UDC: 347.189:004.738.5(497.11)
Review article

ELECTRONIC SIGNATURE: LEGAL AND PRACTICE REVIEW OF THE REPUBLIC OF SERBIA

Dragana RANDJELOVIC, [1] Faton SHABANI[2]

[1]*Department of Legal Sciences, International University of Novi Pazar*
[2]*Department of Civil Law, Faculty of Law, University of Tetova*
[*]*Corresponding author e-mail: faton.shabani@unite.edu.mk*

Abstract

In the modern world, everything has digitalized with time. From online shopping, banking to automation of complex business functions, everything is digital today, and it lays the foundation of our future as well. One of the things that has become more popular and at the same time about which debates have taken place is electronic signatures or e-signatures. This is because in today's practice of contractual legal transactions dealing with terms such as, electronic signature, digital signature, e-signing software, e-signing solution, advanced electronic signature, qualified electronic signature, has become normal. The purpose behind these terms is that they primarily stand for the ability to transform a hard copy document into a digital document or record. An electronic signature is an electronic tool - often a sound, symbol or process - linked to a contract, document, or other record. As such, electronic signature today has taken place in the vast majority of countries around the world gaining the same weight and legal effect as a traditional paper document with a pen and ink signature. Such an extension of electronic signature has resulted in the adoption of legal rules in these countries, which given the tradition of different systems belonging to the states, has resulted in a variety of solutions which occasionally differ substantially between themselves. This was the reason why, at the global level, discussions and preparations for the drafting of rules of international character began, which will provide answers to the controversial issues for electronic signatures on cross-border transactions. In this regard, UNCITRAL is distinguished by model laws and the European Union by directives and regulations for its member states. The objectives of this article are as follows: (1) to identify the need for establishing a legal framework for electronic signatures; (2) to present the overview of the legal framework of the Republic of Serbia regarding the electronic signature; (3) to provide a concise summary of the procedure of getting electronic signature; (4) to explain the problems and challenges faced by the use of electronic signatures in Serbian contractual practice. The authors have achieved these objectives through the review of legal regulations and practice in the Republic of Serbia.

Keywords: electronic signature, digital document, legal framework, practice, challenges.

1. Introduction

The signature has been the prime method a person uses as a proof of identity, and as a material expression of intent and execution of documents. A signature on a document indicates the provenance of the document and the intention of the signatory with regard to that document. With the advent of the electronic era, a form of signature is adopted for electronic documents (Davidson: 2009, 74). Given the pressure that the business faces with electronic commerce, respectively, the impact electronic commerce has on doing business imposed businesses to be under pressure to adapt to the new electronic environment where they operate. Noting that an increasing number of transactions in international commerce are carried out by means of electronic data interchange and other means of communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information (Model Law on Electronic Signatures), it created the need to adopt harmonized regulation to regulate this phenomenon. There is an endless

variety of different types of transactions that could be done electronically. These include contracts for the circulation of goods and for the provision/acceptance of services. This trend inevitably broke into the market and legal practice of the Republic of Serbia, which forced the lawmaker of this country to prepare and adopt the Law on Electronic Signature in the first years of the XXI century. Electronic signature was a central element of the law, as it was considered as a key point in an e-signed contract - data in electronic form, which is logically associated with other data in electronic form and which is used by the signatory to sign.

The use of electronic technology in commerce is proven to be a factor of saving not only money but also time, efforts and resulting in efficiency in realizing business goals. Moreover, electronic commerce and concretely the electronic signature intend to become equivalent to contracting and signing on paper documents. In the Republic of Serbia, despite the existence of legislation that covers in detail the issue of electronic signatures in business contractual relations; difficulties are encountered in the implementation and materialization of legal provisions by business entities and state administration authorities. These theses, the authors during the research have elaborated through scientific methods such as empirical, normative, historical, comparative, analysis and synthesis.

In all the countries where e-signatures are legally binding, its legal status depends on proving the presence of these three elements: Who has signed? What was signed? Has the document been changed or tampered with after signing? Regarding the first part there are a number of methods that can be used to perform identity verification such as using verification via SMS, email, electronic ID. In this case the stricter the identity control there is in the method, the higher the security the method offers. The next part that affects the legal status of a signed document is the content of the document and the intent of the parties. What was signed? Did the parties invite to the contract intend to sign and legally commit to the document? This is where the contract content and what the parties stated in the signed version of the document matter. If a contract changes before being signed, then the new wording becomes a new contract offer. If there is more than one party invited to sign the document, then the contract is only signed when all have signed, thus agreeing on the common content. The final part that is important to determine the legal status of an electronically signed document is the integrity of the document after signing. This means that after the parties have signed the document, it must be kept intact and not be modified or tampered with. By using an electronic signature based on Public Key Infrastructure (PKI), the document gets hashed and signed using an asymmetric encryption key pair. The integrity of the document is thereby protected so that even a slight change in the document, e.g. change of a comma, a point or space, would create a different hash value, thereby revealing that a change has occurred.

This paper examines primarily (a) the need for legal framework for electronic signatures; (b) legislative framework of electronic signature in the Republic of Serbia; (c) the way and conditions for obtaining electronic signature; (d) the process of electronic signing in the Republic of Serbia's practice; (e) the problems faced by the practice; (f) recommendations given in order to find and provide the most adequate solutions to the situation in which the legislation and practice of the Republic of Serbia is.

2. General reviews - the need for legal framework for electronic signatures

The commercialization of the Internet and the development of the global economy contributed to the creation of a new concept in the business of legal entities. The integration of a large number of information systems and networks has led to the globalization of business through the global computer network and the emergence of a new concept called electronic

commerce. Under e-commerce, it is assumed that business operations are carried out using modern electronic technology (Bjelić, 2000:3). Electronic technology implies the combined use of information technology and telecommunications. Among the means of communication encompassed in the notion of "electronic commerce" are the following modes of transmission based on the use of electronic techniques: communication by means of Electronic Data Interchange (EDI) defined narrowly as the computer-to-computer transmission of data in a standardized format; transmission of electronic messages involving the use of either publicly available standards or proprietary standards; transmission of free-formatted text by electronic means, for example through the internet(UNCITRAL Model Law, 1998: 17). In addition, electronic commerce consists of several areas: electronic commerce, electronic payments, electronic communications, electronic production and electronic distribution. In thus new business environment where electronic transactions become the norm, the use of paper to document business transactions is becoming less important, i.e., one of the benefits of concluding business by using digitalized information is that it obviates the need to transmit and store paper.

In the information society a growing number of legal acts are performed electronically. For example, contracts concluded over the Internet are becoming more commonplace. As the value of such transactions, especially in a business-consumer relationship, is usually very small, parties in many electronic transactions refrain from using electronic signatures as means to verify the identity of the other party. In that case the supplier of goods or services knowingly accepts the risk that the other party is not who he says he is. The consumer accepts a similar risk. The general expectancy is that in the future the value of electronic transactions will increase as a result of the growing confidence of enterprises and consumers in electronic commerce. This will lead to a growing need for electronic signatures that can perform the same functions as a hand-written signature (Snijders & Weatherill: 2003, 27).

As a consequence, when contract parties shift from paper-based communication techniques to electronic methods, there is often uncertainty about how existing laws will treat data messages in terms of validity, enforceability and admissibility. This legal uncertainty is an obstacle to the adoption of e-commerce and therefore many governments have amended or supplemented existing laws in order to address it (UNCTAD Information Economy Report: 2006, 299).

The rapid development of information technologies and the development of the internet as a medium between business entities have opened up, above all, a new issue when contract law is at stake. E-commerce is a mayor security issue because business processes take place online, i.e. in front of a large number of people using the internet and thus become susceptible to changes by malicious network users. It means that the security of electronic business transactions has become an important issue. Since business deals are often concluded in the electronic market over great distances and therefore often without any personal contact, special security precautions must be established in order to build trust. It must be guaranteed that any electronic documents do actually come from the source that they are believed to come from, and sensitive data like electronic contracts must not be changed en route. Moreover, the receipt of the electronic documents must be confirmed by the receiver (Meier & Stormer, 2009:93). These risks are reflected in possible problems when determining the authenticity of the business entity with which the correspondence is performed, as well as the determination of the integrity of the information exchanged, which is of great importance in performing monetary transactions (Nikčević & Nikčević, 2011:4). An electronic signature is a technology that

enables authenticity, integrity protection and non-validity of data and documents in electronic commerce.

Contract laws worldwide have traditionally asked the parties to place their signatures in the contract document. In traditional commercial activities, one usually signs a document to express his agreement with the content of the document, and his willingness to enjoy prescribed rights and assume corresponding responsibilities. Thus the signature should be credible, verifiable, and cannot be counterfeited and reused while the signed document should not be modified or denied. In electronic commerce, two parties negotiate and enter into contracts through network. Documents thus formed are mostly in the electronic form (Qin, 2009:144). With the launch of the electronic epoch, electronic signatures also appeared. The electronic signature is defined as "any letter, character or symbol that is manifested by means of electronic or similar means and which is implemented or approved by the party in order to be certified in writing" (Smedinghoff, 1999: 125) or as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication" (Directive on Electronic Signatures, 1999).It is an encrypted message digest (message hash value) (Schneider, 2011:473). It can also be considered as a procedure that guarantees the authenticity of a document (Meier & Stormer, 2009:94). Typically, the electronic signature is attached to the message and stored as a separate data element as long as it maintains a reliable connection with the relevant message. Stephen Mason suggest that it is not necessarily intended that an electronic signature should be manifest in a physical form, which leads to the conclusion that the quality and extent of the evidence to provide intent becomes vitally important in the event it is disputed that an electronic signature was affixed to a document or communication (Mason, 2016:181). Moreover, because the message digest is encrypted using a public key, only the owner of the public/private key pair could have encrypted the message digest. Thus, when the merchant decrypts the message with the user's public key and subsequently calculates a matching message digest value, the result is proof that the sender is authentic. Furthermore, matching hash values prove that only the sender could have authored the message (non repudiation) because only his or her private key would yield an encrypted message that could be decrypted successfully by an associated public key (Schneider, 2011:473).

Aashish Srivastava asks obvious question: Do businesses feel the need to change from the use of manuscript signatures to electronic signatures? And therefore, does the low usage result from a lack of need to change to the new technology? The answer to this question could have shed important insights on the issue of low usage. However, there exists a general ignorance or lack of knowledge about the electronic signature technology in the business community. With such a high level of ignorance and misunderstanding about the technology, and its risks and benefits, it is difficult to conclude whether businesses' low usage of the technology has arisen from a lack of need for it (Srivastava, 2013: 61).

The increased use of electronic authentication techniques as substitutes for handwritten signatures and other traditional authentication procedures has suggested the need for a specific legal framework to reduce uncertainty as to the legal effect that may result from the use of such modern techniques (which may be referred to generally as "electronic signatures"). Due to the nature of electronic commerce it has been perceived that uniform standards for the recognition of electronic signatures would pave the way for the execution of online contracts (Laborde, 2010:227). The risk that diverging legislative approaches be taken in various countries with respect to electronic signatures calls for uniform legislative provisions to establish the basic rules of what is inherently an international phenomenon, where legal harmony as well as

technical interoperability is a desirable objective (UNCITRAL Model Law, 1998: 8). This call was answered by the United Nations Commission on International Trade Law (UNCITRAL), by preparing and adopting two documents: The Model Law on Electronic Commerce in 1996, and the Model Law on Electronic Signatures in 2001. In addition, the United Nations as a whole body adopted the Convention on the Use of Electronic Communications in International Contracts in 2005. Soon, the Model Law was identified as the most competent document for regulating electronic signatures. It constitutes a new step in a series of international instruments adopted by UNCITRAL, which are either specifically focused on the needs of electronic commerce or were prepared bearing in mind the needs of modern means of communication. This Model Law is designed to assist States in establishing a modern, harmonized and fair legislative framework to address more effectively the issues of electronic signatures. The rapid impact that this Model Law has on national legislation regulating issues related to electronic signature is the fact that the Model Law has been adopted in 32 States.

3. Electronic signature in the Republic of Serbia - legislative framework

The first act regulating any of the aspects of e-commerce was the Law on Electronic Signature, which was adopted in 2004. It regulated the use of electronic signatures in legal works, business, rights; obligations and responsibilities related to electronic certificates, the validity and proof of the electronic document are guaranteed. The Law on Electronic Signature is in line with the EU Directive 1999/93 EC on Electronic Signatures adopted on December 13, 1999 and came into force on January 19, 2000. Two main roles of this Law in the light of European trends focused on: defining conditions under which electronic signatures are legally equal to handwritten signatures; and defining which requirements must be met by certification bodies for the issuance of qualified electronic certificates. Other accompanying acts are taking part in the additional definition of the status and process of using electronic signatures have been adopted: Regulation on the Records of Certification Authorities; Regulation on Technical and Technological Procedures for Creating a Qualified Electronic Signature and the Criteria to be met by devices for Creating a Qualified Electronic Signature; Regulation on Specific Terms and Conditions for Issuing Qualified Electronic Certificates; and the Regulation on the Register of Certification Bodies for Qualified Certificates Issuing in the in the Republic of Serbia.

Law on Electronic Signature in Article 2, paragraph 1 prescribes that the electronic signature is a set of data in the electronic form which are joined to or logically connected with an electronic document and the purpose of which is to identify the signatory. The purpose of the digital signature is to confirm the authenticity of the content of the message (proof that the message has not changed on the way from the sender to the recipient), as well as to ensure the guarantee of the identity of the sender of the message. An electronic signature is not an image of a scanned handwritten signature in a document, but its replacement.

Law on Electronic Document, adopted in 2009, regulates the conditions and manner of handling electronic documents in legal transactions, administrative, judicial and other procedures as well as the rights, obligations and responsibilities of companies and other legal entities, entrepreneurs and natural persons, state bodies, bodies of territorial autonomy and bodies of local self-government units and bodies, enterprises, institutions, organizations and individuals entrusted with the performance of public administration affairs, or public authorizations in connection with this document. It regulates the electronic document as a document in electronic form used in legal affairs and other legal actions, as well as in administrative, judicial and other proceedings before a state body. It can be disputed that the validity or proof force can be disputed solely because it is in electronic form, and the electronic signature is completely equal with its own signature. The adoption of the Law on Electronic

Document, preceded by the Law on Electronic Signature in the Republic of Serbia marked the beginning of the process of developing the legal framework necessary for the development of electronic business.

On July 23, 2014, the European Union adopted Regulation No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and repealing Directive on Electronic Signatures. This was soon found to be a big step toward the so called European Digital Single Market. Repealing the 15-year-old European directive on a community framework for electronic signatures (Directive 1999/93/EC), this new regulation aims at providing a common transnational foundation for secure electronic interaction between European citizens, businesses, and public authorities. Thus, by providing the building blocks for ensuring trust, convenience, and security in the online environment, the regulation represents a major contribution to the European Digital Single Market (Bastin & Hedea & Cisse, 70). According to this Regulation, by 29 September 2018, a EU citizen with an eID card (notified according to eIDAS) are able to access any online public service from any EU member state, and perform his/her administrative procedures online with the same trust as if the person was physically present. In practice, eIDAS gives EU member states the opportunity to notify the European Commission of their eID means (articles 7 and 9) and makes it mandatory for other member states to recognize the eID means for authentication on their online public services. The obligation of the Republic of Serbia to harmonize its law with legal regulations of the European Union, as well as the need for simplifying procedures, modernizing public administration and facilitating access to public administration services, and a large number of these services has required the adoption of new Law on Electronic Document, Electronic Identification and Trust Services for Electronic Transactions. This Law was adopted with the aim to establish fundamental legal framework which will provide more room for implementation of electronic forms of conducting business operations and bringing it to the same level of use as the existing classic forms. The Law inter alia governs e-document, electronic identification, trust services for electronic transactions, e-signature, e-stamp and time stamp, as well as electronic delivery. In Article 2, this Law regulates the electronic signature as set of data in electronic form that is associated or logically connected to other (signed) data in electronic form, so that the electronic signature confirms the integrity of these data and the identity of signatories. Advanced electronic signature is an electronic signature that meets the additional requirements for ensuring a higher level of reliability of confirming the integrity of the data and the identity of the signatories in accordance with this Law, and a qualified electronic signature is an advanced electronic signature created by a qualified electronic signature creation tool and based on a qualified certificate for electronic signature. An electronic document is defined as a set of data composed of letters, numbers, symbols, graphic, sound and video material in electronic form. This Law enabled the electronic signature to become completely equivalent to a handwritten signature. This position of the Law is in full compliance with Article 25(2) of the eIDAS Regulation: “A qualified electronic signature shall have the equivalent legal effect of a handwritten signature”. Also, an electronic stamp serves as a substitute for the stamp of the legal entity and the signature of an authorized person. A service is also introduced that will be enable users to electronically identify and electronically sign the document via the username and password, and the PIN is received through the SMS message, which activates the qualified electronic signature option. Three levels of identification are foreseen:

- basic, where users use their e-mail address and mobile code,
- intermediate, where the passwords are used, and

- Advanced level, where there is a special PIN, and there is the possibility of additional protection such as the fingerprint.

On the day of the entry into force of this Law, the Law on Electronic Signature and the Law on Electronic Document end the implementation.

4. How to get an electronic signature?

The Ministry of Internal Affairs of the Government of the Republic of Serbia issues citizens' qualifications for electronic signature on ID card with chip for free. For issuance of a certificate, a password for the ID card is obtained in an envelope when downloading this document is required. An application for the issue of a qualified certificate for electronic signature shall be filed at the police station where the ID card is issued. In addition to the submitted request, in the presence of a police officer at the police station, it is necessary to sign a contract for issuing a qualified electronic certificate on the ID card.

Some of the possibilities of using a qualified electronic certificate are:

- electronic transactions of legal entities,
- submission of electronic application,
- registration, change and cancellation of compulsory social security,
- electronic transactions of citizens,
- e-mail,
- e-contracts,
- access to secured websites,
- electronic signing of documents,
- verification of electronic signature,
- encrypting and decrypting documents in electronic form.

There is no general legal obligation to use a qualified electronic signature if the transactions' parties declared that they do not want the legal and technical security that a qualified electronic signature brings. The most common use of a qualified electronic signature is electronic governments' service for citizens and businesses, for example on the e-Government portal.

5. Electronic signing of the contract in the Republic of Serbia – how does it look like in practice?

It is necessary for an authorized person (who usually signs contracts) to take the following actions:

- open a contract to Acrobat Reader,
- choose the option to sign a certificate,
- find a place to sign and to mark it,
- enter his PIN confirming the identity,
- close the document from further editing,
- record it, and
- send an email to the other party.

Electronic signature is a set of data connected with an electronic document and the purpose of which is to identify the signatory. Today, in practice, the most commonly used solution is

Digital Signature Technology, based on the Public Key Infrastructure Cryptography (PKIC) with electronic certificate according to X.509v3 (RFC 5280). The basis of the digital signature is the content of the message itself. By sending cryptographic algorithms, the sender first creates a fixed length record (e.g. 512 or 1024 bits), which completely reflects the content of the message. This means that any change in the content of the message leads to a signature change. So, the sender creates a digital signature based on the message he wants to send. He codes it with his secret key and sends it along with the message. The recipient upon receipt of the message decrypts the signature of the sender with his public key. He then creates a signature based on the message he received and compares it with the signed signature. If the signatures are identical, it can be sure that the message was sent by the real sender (because the public key has successfully decoded the signature) and that it arrived unchanged (because it was established that the signatures were identical). For authentication and integrity purposes, the public key contained in the digital certificate is used.

With the emergence of electronic services, which can be accessed through the ID card, an increasing number of citizens are interested in obtaining and using qualified electronic signature certificates.

6. Problems and challenges

Law on Electronic Document, Electronic Identification and Trust Services for Electronic Transactions of the Republic of Serbia does not regulate the issue of processing personal data, but it is stipulated that the competent ministry prescribes technical and technological procedures for establishing a qualified electronic signature which is directly contrary to the provisions of Article 42, paragraph 2 of the Constitution of the Republic of Serbia, as well as the decision of the Constitutional Court on which the processing and use of personal data can only be regulated by law, not by sub-legal acts. Also, the Regulation on Technical and Technological Procedures for creating a Qualified Electronic Signature and the Criteria to be met by Devices for creating a Qualified Electronic Signature is inconsistent, since some of its provisions are contradictory, and some foresee the processing of JMBG as optional and some as practically mandatory. As a result, apart from unconstitutionality, there is uneven practice, and a qualified electronic certificate, generated by four of the six certification bodies (Serbian Chamber of Commerce, Ministry of Defense and Army of Serbia, Halcon JSC Belgrade and Ministry of Internal Affairs), in the structure of the names the user contains mandatory and his/her JMBG, or the user can not, when submitting a request for issuing a qualified electronic certificate, choose whether a qualified electronic certificate will contain its JMBG or not.

Qualified electronic certificates are issued by certification bodies, which are listed in the register of the Ministry of Trade, Tourism and Telecommunications. The Ministry of Internal Affairs free of charge issues a digital signature directly on the ID card, but only works on windows computers, so this does not apply to Apple users who can only go to the Post and pay for digital signature. So, the Post is the only certification body that issues digital signatures for individuals which can be used almost on all platforms (Windows, OS X, Linux). There is no possibility for online to complete the procedure for obtaining the certificate, but it is necessary to send the printed request to the Post and fill in the payment and pay, while paying a payment service fee.

The problem that arises in practice concerns the archiving, i.e. making copies of electronically signed contracts. Law on Electronic Document, Electronic Identification and Trust Services for Electronic Transactions stipulates in Article 10 paragraph 3 that a copy of an electronic document on paper is made by printing an external form of an electronic document.

A printed copy of an electronic document has the same probative value as the original act, if the following conditions are cumulatively fulfilled:

(1) The printing of an electronic document has been carried out under the supervision of:
   (a) a natural person, an authorized person of a natural person in the capacity of a registered entity or an authorized person of a legal entity whose acts is, or
   (b) persons who are authorized to verify signatures, manuscripts and transcripts;

(2) That the identity of the printed copy of the electronic document with the original is confirmed, indicating that it is a printed copy of the electronic document:
   (a) the personal signature of a natural person, or
   (b) the signature of an authorized person of a natural person in the capacity of a registered entity or an authorized person of a legal entity, if there is a legal obligation that the act contains a stamp, or
   (c) the person who is authorized to verify signatures, manuscripts and transcripts in accordance with the law governing the authentication of signatures, manuscripts and transcripts (Article 12 of the Law on Electronic Document, Electronic Identification and Trust Services for Electronic Transactions).

However, despite precise legislative regulations, the fact is that the problem exists in practice. It is not enough just passing laws. Its efficient implementation and application by citizens and competent authorities is necessary. There is a problem in the implementation of the law, especially by the state administration due to the insufficient expertise of the staff. In addition to enacting laws, it is necessary to continuously implement an equally lengthy and strenuous process – the process of educating employees in government services, retailers, and consumers themselves to spread awareness of the importance and benefits of e-commerce, but above all to protect consumers.

The procedure for activating an electronic signature and document is still complicated because a special software, a reader and a card is required. Because of this, only 5% of the population has an electronic signature.

7. Conclusion

One of the goals of adopting the new law is acceleration, simplification, and saving time and money in business processes, as well as establishment of companies, which would allow Serbia to keep up with countries in the region and the world. This type of technology allows the sending of a large number of information, over long distances and over a short period of time. This enables an enterprise that uses electronic technology in its business to generate significant saving in operating costs, perform its tasks more efficiently and, therefore, be more competitive on the market. Changing regulations will also allow for changes in procedures in the administration, which will lead to savings of time and money of all citizens.

In practice, it has been shown that the emergence of the Internet had so far a powerful influence not only on the problem of contracting electronically, but also on various aspects of the protection of the right to freedom of expression (freedom of speech) and its abuse, the right to privacy, and the protection of certain intellectual property rights, such as a patent, trademarks and copyrights (Trnavci, 2009; 451). In accordance with the principle of freedom of contract and consensus principle, the UNCITRAL Model Law and all comparative legislations and international sources unambiguously recognize the validity of contracts concluded electronically.

Electronic signing of the contract saves both time and money (it is considered that there is a saving of approximately 300 dinars and minimum of 2 days of walking of paper by courier

services or by mail). Also, the digitalization of paper documents is of particular importance to the economy, as it will allow for considerable savings of time and money (the cost of keeping one box is 59 dinars), but it will also facilitate the search and publication of various documents. It is envisaged to create an electronic warehouse for the storage of documentation with ensuring integrity and without the possibility of changing their contents. This will also prevent a number of abuses that have been made possible in practice because employers have given their signature to employees. Electronic delivery also allows you to see the time of sending and receiving the document, which is important for judicial and administrative proceedings. Qualified electronic delivery service will represent the equivalent of the recommended shipment. However, as already mentioned in the paper, it is not enough to pass only the law and other legal acts that make it possible to implement it. In practice, numerous problems arise in the implementation of these acts, which are the result of citizens' lack of information and inadequate education of employees in competent state authorities.

References

[1]. Bastin Roland, Hedea Irina, Cisse Ismaël, "A big step toward the European Digital Single Market: Regulation EU 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)", https://www.digitalsign.pt/en/media/files/Downloads/lu-a-big-step-forward-the-european-digital-single-market.pdf[06.09.2020].

[2]. BjelićPredrag (2000). *Elektronsko trgovanje,* Beograd: Institut za međunarodnu politiku i privredu.

[3]. Davidson Alan (2009). *The Law of Electronic Commerce*, Cambridge: Cambridge University Press.

[4]. Labored Carolina M. (2010). *Electronic Signatures in International Contracts*, Frankfurt: Peter Lang.

[5]. Mason Stephen (2016). *Electronic Signature in Law*, fourth edition, London: Institute of Advanced Studies for the SASH Humanities Digital Library, University of London.

[6]. Meier Andreas, Stormer Henrik (2009). *E-Business & E-Commerce: Managing the Digital Value Chain*, Berlin: Springer.

[7]. Millstein Julian S., Neuburger Jeffrey, Weingart Jeffrey P. (2003). *Doing Business on the Internet: Forms and Analysis*, New York: Law Journal Press.

[8]. Nikčević Ivan, Nikčević Milorad (2011). "Uvođenje elektronskog potpisa u privredni system Republike Srbije kao segment usklđivanja sa pravnom regulativom Evropske Unije", *Sinergija*.

[9]. Qin Zheng (2011). *Introduction to E-Commerce*, Beijing: Tsinghua University Press.

[10]. Schneider Gary P. (2011). *Electronic Commerce*, ninth edition, Massachusetts: Cengage Learning.

[11]. Snijders Henk, Weatherill Stephen (2003). *E-Commerce Law: National and Transnational Topics and Perspectives*, The Hague: Kluwer Law International.

[12]. Srivastava Aashish (2013). *Electronic Signatures for B2B Contracts: Evidence from Australia*, Heidelberg: Springer.

[13]. Steinmetz Ralf, Dittman Jana, Steinebach Martin (2001). *Communications and Multimedia Security Issues of the New Century*, Boston: Springer.

[14]. Trnavci Genc (2009). "Zaključenje, punovažnost i dokazivanje elektronskih ugovora: komparativna analiza", *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*.

[15]. United Nations Conference on Trade and Development, *Information Economy Report 2006: The development perspective*, Prepared by the UNCTAD Secretariat, New York, Geneva, 2006.

[16]. *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001*, United Nations, 2002.

[17]. *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996,* United Nations, 1998.

[18]. *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures*, Official Journal of the European communities, L 013/12-20, 19. 1. 2000.

[19]. *Regulation on the Records of Certification Authorities*, Official Gazette of the Republic of Serbia, No 48/2005.

[20]. *Regulation on Technical and Technological Procedures for Creating a Qualified Electronic Signature and the Criteria to be met by devices for Creating a Qualified Electronic Signature*, Official Gazette of the Republic of Serbia, No 26/2008.

[21]. *Regulation on Specific Terms and Conditions for Issuing Qualified Electronic Certificates*, Official Gazette of the Republic of Serbia, No 26/2008.

[22]. *Regulation on the Register of Certification Bodies for Qualified Certificates Issuing in the in the Republic of Serbia*, Official Gazette of the Republic of Serbia, No 26/2008.

[23]. *Regulation on Technical and Technological Procedures for creating a Qualified Electronic Signature and the Criteria to be met by Devices for creating a Qualified Electronic Signature*, Official Gazette of the Republic of Serbia No 26/2008; 13/2010; 23/2015.

[24]. *Law on Electronic Document*, Official Gazette of the Republic of Serbia, No 51/09.

[25]. *Law on Electronic Document*, *Electronic Identification and Trust Services for Electronic Transactions,* Official Gazette of the Republic of Serbia, No 94/17.

[26]. http://www.croso.gov.rs/storage/files/euputstva/kvalifikovani_elektronski_sertifikati_i_ovlascenja_21112013.pdf[23.08.2020].

[27]. https://www.euprava.gov.rs/?alphabet=lat[06.09.2020].

[28]. http://www.gaia.rs/2016/07/22/elektronski-potpis-kako-potpisati-ugovor[06.08.2020].