European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com

e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2022.06.93

AMURCON 2021
AmurCon 2021: International Scientific Conference

THE INTERNATIONAL LEGAL REGULATION OF A DIGITAL SIGNATURE: ASIA-PACIFIC REGION EXPERIENCE

Sergey S. Shestopal (a, b, c)*, Dmitriy V. Lobach (d), Evgeniia A. Smirnova (e)l
*Corresponding author

(a) Far Eastern Federal University, FEFU Campus, 10 Ajax Bay, Russky Island, Vladivostok, Russia
(b) Yaroslav Mudryi National Law University, 77 Pushkinskaya St., Kharkov, Ukraine, ss.shestopal@ya.ru
(c) Vladivostok State University of Economics and Service, 41 Gogolya St., Vladivostok, Russia
(d) Far Eastern Law Institute (branch) of the University of the Prosecutor's Office of the Russian Federation, Vladivostok, Russia, dimaved85@mail.ru
(e) Department of Labor and Environmental Law, Far Eastern Federal University, FEFU Campus, 10 Ajax Bay, Russky Island, Vladivostok, Russia, smirnova.ea@dvfu.ru

Abstract

The article examines conceptual legal approaches to the definition of a digital signature and the experience of regulation of the conditions and procedure for implementing electronic document management using electronic signatures in certain countries of the Asia-Pacific region. The study of various conceptual approaches to the definition of a digital signature allows us to identify the principal features, functional purpose and legal nature of this phenomenon, which allowed the authors to formulate and propose the definition of the phenomenon in question as part of comparative legal analysis, the normative definitions of "digital signature" in the legislation of Japan, Singapore, People's Republic of China, South Korea are disclosed. Analysis of foreign experience in the legal regulation of relations arising in connection with the use of digital signatures in the implementation of electronic document management allows us to state a general trend at the national level of some APR countries, manifested in the widespread use of special means of electronic authentication of persons and their intentions regarding the assurance (confirmation) of established contracts. At the same time, unique (inherent exclusively to national legislation) features of the legal regulation of relations associated with the use of a digital signature are pointed out.

Keywords: Digital signature, electronic document management, electronic signature, electronic security, signature

https://doi.org/10.15405/epsbs.2022.06.93
Corresponding Author: Sergey S. Shestopal
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

The extensive and intensive development of information and digital technologies in the globalization's context of international relations and the differentiation of social interaction determines the transformation of the traditional (from the point of view of classical understanding) society into an innovative model of the information society. In the centre of modern socio-cultural discourse, the information society is a new form of organizing social interaction based on the broad integrative use of digital technologies; and socio-economic relations in their development are focused on the production, processing, storage, and sale of information resources in all their diversity. In turn, the worldwide (primarily covering developed and post-industrial countries) trend of informatization and digital transformation of social relations predetermines changes in the field of private and public legal relations arising because of the establishing contracts and execution of documents using electronic (digital) signatures. The development of digital information technologies, in contrast to the analogue methods of recording, storing, systematizing and transmitting information that has existed for millennia, which actively began in the middle of the 20th century, has a qualitative impact on many social relations connected with the economy, management, medicine, politics, education, and other areas (Yakoviyk et al., 2019).

In its most general form, an electronic (digital) signature is the means (tools) for fixing intentions regarding legal relations arising shortly, the authenticity of the author of this signature and confirmation of the fact of a formalized document, included or executed in electronic form.

2. Problem Statement

The unification and diversification of socio-economic interaction between the countries of this region is taking place within the focus of intensive integration processes concentrated on implementing various types of transactions in digital form, which actualizes the need for the use of special means of fixing the will of participants in civil law relations. Adaptive legal regulation of electronic document management and the associated use of electronic signatures accompany the showered trends. So, in many countries of the Asia-Pacific region, special laws have been adopted and are actively applied to regulate relations arising in connection with the use of digital identification means of established agreements.

Without claiming to a comprehensive substantive analysis of special legislative acts within the framework of this work, it seems appropriate in a comparative legal analysis of the declared institution - the institution of digital electronic signature - to dwell on the study of foreign experience in the legal regulation of the procedure and conditions for using digital electronic signatures in countries such as the United States. Australia, New Zealand, Canada, Singapore, Japan, the Republic of Korea, and the People's Republic of China.

3. Research Questions

The concept and mechanism of functioning of a digital signature:

Today, digital signatures have proven to be the most secure way to sign documents on the Internet. Unlike the original digital signature technology, modern digital signatures are easy to use and can be created

https://doi.org/10.15405/epsbs.2022.06.93
Corresponding Author: Sergey S. Shestopal
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

using any computer with an Internet connection. In practice, legislation and legal science, there is no common understanding of a digital signature. In its most general form, a digital signature is a method, process, technology that allows you to attach certain information in the electronic form to other information in electronic form, to identify the signer and establish his connection with the document.

Typically, the digital signature process involves three algorithms:

Key generation - the computer code provides a private crypto key along with its corresponding public key.

Signing - the algorithm produces a signature upon entering the private key and the message to be signed.

Verification is an algorithm for verifying the authenticity of a message, a necessary condition for matching the signature codes and the public key.

The digital signature process requires that the signature generated by both the fixed message and the private key can then be authenticated with the accompanying public key. Using these cryptographic algorithms, a user's signature cannot be reproduced without access to his private key. A secure channel is usually not required. Using asymmetric cryptography techniques, the digital signature process prevents several common attacks when a hacker tries to gain access using the following attack methods.

The digital signature must ensure complete confidentiality, while the signing process must be convenient and secure. Digital signatures are generated and verified using the Digital Signature Algorithm (DSA). DSA allows an entity to authenticate the integrity of the signed data and the identity of the signer. Since a digital signature can only be generated by an authorized person using their private key, the corresponding public key can be used by anyone to verify the signature. Each signer has its own paired public (known to the general public) and private (known only to the user) keys.

General characteristics of the regulatory framework for the use of digital signatures (on the example of Singapore, Japan, the People's Republic of China and South Korea)

Singapore passed the Electronic Transactions Act back in 1998, providing the legal basis for electronic signatures and contracts concluded electronically. Subsequently, the state signed the UN Convention "On the Use of Electronic Communications" of November 23, 2005, which led to changes in national legislation and the adoption in 2010 of a new Law on Electronic Transactions (Electronic Transactions Act, 2010).

The implementation of the provisions of the UN Convention (2005), setting new standards for national legislation in the field of electronic commerce, allowed the national legislator to solve several pressing problems. First of all, the limits of the legal regulation of e-commerce were clearly defined through the conclusion of electronic contracts, the rights and obligations of the parties were determined, the security procedure (including digital signatures) and authentication were fixed. In addition, the problem was resolved regarding the use of electronic documents in the public sector, since public authorities were able to accept electronic applications and documents signed with an electronic signature (The Electronic Transactions Act, 2010). The law was adopted to facilitate electronic communication and electronic commerce through the use of secure electronic signatures, as well as to improve electronic document management in the field of government, establish uniform rules, regulations and standards for the

https://doi.org/10.15405/epsbs.2022.06.93
Corresponding Author: Sergey S. Shestopal
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

authentication and integrity of electronic signatures and minimize the risks of abuse and fraud in the use of electronic signatures.

The Singaporean legislator discloses the concept of an electronic signature through a method (electronic or otherwise) that is used to identify a person and show the intention of that person regarding the information in the corresponding record. A secure electronic signature means such an electronic signature that is unique for a specific person, allows to identify this person, was created by a method or using means under the exclusive control of the person using it, and is associated with an electronic record. Thus, the electronic signature is based on the concept of electronic records, which relate to each other as general and specific. Under Art. 2 of this law, an electronic record is a record created, transmitted, received or stored by electronic means in an information system or for transfer from one information system to another.

In Japan, back in 2000, the Law Concerning Electronic Signatures and Certification Services was accepted. The regulatory goal of this regulatory legal act is to promote the dissemination of information using electronic methods and methods of information processing by ensuring the unhindered use of electronic signatures, which, according to the Japanese legislator, will contribute to improving the quality of life of citizens and the rational development of the national economy. Legislation and enforcement of the digital signature institution are based on the presumption of the authenticity of electromagnetic records (legal authenticity) and an accreditation clause about the assigned certification services. Under Art. 2 of this law, the term "electronic signature" means a measure taken concerning information that can be introduced in an electromagnetic record (that is, any record that is created using electronic, magnetic or any other means not recognized by the natural function of perception, and is used to process computer data), provided that such a measure makes it possible to identify the person who created it, as well as to state changes in the information. The presumption of the authenticity of an electromagnetic record means that information is authentic if an electronic signature is performed by the principal regarding the information presented in the electromagnetic record (Law Concerning Electronic Signatures and Certification Services, 2000).

The Republic of Korea has two special laws - the Digital Signature Act (1999) and the Framework Act on Electronic Documents and Transactions (2002) - regulating relations regarding the use of digital signatures in signing the relevant documents.

According to Korean law, a written signature (traditional signature) is not required when concluding a contract, since contracts signed with an electronic signature have the same legal force as contracts signed by oneself. In this case, it does not matter in what form the agreement was reached between the parties regarding the use of an electronic signature. The Digital Signatures Act 1999 and the Electronic Documents and Transactions Act 2000 explicitly state that contracts cannot be unenforceable just because they are concluded electronically.

By Art. 2 of the Law on Digital Signature, an electronic (digital) signature is “a piece of information in electronic form that is attached to an electronic document or logically combined with it to identify the signatory and verify that the electronic document was signed by the specified signer” (Digital Signature Act, 1999, p. 2).

https://doi.org/10.15405/epsbs.2022.06.93
Corresponding Author: Sergey S. Shestopal
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

According to the Digital Signature Law, there are two types of electronic signatures: a certified electronic signature and an uncertified electronic signature. A valid certified electronic signature is a signature based on a public key certificate that meets the following requirements: the key for creating an electronic signature must be owned and known only by the signer; the signer must control and manage the key at the time of signing; it should be possible to determine whether there have been any changes in the electronic signature since the moment of its provision; it should be possible to determine whether any changes have been made to the electronic document since the date of the electronic signature. A certified electronic signature can be used when signing personnel documents (for example, an employment contract, documents on benefits), commercial documents, documents on opening current accounts, documents that determine the mode of use of the real estate, copyright licenses (Digital Signature Act, 1999.).

The experience of legal regulation of the use of digital signatures in the People's Republic of China (PRC), where trade transactions and business interactions are carried out in a remote format on an unprecedented scale, is no less interesting. Thus, in 2005, the country adopted the Electronic Signature Law of the People's Republic of China (2005), aimed at standardizing acts of electronic standardization, confirming the legal force of electronic signatures and protecting the rights and legitimate concerns of interested parties.

This law defines an electronic signature as data in the electronic form contained in a corresponding message (that is, any information that was created, sent, received or stored using electronic, optical, magnetic or similar means) and which allows to identify of the signatory and recognize the content of messages. The law provides the concept of an electronic signature and other functional and operational definitions (Articles 2, 3, 35), conditions for the use of an electronic signature (Articles 3-7), requirements for the reliability of an electronic signature (Article 8), requirements regarding the addressee (Articles 9-12), the conditions for the reliability of the electronic signature (Articles 13-14), electronic verification services (Articles 15-20), grounds for legal liability for compromising the electronic signature (Articles 29-33).

According to the Digital Signature Law, there are two types of electronic signatures: a certified electronic signature and an uncertified electronic signature. A valid certified electronic signature is a signature based on a public key certificate that meets the following requirements: the key for creating an electronic signature must be owned and known only by the signer; the signer must control and manage the key at the time of signing; it should be possible to determine whether there have been any changes in the electronic signature since the moment of its provision; it should be possible to determine whether any changes have been made to the electronic document since the date of the electronic signature. A certified electronic signature can be used when signing personnel documents (for example, an employment contract, documents on benefits), commercial documents, documents on opening current accounts, documents that determine the mode of use of the real estate, copyright licenses.

The experience of legal regulation of the use of digital signatures in the People's Republic of China (PRC), where trade transactions and business interactions are carried out in a remote format on an unprecedented scale, is no less interesting. Thus, in 2005, the country adopted the Electronic Signature Law of the People's Republic of China (2005), aimed at standardizing acts of electronic standardization,

https://doi.org/10.15405/epsbs.2022.06.93
Corresponding Author: Sergey S. Shestopal
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

confirming the legal force of electronic signature and protecting the rights and legitimate concerns of interested parties.

This law defines an electronic signature as data in the electronic form contained in a corresponding message (that is, any information that was created, sent, received or stored using electronic, optical, magnetic or similar means) and which allows to identify of the signatory and recognize the content of messages. The law provides the concept of an electronic signature and other functional and operational definitions (Articles 2, 3, 35), conditions for the use of an electronic signature (Articles 3-7), requirements for the reliability of an electronic signature (Article 8), requirements regarding the addressee (Articles 9-12), the conditions for the reliability of the electronic signature (Articles 13-14), electronic verification services (Articles 15-20), grounds for legal liability for compromising the electronic signature (Articles 29-33).

4. Purpose of the Study

The main aim of the study is a comparative legal analysis of the special laws of eight countries of the Asia-Pacific region in the field of electronic document management, regulating relations related to the use of digital signatures in various fields.

The Legal Comparative Analysis focuses on the following regulations: Electronic Transactions Law of Singapore 2010 (2010), Electronic Signatures and Certification Services Law of Japan 2000 (eSignature Legality in Japan, 2020), Digital Signature Law of the Republic of Korea 1999 (Digital Signature Act, 2001) and People's Republic of China Electronic Signature Law (Electronic Signature Law of the People's Republic of China, 2005).

5. Research Methods

The article uses methods such as analysis (the concept of "digital signature" as an object of research is divided into components, which are considered from different sides in legal science and the legislation of individual states, which makes it possible to single out individual signs of this phenomenon), synthesis (this method is reflected in the development of a common definition of "digital signature" by combining the signs of the phenomenon identified during the analysis), a formal juridical method that allows analysing national regulatory documents governing relations in using digital signatures; the comparative-legal method is expressed in the comparative ratio of the rules on digital signatures to identify distinctive and specific features.

6. Findings

Conceptual and legal understanding of the notion of "digital signature".

In modern legal science, there are different approaches regarding what a digital signature is. The study of different theoretical and legal views regarding the understanding of the functional, social and legal essence of a digital signature allows us to propose different approaches to constructing a definition of this phenomenon.

Within the framework of the first approach (conditionally it can be designated as "functional"), a

https://doi.org/10.15405/epsbs.2022.06.93
Corresponding Author: Sergey S. Shestopal
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

digital signature is a tool for the legal identification of a person about document authentication. Providing a digital signature means creating a digital identifier for a signer who has an electronic signature certificate issued by an authorized body. The certificate reflects information about the person himself who has such a signature (for example, last name, first name, place of work, date of issue, validity period). Within the framework of this approach, a digital signature is considered as a formal legal attribute of a legal fact, focused on achieving certain goals:

- the signature proves the connection of a specific signer with a specific signed document;
- the need to digitally sign a document emphasizes the signer's attention to its content and its legal implications;
- generates legal consequences for persons who signed a document with an electronic signature, which predetermines the emergence of certain legal relations;
- ease of use of electronic signatures and simplification of electronic document management; ensures the integrity of the document (Chowbe, 2010).

In the focus of the second approach (with a certain degree of convention, it can be designated as "informational" or "technical"), a digital signature is considered as a technology that ensures both the safety of the message itself and the binding to the person (the holder of the digital signature). This technology is based on open-key cryptography, which is an asymmetric scheme in which a pair of keys is used for encryption: a public key, which encrypts the data, and the corresponding secret key for decryption. In this approach, a digital signature is a technique in which mathematical symbols are used to verify the integrity and authenticity of relevant documents (Pial, 2020).

The third approach allows us to investigate the digital signature as a legal phenomenon. In this aspect, a digital signature is a tool, the use of which is regulated by national legislation. It is at the national level that special laws are in place that determines the requirements for the proper use of a digital signature, key concepts, and the limits of the use of this tool.

Selected legal aspects of regulating the use of digital signatures (on the example of Singapore, Japan, the People's Republic of China and South Korea)

Using electronic signatures was legalized in Japan in 2000, with the adoption of The Electronic Signatures and Certification Business Act (eSignature Legality in Japan, 2020.). In the law enforcement aspect, the electronic signature is actively used, for example, when drafting and submitting documents within the framework of administration, trade (commercial) agreements between legal entities, documents on opening bank accounts, as well as when concluding transactions on the use of real estate (for example, a purchase agreement), sales, lease) and drafting agreements on transferring IP addresses. There are still certain areas in which the use of electronic signatures is not allowed. For example, in Japan, certain legal processes directly require handwritten signatures or wet ink seals (hanko). Japanese traditional seals - inkan (or hanko) - are personalized seals that are used every day as an identity card. Most Japanese people have several Inkan seals for different purposes. Such seals are used in preparing official notarial certifications under the Civil Code, the Law on the Lease of Land and Buildings, and the Law on the Voluntary Trusteeship Agreement. However, while the use of personal and corporate seals is a major obstacle to the digitalization of business and the simplification of “テレワーク” (teleworking, as a work from home is called in Japan), it does not reduce the process of digital integration and unification. On the contrary, state

https://doi.org/10.15405/epsbs.2022.06.93
Corresponding Author: Sergey S. Shestopal
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

authorities publish requirements for receiving targeted support to ensure the availability of online applications and acceptance of electronic submissions (Gehrke, 2020).

Korean law does not allow the electronic signature of documents on the transfer of real estate (except for a lease agreement and some other agreements that are allowed by law), contracts providing for the transfer of intangible goods (in particular, the assignment of patent or copyright) and documents on the pledge, registration of marriage, will and articles of association (Rytova, 2019).

Not without interest, it will be noted that in these acts there is a presumption of equal legal force of an agreement signed by a simply written signature (traditional signature) and an electronic signature. However, in some cases, the legislator allows the possibility of challenging such acts, since there are reasonable doubts about the authenticity of the expression of will and the reality of legal relations. Thus, Korean law (the 1999 Digital Signature Law and the 2000 Electronic Documents and Transactions Law) regulate that in exceptional cases, to prove the validity of the contract and the legal relationship that has arisen between the parties, the parties must present evidence in court. Special entities managing digital transactions may provide electronic records that are admissible as evidence by article 2020 of the Civil Procedure Law and article 308 of the Criminal Procedure Law, to confirm the existence, authenticity and validity of the concluded contract (eSignature Legality in South Korea, 2020).

Separately, it is worth to note, the differences in the legal content of the legal definition of a digital signature.

An electronic signature is widely defined in Singapore law. There, the electronic signature is disclosed through a method that is used to identify a person and determine (fix) its intention to confirm the legal fact of the prepared document.

The Japanese legislator also associates an electronic signature with a specific person; through this tool, an individual is identified when performing a legal action. In Japanese law, a digital signature is disclosed through the measure, used with respect to the information. Such information can be written on an electromagnetic record, which can only be processed through a computer. Note, an electromagnetic recording is treated as any recording that is created using electronic, magnetic or any other means that are not recognized by the natural function of perception. Thus, the national legislator of Japan creates a legal space for qualifying other means (except for electronic and magnetic) used to identify a person regarding recorded information as a digital signature.

In some aspects, the Chinese experience of legal regulation of this instrument is similar to the Japanese approach to legislative consolidation of digital signatures. The fact is that both Chinese and Japanese lawmakers agree that the information underlying a digital signature can have different sources, methods of generation and transmission. And, if the Japanese legislator focuses on electronic, magnetic and any other means that are not recognized by the natural function of perception, then the Chinese legislator defines four ways of reflecting such information (electronic, optical, magnetic or similar means).

It should be noted that the legal regulation of the use of a digital signature in civil legal relations is largely due to the action in the society of special that reflects and reveals a legitimate interest in the system of social relations (Oleinykov et al., 2019). These predetermine the vector of development of legal policy, stimulate the legislative function and simulate the legal formula of social compromise in the legislation (Pial,2020). The action of special dominants is to a certain extent interconnected with the intensive

https://doi.org/10.15405/epsbs.2022.06.93
Corresponding Author: Sergey S. Shestopal
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

development and widespread dissemination of information and communication technologies, making possible the simplification of performing legal actions through the use of innovations in the information and digital environment. Thus, there is a digital modernization of social interaction in legal contracts, which ipso facto reduces legal transaction costs and simplifies the legal formalization of civil relations (Lobach, et al., 2021).

7. Conclusion

Analysis of foreign experience in the legal regulation of relations arising in connection with electronic document flow and the use of digital signatures allows us to state a general trend at the national level of several states in the Asia-Pacific region, manifested in the widespread use of special means of electronic authentication of persons and their intentions regarding assurance (confirmation) of the concluded contracts. Despite the different definitions of an electronic signature, which are normatively reflected in special legal acts, a general approach can be distinguished in the legal understanding of this phenomenon. In particular, an electronic signature is determined by entering special information (electronic key) into an electronic document; which allows identifying the owner of the electronic signature; an electronic signature is used as a digital instrument for confirming the will and intention of the parties. A unified approach to the legal understanding of the content of an electronic signature will make it possible to ensure the rights and legitimate interests of all participants more effectively in the electronic document flow, and the improvement of mechanisms for protecting digital data will ensure the safety of this process both at the national and international levels.

Acknowledgments

This paper is a research report carried out under a grant of the President of the Russian Federation No. NSh-2668-2020.6 "National-cultural and digital trends in the socio-economic and political-legal development of the Russian Federation in the XXI century"**Error! Bookmark not defined.**.

References

Chowbe, V. Sh. (2010). Digital Signature: Nature & Scope Under the IT Act, 2000 - Some Reflections. *SSRN Electronic Journal, 2*(1), 201-203.

Digital Signature Act 1999. Amended by Act No. 6360, 16 January 2001 (2001). https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=102472#0000

Electronic Signature Law of the People's Republic of China. (2005). *WIPO.* https://wipolex.wipo.int/en/text/182409

Electronic Transactions Act. (2010). *IMDA*. https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/Acts-Regulations/Electronic-Transactions-Act.pdf?la=en

eSignature Legality in Japan. (2020). DocuSign. – 2020. https://www.docusign.com/how-it-works/legality/global/japan

eSignature Legality in South Korea. (2020). DocuSign. https://www.docusign.com/how-it-works/legality/global/south-korea

Framework Act on Electronic Documents and Transactions of 2002 (2002). *Korean Law Information Center*.

https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=2&query=Framework+Act+on+Electronic+Documents+and+Transactions&section=lawNm&y=38&x=39

Gehrke, N. (2020). Electronic Signatures in Japan. *Explore new perspectives*. https://medium.com/tokyo-fintech/electronic-signatures-in-japan-ee8a2cca1c97

Law Concerning Electronic Signatures and Certification Services. (2000). Docplayer.net. https://docplayer.net/12490944-Law-concerning-electronic-signatures-and-certification-services-unofficial-translation.html

Lobach, D. V. Shestopal, S. S., & Smirnova, E. A. (2021). International Cyberterrorism counteraction within the context of intensive development of information and communication technologies. *LaplageemRevista (International), 7*(3), 200-209. https://laplageemrevista.editorialaar.com/index.php/lpg1/article/view/1286/1150

Oleinykov, S. N., Mamychev, A. Yu., & Shestopal, S. S. (2019). The Factors of Impact on Content and Dynamics of Legislation Evolution. *Humanities & Social Sciences Reviews,* (6), 123-130. https://core.ac.uk/download/pdf/268005622.pdf

Pial, H. R. (2020). Digital Signature Understanding How It Works and Importance. Digital Signature Understanding. FSI: Digital Investigation, (38), 178-186. https://www.researchgate.net/publication/344818547_Digital_Signature_Understanding_How_it_Works_and_Importance

Rytova, N. S. (2019). The fourth industrial revolution as a factor of economic development: a comparative international aspect. *Innovations and investments, 4,* 360-362. https://cyberleninka.ru/article/n/chetvertaya-promyshlennaya-revolyutsiya-kak-faktor-ekonomicheskogo-razvitiya-sravnitelno-mezhdunarodnyy-aspekt

The Electronic Transactions Act (Cap. 88). (2010). IMDA. https://www.imda.gov.sg/regulations-and-licensing-listing/electronic-transactions-act-and-regulations

Yakoviyk, I. V., Baranov, P. P., Shestopal, S. S., & Pokhodzilo, Y. N. (2019). The legal-theoretical issues of the state sovereignty in the globalization. *Opción, 34*(87-2), 369.