ATLANTIS PRESS

Advances in Economics, Business and Management Research, volume 105

1st International Scientific and Practical Conference on Digital Economy (ISCDE 2019)

Regulating criminal liability for violations related to the use of digital signatures in the context of the digitalization of the economy

Grebenkov A. A.
Southwest State University
Kursk, Russia
grebenkov@gmail.com

Sinyaeva M. I.
Southwest State University
Kursk, Russia
mari_sinyaeva@mail.ru

Polyanskaya S.S.
Southwest State University
Kursk, Russia
sveta.sveta1295@yandex.ru

***Abstract* — The legal framework regulating the use of digital signature is one of the necessary conditions for the introduction of electronic document management, which is a required step to ensure the functioning of the digital economy. Currently, a qualified digital signature, the certificate for which is issued by an accredited certifying center, is a full replacement of the handwritten signature. However, in modern Russian practice, there are cases when qualified digital signature is issued and used illegally, for real estate fraud, registering companies, which are subsequently used as "one-day" fronts for carrying out fraudulent encashment and money laundering operations, commercial fraud and tax evasion. Legislature takes measures for prevention of the illegal actions connected with use of electronic signatures, however to be efficient, such actions must be reinforced with establishment of a criminal liability for illegal actions related to the use of digital signatures. In view of this, the authors give reasons for the criminalization of the following acts by the employee of the accredited certifying center: negligence with regard to proper identification of applicants, creation and distribution of digital signature certificates to unauthorized persons, and also acquiring or using digital signature certificates by unauthorized person. This will allow for a greater degree of protection of economic relations in the context of their digitization.**

Keywords — digital signature electronic document management, criminalization, fraud, tax evasion, criminal law.

I. INTRODUCTION

With the digitalization of the economy in modern Russia, the use of digital signature tools within the framework of electronic document management is becoming increasingly important [1]. In particular, the widespread use of electronic signature is required by efforts to create a "digital government" in Russia [2]. Currently, the possibility of using digital signature is recognized by legal professionals and regulated by legal acts, in particular the Federal Law dated 06.04.2011 No. 63-FZ "On digital signature" [3].

This regulatory act provides for the use of three types of digital signatures:

1) simple digital signature is created without the use of cryptographic tools. This type of digital signature has no special protection from forgery and is therefore used mainly in the internal document circulation, or for remote service of individual customers, generally along with other means of identification.

2) unqualified electronic signature is created using cryptographic tools. The technology of encryption with public and private keys is used, which allows verifying the digital signature to prove that the following conditions are met: the document has not changed since the signing and the document is signed by a person who has access to the private key certificate (which has to be kept secret) corresponding to the public key [4]. However, there is a "weak link" in this scheme: one must somehow make sure that the public key used to verify the signature is issued by the counterparty who signed the document [5]. Therefore, this type of signature can be used in document exchange only when parties negotiate an additional agreement, which determines the procedure for exchanging public keys, ensuring necessary precautions [6]. Because of that, the unqualified signature is mainly used in economic relations between corporations, including cross-border document exchange.

3) qualified digital signature (QDS) also uses encryption technology with public and private keys, however, it uses the government-controlled infrastructure for confirming ownership of public keys. QDS uses encryption and hashing algorithms certified by Russian Federal Security Services — FSB (in particular, GOST R 34.10-2012 [7]), and the issuance of certificates of qualified digital signatures is carried out only by a certification center that is accredited by the Russian Federation Ministry of Communications [8].

An electronic document signed by QDS is legally equivalent to a paper document signed with a handwritten signature and can be used in any legal relationship. Documents signed by the QDS are accepted by all government agencies, as well as notaries, and can be used as a legal basis for various acts, including, but not limited to, registration of real estate, corporation and so on [9].

QDS can be issued to corporations and individual entrepreneurs, as well as to individuals who do not have any special legal status.

An important research task is to identify possible threats to the normal order of economic and other social relations associated with the possibility of using QDS instead of a handwritten signature, and to develop ways to counter these threats, for example, by criminalizing common ways to abuse digital signatures.

II. METHODOLOGY

The main research method used is a general philosophical method of materialistic dialectic. Authors also use specific methods of legal research, such as system-structural and formal-legal analysis, methods of comparative law and other methods of analyzing legal documents and situations.

To identify common threats related to use of QDS in document circulations, we use the method of content analysis of media publications and published acts of legal practice, as well as the method of case-study.

III. RESULTS

There were several well-known cases of improper persons obtaining and using QDS by to commit illegal actions.

For example, in early 2019, a resident of Moscow discovered that in the receipt for the payment of utility bills for the apartment that he inherited, the payer suddenly changed. He tried to investigate the matter, and it was found out that his apartment was gifted to a resident of Ufa. The contract which was detailing the agreement, was accepted by the Rosreestr as a basis for changing the entry in the state register of real estate information, making a donee the legal owner of real estate. The identity and will of both sides of the contract was confirmed by a qualified digital signature.

However, neither the former owner of the apartment, nor its new owner, according to information received from them, did not contact the certification centers for issuing the QDS, and did not know anything about the transaction [10].

An investigation into this situation has not yet been completed, but three options are most likely:

1. Fake documents containing the personal information of the apartment owner and the person who subsequently received it under the gift agreement were submitted to the certification center. At the same time, the persons who carried out illegal operations with the apartment impersonated the persons in whose name the CEP certificates were issued. There is no fault of the employees of the certification center in this situation, since they had reason to consider the persons who contacted them subjects of relevant personal data.
2. There was a conspiracy between persons who intended to carry out illegal transactions with real estate, and employees of the certification center, who issued the QDS certificate without carrying out a full-fledged identification procedure.
3. The certification center did not ensure compliance with the proper procedure for issuing QDS certificates, which includes examining the applicant's passport and other identification documents, and confirming his authority. Proper identification procedure allows to prevent the issuance of the certificate to an improper person. In particular, some certification centers issue QDS remotely without personal contact of the applicant with the employee of the certification center, and without following proper procedure for verifying the applicant's identity (for example, using unsigned digital copies of identification documents).

The possibility of the latter option was experimentally confirmed by journalists: they were able to obtain the QDS for the general director of their newspaper using only public data from government registers and scanned copies documents (passports and social security numbers), to which they pasted their photos using image editing software. The certification center swiftly accepted the forged documents without undertaking even the most basic procedures to assess their validity and confirm that the claimant is really the person in whose name the QDS certificates are issued [11].

There are many cases in which corporations are registered using the certificates obtained by the above methods. These corporations are then used for fraudulent cashing and money laundering operations, and also used as "one-day" firms for commercial fraud and tax evasion [12].

The relevance of these threats was noted at the level of government authorities. Federal Law dated 02.08.2019 No. 286-ФЗ "On Amendments to the Federal Law "On State Registration of Real Estate" established that the implementation of registration actions for the alienation of real estate on the basis of documents signed by the QDS is possible only under the condition that the applicant, his legal representative or agent acting on the basis of a notarized proxy directly or by using means of postal service previously provided corresponding written statement paper with proper handwritten signature, with the exception of QDS issued by Rosreestr [13].

Also, members of the Federation Council V.K. Kravchenko, L.N. Glebovoy, M.N. Ponomarev pledged to introduce legislation intended to strengthen the control over the operation of certifying centers (draft law No. 747528-7 «On amending certain legislative acts of the Russian Federation in connection with improving regulation in the field of electronic signature»). As of October 2019, this draft law is to be presented before the State Duma in first reading. This bill contains the following main provisions:

- general rules for issuing QDS certificates and the usage of QDS by individuals, corporations and individual entrepreneurs remain the same, however, additional requirements are set for the issuance and usage of QDS certificates for authorities, their officials and notaries;
- requirements for certification centers are stricter, in particular, bill provides for much larger financial guarantees, and also includes regulations detailing the creation of government supervisory authorities in the field of issuing QDS;
- it is established that the applicant's remote identification (without his personal presence) is carried

out only using information technologies that allow him to be identified without reasonable doubt, such as using another valid QDS certificate to sign electronic copies of identification documents, or using biometric identification systems.

In general, these changes are aimed at counteracting the threats outlined above, but some provisions are controversial, in particular, the norm that forbids any participants of electronic interactions to restrictions on the recognition of QDS. Bill proposes to allow only restrictions that are explicitly included in Federal Law dated 06.04.2011 No. 63-FZ "On digital signature". In fact, the adoption of this provision without additional clarification (which are absent in the draft) will mean that the procedure for carrying out registration actions for the alienation of real estate on the basis of documents signed by the QDS provided by the Federal Law of 02.08.2019 No. 286-ФЗ is disavowed.

This bill is at the stage of discussion and amendment, however, taking into account the approval and support expressed by the Government of the Russian Federation and the relevant committees of the State Duma, it can be expected that it will be adopted during the autumn session of the State Duma.

IV. Discussion

Based on the above, the following major threats related to the misuse of electronic digital signatures, which can be countered with criminal law, can be identified.

First, there are criminal acts, in which a certificate of QDS issued to a certain person is used to impersonate this person without his or her knowledge of that person. Among the examples of such crimes are:

1. Fraud (p. 1-4 art. 159 of the Russian Criminal Code), including commercial fraud (p. 5-7 art. 159 of the Russian Criminal Code) and fraud in the sphere of crediting (art. 159.1 of the Russian Criminal Code). The elements of this crime will be present if the criminal (criminals) carry out the conclusion of deals for the alienation of property or property rights, or the conclusion of other deals with property on behalf of the person to whose name a certificate of QDS is issued, with no intention to fulfill obligations on these transactions. The main constituent sign of this act is deception, which manifests in the fact that the fraudster impersonates another person authorized to make the relevant transactions [14]. In this case, property damage is caused to a bona fide counterparty in a transaction that expects to acquire property legally or to receive other compensation in exchange for the funds provided. Damage may also be caused to the rightful owner of the alienated property if, as a result of a fraudulent operation, state registration of the transfer of rights takes place.

If we are talking about fraud committed by a person using his official position, concerning the valuable property (valued higher than 250 thousand rubles or more than 3 million rubles, if it is a commercial fraud) or especially valuable property (valued higher than 1 million and 12 million rubles, respectively), or committed by an organized group, or associated with deprivation of citizen's right to housing, it is considered a grave crime, which means that preparation for a crime is also punishable by law. Preparation can include any action directed at ensuring the possibility of committing crime sometime in future, including any actions directed at obtaining certificates of QDS (collusion with an employee of the certification center, or actually getting the certificate of QDS, etc.). The commission of a phoney deal to transfer property or property rights to an unauthorized person in order to complicate the subsequent recovery of property by the legal owner can also be considered the preparation for crime.

The attempt to commit a crime, that is, any attempt to use the QDS certificate to certify the documents required to obtain property or property rights, can also be punished.

2. Theft (art. 158 of Russian Criminal Code). The QDS certificate issued to the owner of property without his knowledge can be used to alienate this property in favor of the guilty or third parties. Unlike fraud, the victim of which will be a bona fide acquirer who believes that he is dealing with the legal owner of the property, here the beneficiary is a person who is aware of the illegal nature of the transfer of property and who participates in this scheme for profit.

3. Illegal formation (creation, reorganization) of corporation (art. 173.1 of the Russian Criminal Code). The crime here is the formation (creation, reorganization) of a corporation through a figurehead, as well as the submission of documents to the state organ performing registration of corporations and individual entrepreneurs that entailed the inclusion of information on figureheads in the Unified state register of corporations and entrepreneurs. The term ‘figureheads’ here can mean ‘persons whose data was entered into the Unified state register without their knowledge’. It should be noted that in this case only the actual use of the QDS to submit documents to the registration authorities on behalf of the nominee is punishable. Obtaining the QDS certificate for these purposes, which constitutes preparation for the crime, remains unpunishable, because even the aggravated crime of this kind is just a crime of moderate severity.

4. Legalization (laundering) of money or other property acquired by criminal means (art. 174, art. 174.1 of the Russian Criminal Code), evasion of taxes, fees payable by the organization, and (or) insurance premiums payable an organization that pays insurance premiums (art. 199 of the Russian Criminal Code) and other crimes which are committed by performing commercial operations with corporations registered using the QDS certificates obtained without the knowledge of the person for whom it was issued. In this case, the QDS is also used for the execution of transactions and other financial operations on behalf of the legal entity.

Secondly, criminal law must be used to counter actions aimed at illegally obtaining and using QDS certificate, which acts as an official document granting rights. Under the current wording of criminal law, such actions are punishable only as preparation for a crime or criminal attempt. But other similar actions, such as forging a passport or acquiring a fake passport of a citizen of the Russian Federation in order to commit the same crimes entails criminal liability under Art. 327 of the Criminal Code, and this responsibility is independent of

responsibility for theft or other crime. Indeed, according to par. 7 of Resolution of the Plenum of the Supreme Court of Russia of November 30, 2017 No 48 "About court practice on cases of fraud and embezzlement", theft or illegal acquisition of the rights to property by deception or abuse of trust, committed using an official document forged by criminal, requires additional qualification in accordance with p. 1 of art. 327 of the Criminal Code of the Russian Federation. There are grounds for establishing liability for obtaining a QDS certificate for a third party without the knowledge of that person, since it is in fact similar to the forgery of official identity document.

Thirdly, criminal law must be used to punish the actions of the employee of the certification center that illegally issued the QDS certificate. These actions can be either intentional in the case of conspiracy with the person receiving the certificate, or constitute an improper performance of official duties related to the identification of the applicant due to frivolous or careless attitude to the possible consequences. In the first case, they can be considered as aiding in the commission of a crime. However, it must be established that the employee of the certification center was aware of the nature of the act that the person receiving the certificate intended to commit. Such actions by an employee of the certification center will constitute aiding in the commission of the specified crime committed using the official position, so there is no need for independent criminalization of such actions. In the second situation, at present, no measures of criminal liability can be applied to such an employee, as the only norm that is similar is negligence of government official (art. 293 of the Criminal Code of the Russian Federation), but the employee of certification center (commercial organization) is not a government official.

These employees are not liable under Art. 201, 204 of the Criminal Code of Russia, as they are not executives or top managers in a commercial organization, which is required by these articles.

It should be noted that bill No. 747528-7 stipulates that the employee of the accredited certification center should also bear criminal liability, but do not detail the crimes that these employees should be liable for.

V. CONCLUSION

We can conclude that existing provisions of criminal law aimed at countering threats associated with the illegal use of digital signatures, should be considered insufficient and do not satisfy the requirements of legal practice.

Identified defects of criminal law can be addressed by criminalizing the following acts.

- improper performance of official duties related to the identification of the applicant by the employee of accredited certification center due to frivolous or careless attitude to the possible consequences as a result of an unfair or careless attitude to the service or duties in office, if this has caused major damage or substantial violation of the rights and legitimate interests of citizens or organizations, or the interests of society or the state that are protected by law. Aggravating circumstances of this act may include the infliction of especially large damage, as well as other grave consequences, including the deprivation of a citizen's right to a housing. The punishment for this crime should be the same as provided by art. 293 of the Criminal Code of Russian Federation.
- the creation and issuance of digital signature certificate to unauthorized person by an employee of an accredited certifying center. The punishment for this act must correspond to the punishment for forging a citizen's passport, for which responsibility is provided by p. 2 of art. 327 of the Criminal Code of Russian Federation.
- obtaining or using digital signature of another person without authorization. The punishment for this act must correspond to the punishment for illegal acquisition or use of a citizen's passport, the responsibility for which is provided for in p. 3 of art. 327 of the Criminal Code of Russian Federation.

The establishment of these measures of responsibility will ensure the proper protection of commercial and other relations which require the use digital signatures in a digitalized economy.

References

[1] S. A. Vdovin, E. V. Ubozhenko, E. I. Lobanova, "Formation of development strategies of the digital economy in Russia: review, experience, prospects," Econ.: Yesterday, Today and Tomorrow ["Opyt, problemy i perspektivy strategij razvitiya cifrovoj ekonomiki v Rossii i za rubezhom," Ekonomika: vchera, segodnya, zavtra], vol. 9, pp. 573-582, 2019.

[2] Iu. V. Irkhin, "'Electronic government' and society: world realities and Russia (a comparative analysis)," Sociol. Res., vol. 46, pp. 77-92, 08 December 2007.

[3] L. Garifova, "The economy of the digital epoch in Russia: development tendencies and place in business," Proc. Econ. Financ., vol. 15, pp. 1159-1164, 2014.

[4] S. J. Aki, "Digital signatures: a tutorial survey," Computer, vol. 16, pp. 15-24, February 1983.

[5] W. E. Lupton, "The digital signature: your identity by the numbers," Rich. J. Law Tech., vol. 6, Fall 1999.

[6] S. E. Bluthe, "Digital signature law of the United Nations, European Union, United Kingdom and Untied States: promotion of growth in e-commerce with enhanced security," Rich. J. Law Tech., vol. 11, 2005.

[7] A. Beresneva, A. Epishkina, O. Isupova, K. Kogos, M. Shimkiv, "Special digital signature schemes based on GOST R 34.10-2012," 2016 IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference, pp. 135-140, 2016.

[8] A. A. Chesnokova, I. V. Kalutskiy, A. G. Spevakov, "Electronic document management: the safety stages of implementation and operation," Proc. Southwest State Univ.: Control, Comp. Eng., Inform. Sci., Med. Ins. Eng. ["Elektronnyj dokumentooborot: bezopasnost' na etapah vnedreniya i ekspluatacii," Izvestiya YUZGU: Upravlenie, vychislitel'naya tekhnika, informatika, medicinskoe priborostroenie], vol. 7, pp. 13-23, 2017.

[9] A. O. Inshakova, I. A. Goncharov, V. E. Smirenskaya, V. V. Dolinskaya, "Modern communication technologies in notification of notarial actions in Russia," J. Adv. Res. Law Econ., vol. 8, pp. 2144-2151, Winter 2017.

[10] A. Rassokhin, “Electronic signature left a man without an apartment” [Online], Kommersant [“Elektronnaya podpis' ostavila bez kvartiry”], 16 May 2019, URL: https://www.kommersant.ru/doc/3969174.

[11] Yu. Gilmshina, “We sell under the electronic key the government, merchants, apartments. Fast, easy, cheap” [Online], 47News [“Prodayom pod elektronnyj klyuch pravitel'stvo, kommersantov, kvartiry. Bystro, legko, deshevo”], 20 May 2019, URL: https://47news.ru/articles/156549.

[12] A. Khabibrakhimov, “Open firms to withdraw money and take microloans: why fraudsters steal electronic signatures and how to protect yourself” [Online], Vc.ru [“Otkryvayut firmy dlya vyvoda deneg i berut mikrozajmy: dlya chego moshenniki kradut elektronnye podpisi i kak zashchitit' sebya”], 9 August 2019, URL: https://vc.ru/legal/74802-otkryvayut-firmy-dlya-vyvoda-deneg-i-berut-mikrozaymy-dlya-chego-moshenniki-kradut-elektronnye-podpisi-i-kak-zashchitit-sebya.

[13] L. Sarimova, “Selling an apartment without leaving home — digital signature not to save from a visit to Rosreestr” [Online], Realnoe Vremya, 15 August 2019, URL: https://realnoevremya.com/articles/3748-baw-on-digital-signature-comes-into-force-in-russia.

[14] Yu. B. Tubanova, K. M. Timokhin, “Risks of using electronic signatures and measures to minimize them”, Tax Pol. Pract. [“Riski pri ispol'zovanii elektronnoj podpisi i mery po ih minimizacii,” Nalogovaya politika i praktika], vol. 6, pp. 68-73, 2019.