansreckovic.js@gmail.com

Addressing the topic of internet fraud and educating colleagues and the general public are aimed at preventing fraud. The lack of awareness about how internet scams operate continually leads to new victims, and insufficient knowledge of legal provisions and potential penalties can create potential perpetrators of this crime. When complex topics are explained in simple terms, it represents a significant step in educating individuals, both in the legal and technological aspects from a legal perspective.
Such academic work should not deter people from using the Internet, nor should it present an obstacle to progress and the digitization of difficult and time-consuming paperwork obligations. Instead, the objective is to timely educate individuals so that the utilization of the digital world can be integrated into all segments of society as quickly as possible. This will facilitate the functioning of daily life, including business operations, while still remaining within the bounds of legal regulations. Therefore, it is extremely important to educate people on how to avoid internet fraud.

Keywords: *Internet law, criminal acts, privacy, data protection, internet fraud.*

1. Introductory remarks

The management of the Internet today represents a complex structure and processes, which to some extent dictate the regulation and policies concerning the Internet (Milić & Đukić, 2022, p. 215). Given the sensitive relationship between Internet service providers and users, the right to privacy, collection of personal data (including trading and misuse of the same), protection of payment card and bank account data, represent one of the biggest problems facing network users today. Therefore, the companies that collect the mentioned data are expected to do everything in order to prevent hacking attacks and other illegal activities. The other side of the coin is the legal activities of providers, social networks and platforms that collect personal data, and which, with the formal consent of users, use the same for the purpose of gaining profit and increasing the value of their own companies. Monitoring of user activities by official governments and state institutions is a special problem that threatens both the neutrality of the Internet in general and the privacy and personal interests of individual users (Popović, Budimlić & Puharić, 2009. p. 9).

Internet security, the protection of intellectual property and copyright rights online and the ease with which they can be violated in the online sphere are also very widespread problems for which there is no 100% protection, but

through legal regulation, attempts are made to establish the greatest possible degree of legal security and unhindered use of the Internet. One of the important areas covered by Internet law is the criminal law protection of legal and natural persons who use the network for primary or business purposes. In addition to the repressive effect by prescribing the type and degree of sanctions for the execution of certain legally prescribed acts, internet law also deals with the study of network weaknesses and its improvement, which significantly contributes to the prevention of criminal acts in cyberspace. In almost every developed country in the world, special, well-trained and equipped departments within the police and prosecutor's offices have been established to solve these cases. Although it is up to the state authorities to provide protection to Internet users, a lot can be prevented by informing citizens, ie employees in companies, about all important aspects of protection and preventive action. That is why it is important to be informed regularly, because technology is developing rapidly, so those who use it to commit criminal acts improve and upgrade it just as quickly. These types of crimes have the highest growth rate in the world. The global network enables cross-border action, so these problems are no longer part of national legislation, but a problem of the whole world, the solution of which must be coordinated and united. The current Criminal Code of the Republic of Serbia, the section that regulates criminal offenses committed on the Internet or in connection with high technologies, is called Criminal offenses against the security of computer programs in the Republic of Serbia. Thus, the offense of Damage to computer data and programs is provided, for which, depending on the amount of damage caused, a prison sentence of up to 5 years can be imposed. Also, the same is prescribed for entering, destroying, changing or concealing software or digital records, as well as hardware information carriers that prevent their use, i.e. significantly hinder the transfer or processing of data that serve state bodies or other institutions (committing the criminal act of computer sabotage) the amount of the fine. For the production and introduction of a virus into someone else's computer or computer system, the penalty can be up to 2 years in prison, depending on whether it caused damage.

According to the Criminal Code of the RS, the traditional act of Fraud has also acquired its own special form if it was committed on the Internet or in connection with computer data. Due to the degree of importance of protection on the Internet against fraud, the legislator prescribed a penalty of up to 10 years in prison for frauds that cause damage of over 1,500,000 RSD.

For unauthorized access to a protected computer, computer network and electronic data processing, a penalty of 6 months is prescribed, and if the

information thus obtained is used, the penalty can reach 2 years in prison, while if serious consequences occur, 3 years. The law also prohibits the actions of preventing or limiting access to a public computer network, i.e. the use of someone else's computer or network.

2. The concept of Internet fraud

By their nature, internet fraud is the closest to economic crime, and in the literature, almost without exception, these phenomena are treated as a form of economic crime.Internet fraud involves the use of online services and software with Internet access to defraud or exploit victims (Bjelajac & Filipović, 2021). The term internet fraud generally covers cyber crimes that occur over the Internet or via e-mail, including crimes such as identity theft, phishing, and other hacking activities designed to steal money from people. Internet scams that target victims through online services represent millions of dollars in fraudulent activity each year. And the numbers continue to grow as Internet usage increases and cybercriminal techniques become more sophisticated.

Internet fraud is a type of cyber fraud or fraud that uses the Internet and involves concealing information or providing false information in order to defraud victims of money, property and inheritance. Internet fraud is not considered a single, independent crime, but includes a series of illegal and illegal actions committed in cyberspace, but it differs from theft because in this case the victim voluntarily and knowingly gives information, money or property to the perpetrator. Another characteristic is that the perpetrators are separated in time and space.

Today's computer technology can be misused in many ways. One of the forms of abuse of information technology is fraud through the Internet. It represents the most widespread form of computer crime and is predominantly of a monetary nature (acquiring illegal material benefits). A special form of Internet fraud is the "Ponzi scheme" – a method of committing a criminal offense of fraud with the help of computers and the Internet. It usually starts with false promises, which seem like a fairy tale, offers enrichment "overnight", there are also certain indispensable conditions, such as investing money at the very beginning and involving more people, etc. The issue of misuse of information technology is not only a legal issue. Since this is a problem that causes large financial losses, it is necessary to consider the economic impact on economic flows in each country (Bjelajac, 2011).

In relation to traditional forms, cyber crime is rapidly changing its forms and forms of expression, borders between countries, and the type of victim.

These acts are usually difficult to detect, even more difficult to prove, and remain undetected for a long time because the injured party does not have to suffer damage that is immediately visible. Thanks to the constant development of technology, new and more complex forms of cybercrime appear every day. New, more subtle and significantly more dangerous forms of criminal behavior are emerging, hitherto unknown to criminal practice (Bošković & Marković, 2015. p. 297). The perpetrator can attack a specific computer or network from anywhere, regardless of where it is located, so space and time frame have little significance in most cybercrime acts. Criminal acts are committed in the information environment, i.e. faster and easier and in more diverse ways and most importantly mostly anonymously, because today more than ever the network provides ideal conditions for perpetrators to cover up their criminal acts. Only a small number of committed criminal acts are reported and investigated. When financial institutions, banks and business entities come forward as victims, the reason for not reporting is the fear of losing the trust of their business partners. Also, in the event of an attack being published, clients are afraid that their data is not in safe hands and are looking for new business partners. A small number of injured persons are aware that they have been a victim of a criminal act, in most cases even if a report is made it is too late to take any appropriate measures.

Computer embezzlement is difficult to detect, because control is often complicated and evidence is hard to come by. The main characteristic of this part is the acquisition of illegal property benefits by appropriating values from the one to whom these values are entrusted. As information technology when it comes to the economy was first introduced in financial institutions, the first abuses were committed in banks, but in large business systems with several thousand employees. Computers and information technology were used in embezzlements in which: falsification of accounting documents, issuance of fictitious invoices, issuance of fictitious travel orders; creation of fictitious payrolls, creation of fictitious inventory list, creation of fictitious customers, artificial increase in stock of goods, inaccurate presentation of losses on goods, falsification of credit reports, creation of false financial data, etc. cases.

2.1. The concept of "Ponzi Schemes"

Charles Ponzi was born Carlo Pietro Giovanni Guglielmo Tebaldo Ponzi on March 3, 1882, in Lugo, northern Italy. They say that Ponzi showed criminal tendencies early on, stealing from his parents and even the parish priest. Although few people outside of financial circles know who Charles

Ponzi was, most can guess what he is known for, given his last name. The term "Ponzi scheme" is known as an investment scam in which money from a steady stream of new investors is used to pay off earlier investors while simultaneously enriching the scheme creator.

The scheme or scam continues until, as it always does, it collapses when there are no more new investors. Although Ponzi was not the first to use this scam to make money, he is the most famous and therefore the one it is named after. In 1920, Ponzi organized a company called the Securities Exchange Co. in which he sold shares advertising 50% interest after 90 days. Funds received from investors were to be used to purchase an international coupon for redemption in the US. Instead, Ponzi used funds received from new investors to pay off old investors.

Soon, many people heard about his teachings and learned his art of deception. A new financial fraud was born, called "Ponzi scheme". The "Ponzi Scheme" flourished with the advent of the Internet, everyone is networked, there is no excessive protection, it is easy to get in touch with ignorant people, and also all data is poorly protected. In a word, a utopia for fraudsters, as well as for the most famous "Ponzi scheme".

2.2. The concept of "pyramid schemes"

Pyramid schemes are so named because their compensatory structures resemble a pyramid. The scheme starts with a single point at the top where there are original members and becomes progressively wider towards the bottom as people are recruited by all levels of recruits.

A pyramid scheme is an unsustainable business model that involves making money primarily by involving other people in the scheme, usually without any product being sold or any service performed. This type of scam comes in many variations.Typically, pyramid schemes recruit members at seminars, home meetings, by phone, email, mail, or social networks. In a typical pyramid scheme, you have to pay to join. The basis of the scheme is to convince people to join and also participate with their money. In order for everyone in the scheme to make money, there must be an infinite number of new members. In reality, the number of people who are willing to join the scheme, and therefore, the infinite amount of money that goes into the scheme, which quickly disappears. Some pyramid scheme promoters pretend that their real intention is to introduce products that are overpriced, or of poor quality, difficult to sell, or of lesser value. Making money by employing people is his main goal. Promoters at the top of the pyramid make money by getting people

to join the scheme. They charge fees and other charges to other people who are subordinate to them. When the scheme fails, relationships, friendships, and even marriages can be destroyed because of the money lost in the scam. It is illegal to promote or participate in a pyramid scheme.

In a variation of a pyramid scheme, investors at each level charge start-up fees that are paid by the next layer of investors. Part of this compensation is paid to those in the upper layers of the pyramid. In the end, no one stays to recruit. The pyramid is collapsing.

2.3. The legal nature of "Ponzi" and "Pyramid" schemes

What is the difference between a "Ponzi Scheme" and a "Pyramid Scheme"?

A Ponzi scheme is a mechanism to attract investors with the promise of future returns. The operator of a "Ponzi scheme" can only maintain the scheme as long as new investors are attracted. On the other hand, the "Pyramid Scheme" recruits other people and encourages them to further bring in other investors. A member in a "Pyramid Scheme" earns only a portion of his income and is "used" to generate profits by members higher up the pyramid.

The essential difference between these two scams is that a "Ponzi scheme" generally only involves investing in something from its victims, with a promised return at a later payout date. "Pyramid schemes", unlike "Ponzi schemes", usually offer the victim the opportunity to "make" money by recruiting more people into the scam. What they have in common is that both fraud schemes operate 90 percent over the Internet these days.

Consider a very simple example where Person A promises a 10% return to Person B. Person B gives person A 1,000 euros with the expectation that the value of the investment will be 1,100 euros in one year. Then, Person A promises a 10% return to Person C. Person C agrees to give Person A 2,000 euros. With €3,000 now available, Person A can raise Person B by paying him €1,100. In addition, person A can steal €1,000 from the collective fund if he believes he can get future investors to give him money. In order for this plan to succeed, person A must constantly receive money from new clients in order to pay back older ones.1 Another example: "Entrepreneur" announces that he is working on a very profitable business that guarantees high income and profits, but he needs a loan, i.e. cash Money. "Investor" A gives "Entrepreneur" a loan of $1,000 with a 90-day repayment term and $100 interest payable on the 90th day. During those 90 days, the "Entrepreneur" finds new "Investors" B and C promising them the same. At the end of the period, he offers the "Investor" to return the 1000 dollars and the interest of 100, but also not to raise the principal

and the interest, offering again the same excellent conditions. He owns the money for that purpose because he also received funds from "Investors" B and C. Most of the "Investors" take it slow and do not withdraw money, i.e. reinvests. Individuals who do not believe are paid on the spot, from the money he received from others, and this raises the "rating" of the "Entrepreneur" as a business and serious person. The number of "Investors" is increasing. This operation lasts for a while and ends with the "Entrepreneur" running away with the money or announcing payment problems or bankruptcy, because there was a disruption in the "market" from which he had a large income. The most common way of "fishing" gullible people and victims is carried out through phantom companies. Its characteristics are a very well-arranged website with several presentations, but the deeper it is investigated, the more often it comes to the fact that the company has registered headquarters in a virtual office, no employees, fake pictures of employees, fake business partners, zero completed and closed deals. It is mostly about very sweet-talking and sharp-witted people who are ready to "sell" any story without any compassion, usually the one that the "victim" wants to hear, and it all sounds too good to be true.

Internet fraud in Serbia, as well as in the world, can be characterized as a form of organized crime, according to the facts that all conditions are met. The characteristics of organized crime are significant when defining organized crime. Precisely in relation to the primary elements (characteristics) of organized crime, two understandings are dominant: according to the first understanding, when defining organized crime, the primary element is the criminal organization, i.e. the structure of the criminal group, while according to the second understanding, the type of criminal activity is decisive for the existence of organized crime, undertaken by a criminal group (Bjelajac, 2013, p. 53).

One of the problems in Serbia is that there is not a sufficiently developed system of combating internet fraud and fraud generally done digitally. This is regulated by Article 208, paragraph 1 of the Criminal Code of Serbia, which reads: "Whoever, with the intention of obtaining an illegal property benefit for himself or another, misleads someone by falsely presenting or concealing facts or keeps him in a delusion and thereby leads him to harm himself or others property, does or does not do something, will be punished with imprisonment from six months to five years and a fine."[1]

[1] The perpetrator causes a person to make a decision to do or not do something. This can be done by doing, not doing, and even by conclusive actions. If the crime was committed against a spouse, relative, adoptive parent or adoptee or other persons with whom the perpetrator lives in a common household, criminal prosecution is undertaken by private criminal action (Features of the criminal offense of fraud, Dragan Jovašević, selection of court practice, no. 7/96, p. 12).

Given that internet fraud is carried out via high-tech devices, the department for high-tech crime carries out work and tasks under the jurisdiction of the Republic Public Prosecutor's Office in connection with criminal acts of high-tech crime, fulfilling the obligations assumed by the Law on the Ratification of the Convention on High-tech Crime, coordinating work with special by the department of the Higher Public Prosecutor's Office in Belgrade for high-tech crime, as well as the coordination of work with the prosecution offices of general jurisdiction, in connection with criminal acts of high-tech crime.

2.4. "Nigerian Scam"

One of the most well-known forms of fraud via the Internet is the *Nigerian fraud* and it belongs to the group of frauds that are carried out by investing a certain amount of money by the defrauded person in certain businesses, of course with the fraudster's previous promise that a significantly higher monetary profit will be achieved. This type of fraud appeared for the first time in the 1980s and was associated with the rapid economic growth of Nigeria. Frauds were mainly carried out by sending business offers to foreigners for trade or exploitation of oil, thanks to which Nigeria has become economically stronger. Frauds were carried out by sending fake messages via computer or e-mail, about alleged winnings on games of chance, and by sending messages related to humanitarian contributions, messages related to "love and business offers", inheritance of property, usually some unknown relative. carried out by initially selecting the victim and later persuading her by social engineering methods to pay a certain amount of money in advance. That amount of money is in most cases incomparably smaller than the amount they should receive as a benefit from a fund, that is, from the sender of the message. By e-mail, the recipient was asked for help in order to obtain large sums of money, from a few hundred thousand to a few tens of millions dollars, and upon payment he would receive a certain percentage of the promised earnings. According to the citizens of Serbia who were victims of this form of fraud, the action of execution was carried out in several ways: by sending notifications about false winnings of games of chance, after which the victims paid certain sums of money to enable them to withdraw the prize, as well as by sending notifications about inheritance using who are victims of fraud using social engineering methods led to believe that they have inherited a certain amount of money, after which they pay certain sums of money to enable them to pay out the inherited money (Urošević, 2009, pp. 145-156).

3. Organized crime, Cyber crime and White collar crime relations

As legitimate business also implies a certain organization and exhibits features of institutionalization, the question arises what is the difference between "white collar" crime, more precisely, its subtype of corporate crime and organized crime. Edwin Sutherland believes that this difference actually does not exist. way, is joined by Larry Siegel, who classifies both of these types of crimes in the same group, where he sees the only difference in the fact that "white collar" crime is about the illegal activity of individuals and institutions that entered the business in order to make a profit legitimate business, while organized crime as well as legitimate business implies a certain organization and exhibits features of institutionalization, the question arises what is the difference between "white collar" crime, more precisely, its subtype of corporate crime and organized crime. Edwin Sutherland believes that these differences actually do not exist In a way, he is joined by Larry Siegel, who classifies both of these types of crimes in the same group, whereby he sees the only difference in the fact that "white collar" crime is about the illegal activity of individuals and institutions that are in entered the business in order to gain profit through legitimate business, while organized crime involves illegal activities of subjects whose goal from the beginning was profit obtained in an illegitimate way. Their common point is, among other things, the effort to violate the principles of free market operations. Thinking similarly, Mark Ђaler subsumes both of these types of crime under the category of "illegal business activities" as a common name for the sale of illegal goods and services to customers who know that these goods and services are illegal. The aforementioned Edwin Sutherland once emphasized that "financial the damage caused by "white-collar" crime, although huge, is still less important than the damage done to social relations and social morals" (Bjelajac, 2013, p. 51). Unlike conventional crime, which has an insignificant effect on social institutions, as some authors point out this form crime strengthens social disorganization, and its perpetrators, respected members of society, are very rarely prosecuted due to the de facto immunity they enjoy as respected businessmen. In most cases, frauds on the Internet are well organized by several people, which indicates to us that it is an organized crime. The bridge that connects "white-collar" crime and cyber crime (in this case fraud via the Internet) is exactly organized crime. When we talk about the definition of cyber crime, for now there is no generally accepted definition, nor is there agreement on whether "cybercrime" is a new type or just a new

form of execution of an already existing crime (Bošković & Marković, 2015, p. 296).

In 2001, the EU Commission defined cyber crime in the broadest possible sense, so that cyber crime means any criminal offense that in any way involves the use of information technology. At the XI Congress of Crime Prevention and Criminal Justice held in Bangkok in 2005, the Working Group of the United Nations defined cyber crime as a general term that includes criminal acts committed using a computer system or network, in a computer system or network, or against a computer system. or networks. Professor Vidoje Spasić presents computer (cyber) crime as crime committed in a digital environment and represents a specific form of illegal behavior in which computer networks appear as a means, goal or evidence of the commission of a criminal act (Spasić, 2006, p. 107; Vidojković, 2015, p. 4).

Although there is no single definition, what everyone agrees on is that cyber crime is criminality that is specific in terms of its structure, scope, and peculiarities, and that everywhere in the world it records progressive growth and the appearance of new criminal acts (Bošković & Marković, 2015, p.295).

The main characteristics of *white-collar* crime are the following: a) it is committed by persons with a prestigious social status within the profession they perform, and a white-collar criminal is any person with a high socio-economic status who violates the laws that determine their professional activity; b) appears in activities related to bank insurance, trade, railways, state institutions, inspection or tax services, police and customs services, medicine; includes fraud in business operations, stock exchanges, suspicious transactions arranged by illegal trades, transactions in currency and bills of exchange, fake accounts, insurance fraud, malfeasance related to tax evasion, corruption; c) social power and reputation and privileges are used to acquire enormous material goods, and enormous damage is caused to society (measured in tens of billions of dollars per year in developed countries) (Bjelajac, 2013, p. 50). What is most dangerous about this form of crime is that it leads to both large material losses, as well as damage to the health, injuries, and even death of a large number of people, (Ignjatović, 1996, p. 207), since in addition to fraud with prices, false presentation of income, money laundering and multinational and bribery, training and violation of quality and health regulations, environmental regulations, etc. The "de facto" abolition of arrest and criminal prosecution is relatively high, not only due to the lack of awareness of the degree of social danger of this act ("useful embezzlement"), but much more due to the fact that the perpetrators are "reputable businessmen" with high corruption potential. However, this sends

signals from the social elite themselves that malfeasance is justified and useful. Because the types of "cybercrime" can be: computer fraud, computer sabotage, computer terrorism, computer vandalism, piracy, all via the Internet, of which financial fraud is the most common. For all the mentioned criminal actions, it is necessary that persons are educated in that field, highly informed, socially trained for such a thing, as well as with previous experience. We conclude that the connection between "cyber crime" and "white collar" crime is not only in criminal liability, but in those specific characteristics that the perpetrators of these crimes possess and share with each other.

When we compare the profiles of the perpetrators of *white-collar* crimes and the current profiles of the perpetrators of "cyber crime", we get a synergy of character traits. Given that the Internet has not always existed, we can only assume whether "white-collar" crime would be effective for the first time through the Internet. In all of the above, and looking from the perspective of criminal responsibility, the methods of "catching" criminals, as well as the type of protection of potential victims, we can freely say that any financial fraud in the real world shares operational tools and principles as well as Internet fraud, the so-called cyber crime.Criminal groups are increasingly turning to the use of various aspects of high technology, primarily in order to facilitate criminal activities, but also to create new types of illegal activities that represent a symbiosis of "classic" organized crime and high-tech crime (Komlen-Nikolić, Gvozdenović, Radulović, Milosavljević, Jeković, Živković, Živanović, Reljanović & Aleksić, 2010, p. 183).

Is it possible for criminal association of individuals or groups in virtual space? Yes, but not in the way that individuals would probably imagine it. In the simplest terms, when an individual has a "quality" idea on how to pull off a particular scam, but lacks the financial means or equipment, or simply wants to reduce the risk of getting caught by 50%, they will team up with another individual. What is special about such an "organization" is that its members never have to see each other, nor know the identity, appearance or any private information of other persons with whom they are connected in this way.

4. The legal nature of Internet fraud

"Cybercrime" and everything that falls under it (financial fraud, etc.) is an international problem and there are several international documents that provide for the sanctioning of such crimes by states and somehow classify certain forms of "cybercrime". In this regard, the Recommendation of the Council of Europe from 1989 and the Convention of the Council of Europe

on cyber crime from 2001, which entered into force in 2004, Serbia ratified and implemented through our legal system in 2009, are significant. An additional protocol to the Convention was adopted by the Council of Europe in Strasbourg on January 28, 2003, and it refers to the prosecution of acts of a racist and xenophobic nature committed with the help of computers, i.e. it regulates behavior related to the spread of hatred, bigotry, intolerance through computer systems towards racial, religious , national groups and communities. The convention on cyber crime consists of four chapters that define basic terms, determine legislative measures, prescribe international cooperation and, finally, allow the possibility of protecting new elements. In this way, each country is able to identify the nature of the criminal offense and the way in which it is recorded or defined in its legal system (Convention on High-Technological Crime, Budapest, 2001).

It should be noted that the Council of Europe recognized various forms of computer abuse in 1976, but nine years passed from the recognition of the problem to the initiation of the initiative, and another eleven years passed until this law was enacted.

At the level of the European Union, there are several other documents that deal with this issue, the most important of which is the "Framework Decision on Attacks on Information Systems" from 2005. All these documents aim to reduce the disparity between national laws, introduce new powers in discovery and proof cyber crime and the improvement of international cooperation in the fight against high-tech crime.

Although in today's society it is impossible to function completely without the use of computers and modern technology, in addition to useful use, it can also be used for illegal, unlawful purposes, primarily for the acquisition of illicit material benefits. In addition to the conclusion that it is necessary to adopt appropriate material and procedural laws that contain measures in accordance with the Convention on High-tech Crime, and in accordance with the capabilities of each country, it is necessary to emphasize the fact that a greater level of attention from the scientific and professional public is needed, at least in the segment necessary to adequately appreciate the characteristics of misuse of information technology. The issue of Internet abuse, especially when it comes to phenomena involving various types of fraudulent manipulation of computer elements, is not only a legal issue.

All significant forms of computer crime are defined in our law as criminal offenses covered by paragraph (XXVII) of the Criminal Code of the

RS – Criminal offenses against the security of computer data.[2] It should be emphasized that in addition to criminal acts directed against the security of computer technology, there are a large number of traditional criminal acts that are carried out faster and easier with the help of the Internet, the perpetrators are more difficult to track down, and the consequences are far more serious and greater (Kojić, 2015, p. 472).

Some crimes are very difficult to prove. Specific knowledge is required for its discovery, as well as the collection of evidence. Internet frauds are also included in such crimes, which are very dangerous, given that they represent in most cases a form of financial fraud.4 Given that computer crimes are committed in a specific environment, called cybernetic or cyber space, this entails a multitude of new and interesting implication. Therefore, bearing in mind this important characteristic of computer crime, "the fact that it is carried out in the information environment, gives it certain specificities that are reflected in the fact that crime in the information environment is carried out easier, faster, more diverse, more extensive and, as is particularly significant from the point of view of criminals, more anonymous (Petrović, 2004, p. 6). Advantages that lead to the spread of Internet (cyber) crime can be: 1. Sophisticated technology that makes detection difficult; 2. Incompetence of the investigator; 3. Victims do not use safety tips and often do not feel threatened by such actions.

A special problem in this area is the collection of evidence related to the perpetrators of such crimes. The problem is that the communication and organization of the group takes place virtually and there are no procedural provisions that would regulate such a situation. In fact, the positive legal procedural legislation in our country does not recognize the peculiarities of internet abuse and, in this sense, does not contain adequate procedural norms.

[2] High-tech crime includes a set of criminal offenses against the security of computer data:Damage to computer data and programs; Computer sabotage; Creation and introduction of computer viruses; Computer fraud; Unauthorized access to a protected computer, computer network and electronic data processing; Preventing and limiting access to a public computer network and Unauthorized use of a computer or computer network.In addition to the above-mentioned crimes, this area also includes crimes against intellectual property, property and legal traffic, where computers, computer networks, computer data, as well as their products in material or electronic form appear as the object or means of committing crimes. In accordance with this legal definition, the area of high-tech crime also includes crimes where computers and computer networks appear as a means of committing criminal acts of fraud, abuse of payment cards on the Internet, abuse in the field of electronic commerce and banking, abuse of children for pornographic purposes on the Internet (so-called child pornography), hate speech on the Internet (spreading national, racial, religious hatred and intolerance, etc.).

5. Concluding considerations

In order to achieve the most adequate protection and the most effective mechanism for combating crime via the Internet, we should start by improving the legal regulations. In the legal text, the most complete criminal procedural system of reaction to this form of crime must be built. High-tech crime as a transnational social phenomenon calls into question basic values in the largest number of modern countries, which is why it is crucial to create a protection system in accordance with internationally accepted standards that have yielded positive results in practice. In this context, the key thing is the exchange of information between entities fighting crime at the international level, the collection and exchange of evidence, as well as the implementation of joint investigations by law enforcement agencies of different countries. The legislation of the Republic of Serbia very well regulates computer crime and generally financial fraud via the Internet in the material part of the criminal law matter, because it is harmonized to a significant extent with international standards. However, serious investments are needed in personnel, i.e. in persons who are authorized to act in these cases. There is a need for permanent education and training in accordance with world trends in the fight against Internet crime, as well as raising the level of information literacy of these persons, all with the aim of their more efficient work.

Not all legal systems have the same level of protection, ie. they do not have the same approach to the concept of privacy, which can range from a subjective right, the realization of which is a personal matter of the individual, to a category that elevates personal data and the right to protection of the same to the level of basic human rights, as proclaimed by EU regulations. Our legislation followed the same path by passing the Personal Data Protection Law of the RS[3], which began to be implemented in August 2019, and which was written according to the model and in accordance with the General Data Protection Regulation

[3] This law regulates the right to the protection of natural persons in connection with the processing of personal data and the free flow of such data, the principles of processing, the rights of persons to whom the data refer, the obligations of handlers and processors of personal data, the code of conduct, the transfer of personal data to others states and international organizations, supervision over the implementation of this law, legal remedies, liability and penalties in case of violation of the rights of natural persons in connection with the processing of personal data, as well as special cases of processing. This law also regulates the right to the protection of natural persons in connection with the processing of personal data by competent authorities for the purposes of preventing, investigating and detecting criminal offenses, prosecuting perpetrators of criminal offenses or enforcing criminal sanctions, including preventing and protecting against threats to public and national security. , as well as the free flow of such data.

"GDPR". In this regard, our legislation is in step with European regulations, with the aim of harmonizing personal data protection mechanisms on a global level, as a particularly sensitive and important category of data, which actually represent the private, personal sphere of each individual.

Are there frauds with illegal acquisition of property benefits over the Internet, are they theft and abuse? of personal data over the Internet, is it simply an unwanted form of communication over the Internet, what is very important and serious for our country and our people, as well as for global civilization, is that the Internet sky extends over the entire planet, but there are very few pillars of support that give security to the inhabitants of the planet. Insufficient control, insufficient legal regulations, insufficient amount of will to improve and deal with the Internet and its security. Of course, we must never leave reality, in the end everything happens in the material world, but the digital world, which is full of fraud and all kinds of criminal acts, needs to be arranged, as well as the material world, so that we do not run away from the material world into the digital one, and at the same time, from the digital to the material, because as the years go by, the digital world will be increasingly represented. The digital world without fraud and other criminal acts will be a legally and ethically regulated environment for the functioning of business and legal activities. Prevention is first of all necessary and most important, and probably the most effective. The step we should have already taken is education or recruitment of personnel for this form of crime. The creation of international cooperation at the highest level in the prevention and fight against cyber crime is also of key importance, because cyber crime, first of all, knows no borders.

This study aimed to explore the prevalence and underlying factors of internet fraud, shedding light on its impact on individuals and society. Through an extensive analysis of real-life cases and in-depth interviews with victims, to uncover significant findings that contribute to understanding of this complex issue. The point was to reveal a disturbingly high prevalence of internet fraud across various online platforms, with a particular emphasis on identity theft, phishing scams, and online investment fraud. Additionally, to identifify several key factors that increase individuals' vulnerability to fraud, such as lack of digital literacy, overconfidence in online security, and susceptibility to social engineering tactics. The implications of these findings and statements are far-reaching. Law enforcement agencies can leverage this insights to enhance their investigative techniques and develop targeted strategies to combat internet fraud. Financial institutions can employ from these to strengthen their fraud detection systems and educate customers about

potential risks. Moreover, the point of this topic and research was to highlight the urgent need for comprehensive educational programs to empower individuals with the knowledge and skills necessary to protect themselves online. Additionally, incorporating more qualitative methods, such as focus groups or observational studies, could provide a deeper understanding of the psychological and behavioral aspects of internet fraud victimization. Looking ahead, future research should explore emerging forms of internet fraud, such as cryptocurrency scams or deepfake-based fraud, as technological advancements continue to evolve. Additionally, collaborative efforts between researchers, law enforcement agencies, and industry stakeholders are essential to stay ahead of fraudsters and develop proactive measures.

In conclusion, this study underscores the urgent need to address internet fraud, which poses significant threats to individuals, organizations, and society at large. By leveraging these findings, policymakers, law enforcement, and cybersecurity experts can work together to develop effective preventive measures, raise awareness, and mitigate the devastating impact of internet fraud. Only through a multidisciplinary approach can we create a safer digital environment for everyone.

Srećković Jovan
Pravni fakultet za privredu i pravosuđe u Novom Sadu, Univerzitet Privredna akademija u Novom Sadu, Srbija

INTERNET PREVARE

REZIME: Internet pravo predstavlja jednu od najmlađih grana prava, nastalu iz potrebe proširenja postojećeg i stvaranja novog regulatornog okvira koji bi regulisao internet i uveo neophodnu pravnu sigurnost i sigurnost njegovih korisnika. Internet pravo ili sajber pravo je u velikoj meri isprepleteno sa Zakonom o informacionim tehnologijama i komunikacionim tehnologijama, čija pravna oblast obuhvata uređenje ugovornih odnosa uspostavljenih sredstvima informacionih tehnologija, pravo na privatnost i zaštitu podataka, slobodu govora i intelektualne svojine, internet bezbednost, autorska prava na šifre kompjuterskih programa i baza podataka, krivična dela proistekla iz radnji na internetu, kao i poreski aspekt razmene dobara i usluga onlajn. Za razliku od šireg

obima IT prava, internet pravo podrazumeva uži deo ove pravne oblasti koji se odnosi na internet, regulisanje upravljanja internetom na svim nivoima, upravljanje nazivima internet domena i IP adresama itd.

Internet pravo (ili sajber pravo) kako se još naziva, u širem smislu, obuhvata one delove pravnog sistema i pravne oblasti koje su vezane za internet i pruža zaštitu korisnicima interneta. Da bi se pristupilo problemu odgovornosti registranta imena internet domena i utvrđivanja njegovog identiteta, potrebno je prvo objasniti upravljačku strukturu interneta, odnosno informatičku i pravnu prirodu internet domena, ime se mora razumeti. Iako se za internet često kaže da je besplatan i da pripada svima, ovaj složeni sistem ne funkcioniše sam po sebi, odnosno nije savršen u meri u kojoj je njegova struktura automatizovana.

Bavljenje internet prevarama kao temom i edukacija kolega i šire javnosti ima za cilj sprečavanje prevara. Nedostatak svesti o tome kako internet prevare funkcionišu kontinuirano dovodi do pojave novih žrtava, dok nedovoljno poznavanje zakonskih odredbi i potencijalnih kazni može stvoriti potencijalne izvršioce ovog krivičnog dela. Kada se kompleksne teme objasne jednostavnim jezikom, to predstavlja značajan korak u obrazovanju pojedinca, kako u pogledu pravnih, tako i tehnoloških aspekata problema, ali iz pravnog ugla.

Ovakav jedan akademski rad ne bi trebalo da odvraća ljude od korišćenja interneta, niti da predstavlja prepreku napretku i digitalizaciji teških i dugotrajnih administrativnih obaveza. Umesto toga, cilj je da se ljudi pravovremeno edukuju kako bi digitalni svet mogao što pre da se integriše u sve segmente društva. To će olakšati svakodnevno funkcionisanje i poslovanje, uz poštovanje zakonske regulative. Zbog svega prethodno pomenutog, izuzetno je važno edukovati ljude o tome kako da izbegavaju internet prevare.

Ključne reči: *Internet pravo, krivična dela, privatnost, zaštita podataka, internet prevare.*

References

1. Bjelajac, Ž. (2013). *Organizovani kriminalitet – imperija zla* [*Organized crime – the evil empire*]. Novi Sad: Pravni fakultet za privredu i pravosuđe
2. Bjelajac, Ž. (2011). Pranje novca kao faktor ekonomske destabilizacije u nacionalnim i međunarodnim razmerama [Money laundering as a factor of economic destabilization on a national and international scale]. *Poslovna ekonomija, 5*(2), pp. 151-170

3. Bjelajac, Ž., & Filipović, A. (2021) Fleksibilnost digitalnih medija za manipulativno delovanje seksualnih predatora [The flexibility of digital media for the manipulative action of sexual predators]. *Kultura polisa, 18*(44), pp. 51-67
4. Bošković, M., & Marković, M. (2015). *Kriminologija sa elementima viktimologije* [*Criminology with elements of victimology*]. Novi Sad: Pravni fakultet za privredu i pravosuđe
5. Convention for the Protection of Individuals with regard to AutomaticProcessing of Personal DataStrasbourg, 28.I.1981, Downloaded 2023, April 1 from https://rm.coe.int/1680078b37
6. Convention on High-Technological Crime, Budapest, 2001, Downloaded 2023, April 1 from https://rm.coe.int/1680081561
7. Ignjatović, Đ., (1996). *Kriminologija* [*Criminology*]. Beograd: Nomos
8. Kojić, M. (2015). *Izazovi kompjuterskog kriminala – monografska studija* [*Challenges of computer crime – monographic study*]. Novi Sad
9. Komlen-Nikolić, L., Gvozdenović, R., Radulović, S., Milosavljević, A., Jeković, R., Živković, V., Živanović, S., Reljanović, M., & Aleksić, I. (2010). *Suzbijanje visokotehnološkog kriminala* [*Suppression of high-tech crime*]. Beograd: Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije
10. Krivični zakonik Srbije [Criminal Code of Serbia]. *Službeni glasnik RS,* br. 85/05, 88/05 – ispr., 107/05 – ispr., 72/09, 111/09, 121/12, 104/13, 108/2014, 94/16 i 35/19
11. Milić, D., & Đukić, D. (2022). Pitanje utvrđivanja identiteta registranta naziva intertnet domena u svetlu važećih propisa o zaštiti podataka o ličnosti [The issue of determining the identity of the registrant of an internet domain name in the light of current regulations on the protection of personal data]. In: Perović Vujačić, S. (ur.*), Zbornik radova 35. Susreta Kopaoničke škole prirodnog prava* [*Proceedings of the 35th Meeting of the Kopaonička School of Natural Law*]. Beograd: Kopaonička škola prirodnog prava – Slobodan Perović
12. Petrović, S. (2004). O informacionoj revoluciji u kontekstu zloupotrebe informacione tehnologije [About the information revolution in the context of misuse of information technology]. In: *Naučno stručno savetovanje Ziteh* [*Scientific professional consultancy Ziteh*] (pp. 1-14). Bijeljina
13. Popović, D., Budimlić, M., & Puharić, P. (2009). *Kompjuterski kriminalitet kriminološki,krivičnopravni, kriminalistički i sigurnosni aspekt* [*Computer crime, criminological, criminal law, criminal and*

security aspects]. Sarajevo: Fakultet za kriminalistiku, kriminologiju i sigurnosne studije
14. Urošević, V. (2009). 'Nigerijska prevara' u Republici Srbiji ['Nigerian fraud' in the Republic of Serbia]. *Bezbednost, Beograd*, *51*(3), pp. 145-157
15. Zakon o potvrđivanju konvencije o visokotehnološkom kriminalu [Law on ratification of the convention on high-tech crime]. *Službeni glasnik RS,* br. 19/09
16. Zakon o zaštiti podataka o ličnosti [Law on Personal Data Protection]. *Službeni glasnik RS*, br. 87/18