

# ABUSE OF E-COMMERCE FROM THE ASPECT OF CYBERCRIME

**Milica Stojković, PhD<sup>1</sup>**

Faculty of Law for Commerce and Judiciary,  
University Business Academy, Novi Sad, Serbia

**Milica Cvetković, PhD**

High School for Criminalistics and Security, Niš, Serbia

**Abstract:** The spirit of modern business life cannot be imagined without the Internet and its networks. Electronic commerce enables easy and fast communication, quick transmission of large amounts of data over long distances, digital delivery of goods and services, money online payments, creation of virtual organizations. The rapid increase in computer crime has led to technical, legal and operational problems. The primary task of legal regulation of electronic trade is to encourage its development, while at the same time trying to prevent its abuse. It is difficult to estimate the number and type of criminal offenses in the area of computer crime that occur in the course of e-commerce, as well as the economic damage caused by the commission of these crimes. This fact makes this subject legally current and still insufficiently explored in practice.

**Keywords:** e-commerce, crime, abuse, computer, damage.

## INTRODUCTION

The development of science and technology has led to the emergence of the digital age, which has also caused changes in human life, as well as in the way of doing business. In business, the quality of business processes is improved, they are done much faster and thus provide an increase in business volume. With the advent of the digital economy, information technology, which is changing the way of doing business at all levels, both countries, companies and individuals, is especially important. The digital economy directly changes business, trade and organization of the market, through a new way of learning and knowledge exchange, which accelerates the overall economic and social development.

---

<sup>1</sup> mstojkovic1@yahoo.com

The term cybercrime refers to a set of criminal offenses where computers, computer networks, computer data, computer systems, as well as their products in material and electronic form, occur as an object of execution and as a means of committing a criminal offense. It should also be noted that digital economy and e-commerce become particularly significant area for organized criminal groups. (Kostić, Konstatinović-Vilić, Nikolić-Ristanović, 2011) The disconnection of electronic commerce in the cyber space carries with it certain specificities, which will be discussed in this paper, both from the criminal-legal and from the economic aspect.

## THE TERM E-COMMERCE

Electronic commerce presents a modern form of doing business electronically and encompasses a range of different activities, including electronic trading of goods and services, on-line delivery of digital content, electronic money transfer, electronic trade of securities, invoice billing, public procurement, direct marketing of consumers and post-sale services. Within the European Union, there is no universally accepted definition of e-commerce so far, but it is clear that it involves commercial transactions, via telecommunication networks, using electronic means. The transactional nature of the exchange is a key feature, including an agreement to deliver goods, to perform services or transactions of intellectual property rights.

With a fast-paced environment, e-commerce has created a wide range of innovative businesses, markets - creating new features and new revenue. As far as the very concept of electronic commerce is concerned, there are different definitions in theory and in the legislation. According to Article 4, paragraph 2 of the Law on Electronic Commerce, electronic trade in goods and services is a form of district trade in the sense of the law governing trade. According to Article 3 of the Law on Trade of the Republic of Serbia (Official Gazette of RS no. 53/10 and 10/13) trade is a set of business activities of goods traffic, that is, services aimed at generating profit, as well as another socio-economic goal. As far as the very concept of electronic commerce is concerned, there are different definitions in theory and in legislation. According to Article 4, paragraph 2 of the Law on Electronic Commerce, electronic trade in goods and services is a form of district trade in the sense of the law governing trade. According to Article 3 of the Law on Trade of the Republic of Serbia trade is a set of business activities of goods traffic, that is, services aimed at generating profit, as well as another socio-economic goal.

## SOME LEGAL ASPECTS OF E-COMMERCE

Electronic commerce represents the massive use of computers in mutual communication for the purpose of trade. The rapid development of computer technol-

ogy and Internet communications, with its technical capabilities and characteristics, has caused doubts about the legal nature. The United Nations Organization, through its specialized UNCITRAL organization, developed in 1996 UNCITRAL Model Law on Electronic Commerce. The Law regulates the conditions and ways of providing information society services, the obligation to inform the users of services, the electronic commercial message, the rules regarding the conclusion of the contract in electronic form, the responsibility of the provider of information society services, supervision over the implementation of laws and violations.

Our Electronic Commerce Act ("Official Gazette of RS", No. 41/2009) is drafted based on this model. It should be emphasized that this is a special law, but does not exclude the application of other regulations governing commercial messages, certain services, contract conclusion, consumer protection. It excludes its application if this application is more unfavorable to consumers. The Law on protection of consumers ("Official Gazette of RS", No. 79/2005) also refers to the application of the rules envisaged for the so-called distance selling.

Electronic Commerce first appeared in the United States, using the Internet as a communication channel through which direct communication between sellers and customers was facilitated, thus reducing operating costs and delivery times. E-business was first introduced by the U.S. company IBM dealing with computer technologies, i.e. production of computer software, hardware and having the largest number of inventions in this field. (Petrović, 2018)

In practice, the concepts of e-business and e-commerce are often identified. E-business is a wider and more comprehensive concept of e-commerce, because it involves the purchase and sale of products and services, and also includes providing customer service, cooperating with business partners, applying e-learning and transactions within business systems. E-commerce is a part of electronic business. The development of information and telecommunication technologies directly affect the continuous development and improvement of electronic commerce. From the moment of moving transactions from real to the Internet space, the development of electronic commerce progresses at a high speed.

Broadly speaking, e-commerce is defined as the sum of business operations, using modern technology. It can be said that e-commerce in the trade encompasses all forms of transactions relating to commercial activities, including organizations and individuals, based on the production and transmission of digital data, containing textual, visual, and sound recordings. (Končar, 2008:147)

## Conclusion of the contract in electronic form

The Electronic Document Act, electronic identification and trust services in electronic commerce regulates electronic document, electronic identification and trust services in electronic commerce. ("Official Gazette of RS", No. 94/2017) In the case of a contract concluded with the statement by electronic means, it is not a matter of any new form, but only about the way of expressing the will. The form is a requirement

from the angle of the law, and the form is a way of expressing the content, both in the electronic offer and when accepting the offer. Any possibility of fraud during the conclusion of a contract can always be easily fixed by direct contact.

The Law on Electronic Signature ("Official Gazette of RS", No. 135/2004) proclaims that the validity of the contract cannot be challenged solely because it is concluded in electronic form. When the contract is allowed in the oral form, it can be concluded in electronic form. If a written form is required, it is also necessary to use an electronic signature during electronic communication. Exceptionally, certain statements of will, including some contracts, cannot be completed electronically. The obligation to provide certain data before the conclusion of the contract in electronic form is also established. The contract is considered concluded when the bidder receives a response containing the acceptance of the offer.

## COST-BENEFIT ANALYSIS OF E-BUSINESS

Electronic commerce offers many advantages over performing traditional commercial transactions. These benefits are numerous, both for vendors and for customers. Greater use of e-commerce provides a number of benefits, and thus grow their character, and the possibility of abuse of the same. While traditional business is based on the use of paper documents in communication between participants, e-commerce provides an opportunity to all transactions carried out by Video Digital and control information system of the enterprise. Most companies combine segment of e-commerce with traditional performance activities and such organizations are called composite organizations (Rainer& Turban, 2009).

The benefits of e-business are:

1. offers companies the possibility of expanding the national and international markets with minimal investment;
2. lowers the cost of communication services, because the Internet is more favorable;
3. companies using the Internet to communicate with customers and get information about their needs;
4. cost digital promo-materials are significantly lower than the cost of printing and mailing paper catalogs;
5. electronic commerce allows companies to offer their products or services to a larger number of potential customers;
6. use of marketing distribution channels is drastically reduced, making the product cheaper and higher profits for the seller;
7. e-commerce reduces stockpiling, telecommunication costs, reduces the time between payment and receipt of goods, etc.

The main benefits that customers have from e-business are:

1. reduce the cost of your purchase, because there are no costs of performing the purchase (go to the store, transportation costs, etc.);
2. the possibility of finding a cheaper product or service;
3. possibility of electronic auctions;
4. electronic commerce often provides customers cheaper products and services allowing them to buy in many places, and to implement quick comparison of price environment;
5. customers can buy or carry out other transactions throughout the year;
6. electronic commerce allows customers to communicate with other buyers and sellers in the electronic community. (Panić, 2015)

Lack of e-commerce is the lack of live contact with the seller, which means many customers. A large number of customers are convinced by sellers that a particular product is right for them. Furthermore, a classic store allows a customer to come into physical contact with a product. Testing the product on the site is an important factor for a potential customer to decide to purchase. Electronic commerce is increasingly reminiscent of the market, where a catalog offers everything that a classic trade cannot sell. Payment by installments is just one of the tricks of the marketing of e-commerce. Often, the customer gets the product to his/ her home, which is of lower quality than the one he / she ordered, so that the costs of returning products is often higher than the price of the product itself.

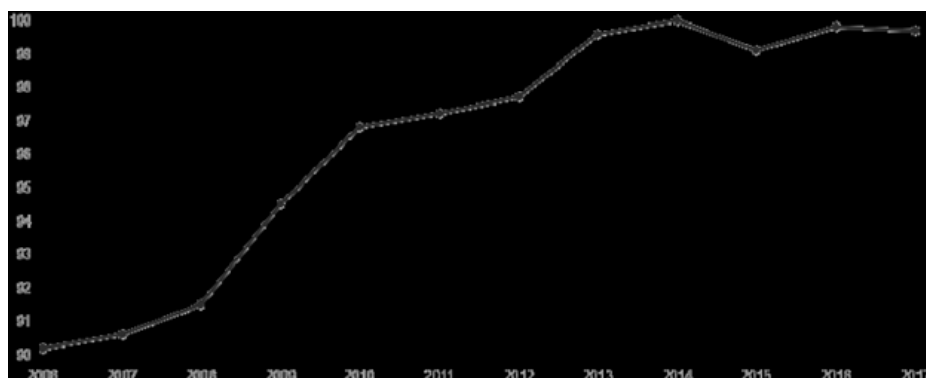
Development of the developed world economy is based on information. Realizing the importance of e-business and the possibility of abuse of the same, the developed countries have regulated this question within adequate legal framework. Misuse of e-business results in a phenomenon of cyber crime. The Republic of Serbia is a little late with the regulations in this area, but in recent years this activity has intensified, thus creating the legal framework and specific institutions whose task is to fight against cyber crime.

## THE IMPACT OF ELECTRONIC COMMERCE ON TRADE FLOWS OF THE REPUBLIC OF SERBIA

On the territory of the Republic of Serbia, the use of e-business and e-commerce is still at the beginning, because the adopted legislation encompasses the traditional way of doing business. Limits of use complete e-business is the lack of infrastructure to facilitate the execution of business transactions.

In relation to the public sector, private companies in the Republic of Serbia have replaced the traditional way of doing business electronically, via the Internet. Prospects for the development of electronic business in the Republic of Serbia is indicated by the fact that an increasing number of citizens are traded via the Internet. E-commerce allows quick finding the desired items, easier price comparison and payment transactions without visiting the bank.

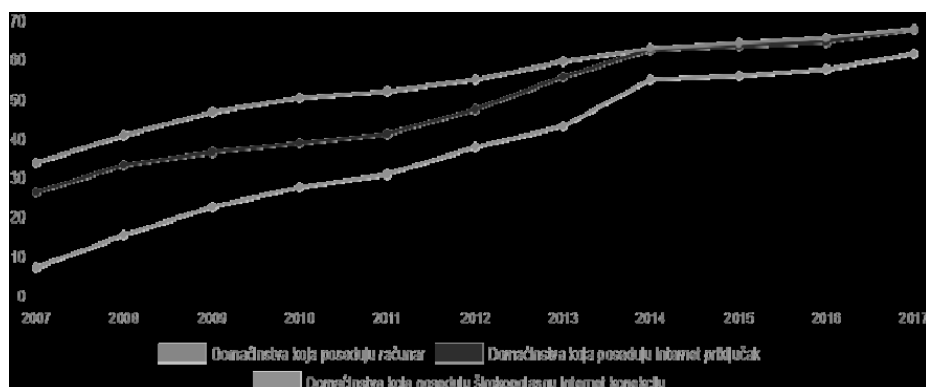
Based on the research carried out in 2017, approximately 41.4% of enterprises ordered products and services through the Internet, and 23.8% of enterprises received orders via the Internet. Social networks are increasingly present in business. Around 40% of companies use a social network for their business. In addition, 9.3% of companies paid cloud services. In Serbia, 99.7% of companies have Internet Web, sat owns 80.4% of the company (Petrovic, 2018).



**Chart 1:** *Use of the Internet in enterprises in Serbia*

Source: National Bureau of Statistics, the use of information and communication technologies in the Republic of Serbia, 2017

Graphic shows a tendency to increase the number of companies using the Internet, which indicates the increase in the use of e-business and e-commerce.



**Chart 2:** *Households with Internet connection, a computer and Internet connection*

Source: National Bureau of Statistics, the use of information and communication technologies in the Republic of Serbia, 2017

Nearly 70% of households in the Republic of Serbia have Internet connections. The highest prevalence of the Internet in the area of the capital with more than 75%, in Vojvodina it amounts to about 70%, while in central Serbia slightly above

60%. Over 90% of households have a mobile phone with Internet access, 43.7% have computers and 61.9% have a broadband Internet connection as shown in the graph No. 2. (Republic Institute for Statistics of RS, 2017)

Based on the previous data obtained from the Republic Institute for Statistics, it can be concluded that as far as households are concerned, they are expected to further increase the trend of computer users and Internet users, which is a good indicator of the development of electronic commerce in the Republic of Serbia. As for the companies and the use of communication technologies, the fact is that they have not exploited all the possibilities and opportunities offered by electronic commerce, but it is expected that it will change in the future.

E-business in commerce aims to create a successful and long-term market position. Market positioning provides long-term achievement of the objectives of business for companies. The primary objectives of enterprises in electronic commerce are to meet the needs of customers and realize good level of profit. A successful market position is an important target for trade. The chances of a successful business are far greater if the positioning is anticipated and planned, and it is one of the reasons why e-commerce is important for positioning in the market.

## CYBERCRIME

Technology and the Internet have contributed to rising crime. The anonymity provided by the Internet technology enables perpetrators to make a false online applications for bank loans, credit card bills, insurance, brokerage accounts, health care, etc. (National Fraud Centar, 2000). The emergence of computer crime dates back to the 70s of XX century to the 80s and 90s when many economies realized the danger of this type of crime. Computer crime is a special kind of crime directed against computer systems as a whole, or partially, in different ways and by different means in order to gain profit for oneself or others, or to cause damage. (Parker, 1983).

Computer security is a human problem that cannot be independently solved by means of technology. Security is an issue of management. The fact is that policy managers are critical to the success of the security program. Many companies do not pay enough attention to computer security. Many managers do not understand the problem and they do not think they are at risk. What is important is that managers understand the practical, ethical and legal issues of security, and inform their employees about the importance of security issues and security risks (Milosavljević, Veinović & Grubor, 2009).

With the development of electronic commerce, economic crime gets a new shape and a new environment. Computer technology has become the source of transnational crime, eliminating the differences between the countries. Computer crime is a form of criminal behavior in which the use of computer technology and information systems are manifested as a crime scene, or the computer is used as

an agent or as a target of the crime, which results in a consequence in legal terms. Cybercrime is also against legal violations of property in which the computer data are changed (computer manipulation), destroyed (computer sabotage), or used with hardware (stealing time) (Stojanović, 2011). An important feature of a computer crime is a rapid pace of development. Numerous forms and manifestations of cyber crime are constantly increasing, and the main cause of this is the continuous development of technology. Computer technology is used in all spheres of life, resulting in a significantly more dangerous forms of criminal behavior which have not previously be known in the criminal and judicial practice. Cybercrime knows no borders between countries and continents. This is a consequence of the spread of the Internet use in the world.

The most common method of carrying out scams on the Internet involves creating fake Web addresses where lower cost electronic products are sold. Buyers are attracted by the low prices of the products and a significant discount. A characteristic of these cases is the lack of ability to pay by card, even if there is, it is very expensively charged. After the advance payment, online retailers disappear, leaving customers with neither money nor products.

Almost all forms of crime include various forms of “laundering” money, tax evasion, abuse of various businesses, investment scams and the like. Fraud in accounting lead to the presentation of false information about the financial condition, performance and net assets of the entity, and therefore cause false and falsified financial statements. Fraud in business often has support in accounting, which on one hand is the instrument of their execution and concealment, but on the other hand can be an instrument of detection of a criminal activity (Cvetković & Kesetović, 2018).

Challenges as regards detecting computer fraud are an open question whether a criminal investigation is the appropriate instrument for criminal acts. Computer fraud is the sphere of organized crime, so it is necessary to intensify the proactive work of the police and the judicial (public prosecution), to reduce the percentage of commission of computer frauds. To achieve this goal, it is necessary to intensify cooperation between state organs that have relevant information concerning crime prevention.

In the domain of domestic regulations, the most prominent is the Law on Organization and Jurisdiction of State Authorities for Combating High-Tech Crime (“Official Gazette of RS”, No. 61/2006 and 104/2009) In the area of inter-state law, this legal topic relates to the United Nations Convention against Transnational Organized Crime (Official Gazette of the FRY- International Treaties, No. 6/2001), which was adopted in 2000 in Palermo and the Council of Europe Convention on Cyber Crime, which was adopted in Budapest in 2001. Cybercrime is “the commission of offenses for which its subject and object have the Internet as a global computer network and a computer that makes the trained persons in order to cause harmful effects or obtaining illegal material benefit”. (Stamenković, 2014)

## CRIMINAL ACTS AGAINST THE SECURITY OF COMPUTER DATA

Criminal offenses against the security of computer data enters the so-called high technology or computers crime, or, cybercrime. (Martin&Martin, 2001) The Criminal Code (Official Gazette, 85/2005...94/2016) provides for criminal offenses against the security of computer data. Criminal law protects the use of information technology for permitted purposes, and the concepts of "computer systems" and "computers" are introduced into criminal law. The Criminal Code prescribes a total of eight criminal offenses against the security of computer data. The object of protection of these crimes is the security of computer data and systems, or, computer networks. (Vodinelić, 1990)

In the case of a criminal offense Damage to computer data and programs, the act of committing a criminal offense is the deletion, alteration, damage, concealment or otherwise the use of unusable computer data or a computer program. The consequence of a criminal offense is to prevent computer programs and data serving their purpose, and the specified execution actions must be taken unauthorized. The object of execution actions is computer data or a computer program. As far as the subjective character is concerned, an intent is needed, and the perpetrator of this criminal offense may be any person. If another offense was committed by the act of committing this criminal offense, as a rule, there will be only that other criminal offense.

In the case of a computer-sabotage offense, the act of committing a crime is the filing, destruction, erasure, alteration, concealment, or otherwise making unusable computer data or programs. The second act of execution is destruction and damage to the computer or other device used for electronic processing and data transfer. For the existence of a work, a computer-focused action should be important for state authorities, public services, institutions, or businesses.

When it comes to Making and Involving Computer Viruses, the act of committing this form of criminal offense is the creation of a computer virus that has the ability to cause the computer to operate incorrectly and cause damage. When a computer program is created, the job is completed and it exists only if a computer virus is created in order to be entered into another computer. There is another form of commission of this crime that consists in entering a computer virus into another computer and a computer network.

A particular form of fraud is reflected in the act of committing a criminal offense by entering inaccurate data, failing to enter the correct data or concealing another way of accurate data or false display of data. The goal of computer fraud is to achieve an altered result of electronic data processing, with the intent to acquire unlawful material gain, thus causing damage to the other. It is interesting that for a complete criminal act, it is not necessary that this intention and the achieved, hardest and most difficult form is determined in accordance with the amount of property gain obtained, while the privileged circumstance makes the

intention to damage only the other person, without the intention of obtaining unlawful material gain and necessity left intentions.

Unauthorized inclusion in a computer, a computer network, or unauthorized access to electronic data processing constitutes an act of execution of the basic form of a criminal offense with an irrelevant intent of execution. In a more severe form, we recognize the use of data that results from the offense.

The other heavier forms of criminal offense exist in the case with the consequences of a more severe degree, with the existence of an intent.

Preventing and restricting access to the public computer network except the security of computer data aims to protect certain freedoms and rights of citizens. The act of a criminal offense is the prevention or obstruction of access to the public computer network unauthorized. A severe form exists if an official appears as an executioner in the performance of a service.

In the case of Unauthorized use of computers and a computer network, the execution is an unauthorized use of computer services and a computer network. Users of Internet Service Providers and Providers are affected. It is necessary to have an intent and intention to acquire unlawful material gain for oneself or others, although it is not necessary that the intention be achieved. It is interesting that mostly the perpetrator performs this unlawful act repeatedly, and there is only one criminal offense. In this part, it is interesting that criminal prosecution is undertaken solely by a private lawsuit.

Article 304a of the Criminal Code determines as a criminal offense the Creation, acquisition and giving of other means for the commission of criminal offenses against the security of computer data. In the legal text, this work is among the latest in the group of criminal offenses against the security of computer data.

## CONCLUSION

The rapid increase in computer crime has led to a number of problems: technical, legal and operational. Regarding procedural items, the main problem is in finding and collecting evidence. In the case of criminal offenses committed by computer, evidence is in electronic form. The cyber space does not recognize the territorial and state boundaries. Many acts cannot be localized. The issue of jurisdiction is a problem when it comes to the fight against computer crime, and it is necessary to consult one of the states that pretend to be competent in order to determine under which jurisdiction the procedure would be most effective. Special police training, prosecutors and judges are needed, so that the state apparatus can put a stop to this type of crime.

The use of e-commerce has taken on huge borders today, so in practice there are inevitable encounters of various types of criminal offenses against the security of computer data in commercial traffic. It is difficult to estimate the number and type of these crimes, as well as the economic damage. The methods of committing

crimes are very diverse. Criminals are distinguished where computers appear as a means of committing a criminal offense and as objects of execution, as well as criminal offenses in which the elements of the illegal use of the Internet appear. In one group there are new offenses such as the spread of computer viruses, the destruction of files or software, and the like, or the offenses in which the computer is the means of attack. The second group is a classical offense, such as scams, copyright infringement, and the like, in which the computer is used as a means of execution and which, in turn, gets a new form of cyber space in which electronic commerce takes place on a daily basis.

## REFERENCES

1. Cvetković, D., Kesetović, Z., (2018) *Ekonomski kriminalitet i uloga forenzičkog racunovodstva u njegovom otkrivanju*, Finansijski kriminalitet, Institut za uporedno pravo, Zrenjanin
2. Parker, D.B., (1983) *Fighting computer crime*, New York (USA)
3. Krivični zakonik ("Službeni glasnik RS, br.85/2005, 88/2005- ispr., 107/2005- ispr, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 i 94/2016")
4. Končar, J., (2008), *Elektronska trgovina*, Subotica
5. Kostić, M., Konstatinović-Vilić, S., Nikolić-Ristanović, (2011) *Kriminologija*, Prometej-Zemun
6. Martin, D., Martin F.P., (2001) *Cybercrime, menaces vulnérabilités et rispostes*, Paris
7. Milosavljević, M., Veinović, M., Grubor, G., (2009) *Informatika*, Univerzitet Singidunum, Beograd
8. National Fraud Center (2000) *The Growing Global Threat of Economic and Cyber Crime*, Georgia, National Fraud Centar
9. Panić, M., (2015) *Pravni aspekti prodaje na daljinu putem interneta*, Pravni fakultet, Kragujevac
10. Petrović, D., (2018) *Vojno delo*, Ministarstvo odbrane Republike Srbije
11. Rainer, R. K. Jr., Turban, E., (2009) *Увод у информационе системе*, Дата Статус, Београд
12. Republički zavod za statistiku, *Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji*, 2017
13. Stojanović, I., (2011) *Elektronska trgovina i kupovina putem interneta u Srbiji*, Univerzitet Singidunum, Beograd
14. Stamenković, B., (2014) *Visokotehnoški kriminal- praktični vodič kroz savremeno krivično pravo i primjere iz prakse*, Podgorica
15. Vodinelić, V., (1990) *Metodika otkrivanja, razjašnjenja i dokazivanja računarskog kriminaliteta*, Zagreb

16. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala ("Službeni glasnik RS", br. 61/2006 i 104/2009)
17. Zakon o elektronskoj trgovini ("Službeni glasnik RS", br. 41/2009")
18. Zakon o elektronskom potpisu ("Službeni glasnik RS", br. 135/2004)
19. Zakon o trgovini ("Službeni glasnik Republike Srbije", br. 53/10 i 10/13)
20. Zakon o zaštiti potrošača ("Službeni glasnik RS", br. 79/2005)
21. Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju ("Službeni glasnik RS", br. 94/2017)