USE OF DOCUMENTS SIGNED BY DIGITAL SIGNATURE IN THE CIVIL PROCESS

Alexey V. Bilalov[1]
Ivan I. Korolev[2]

[1] Faculty of Law, Kazan Federal University. E-mail: bilalov.alex@yandex.ru
[1] Faculty of Law, Kazan Federal University. E-mail: IIKorolev@kpfu.ru

ABSTRACT

This paper analyzes the use in civil proceedings of documents signed with digital signatures. Information technologies for their implementation in legal proceedings must meet high criteria of reliability and security. The paper analyzes the regulatory framework governing the use of digital signatures. There are the following types of digital signatures: simple digital and enhanced digital signatures. Also, there are distinguished an enhanced non-qualified digital signature and an enhanced qualified digital signature. A simple digital is a signature that confirms the fact that the digital signature has been generated by a specific person through the use of codes, passwords or other means.

Keywords: digital signature, document, civil procedure, proof.

1.INTRODUCTION

The list of evidence on electronic media and their legal nature are among the controversial issues of the civil procedural law doctrine. This is primarily due to the inevitably rapid development of information technologies, the variety of electronic evidence types, a differentiated approach to the regulation of means of proof in procedural codes, debatable legal nature of evidence carried by electronic media, etc.

Electronic technology and communication means have become part of the material basis used by the judiciary. Thousands of employees and objects of information are involved in the implementation of the automated system Justice; a whole stratum of procedural relations that requires a scientific definition and a regulatory settlement has been formed. [Nakhova, 2018].

Of particular interest is the category of electronic evidence.

The regulatory framework governing the use of electronic documents in circulation consists of the following acts: Federal Law dated April 6, 2011 No. 63-FZ On digital signature, Resolution of the Government of the Russian Federation dated November 28, 2011 No. 976 On the federal executive body authorized in the use of digital signatures, Orders of the Federal Security Service of Russia dated December 27, 2011, No. 796 On Approving Requirements for Digital Signature Means and Requirements for Certifying Center Means and No. 795 On Approving Requirements for the Form of a Qualified Certificate of a Digital Signature Verification Key. Since January 1,

2017, changes that regulate in detail the scope of electronic documents application in courts have been entered into force.

In Great Britain, the digital signature regulates a large number of acts. The meaning of a document is set forth in Section 13 of the 1995 Law on Civil Evidence as everything where information of any description is recorded. The same definition is provided in 20D (3) of the 1970 Tax Administration Act. This definition appears to include a very old form of document that conforms to adhere.

2.METHODS

This study analyzes the work of both Russian and foreign experts in civil proceedings, as well as on electronic technology. Analyzed are the works of Russian scientists on this issue. It also examines the work of foreign scientists (Stephen Mason, Daniel Sen, Uwe Rasmussen), US and UK legislation, and European experience presented by EU directives. Great importance for writing this work was played by the fourth edition of Electronic Evidence [Kirillov, 2018] sponsored by Stephen Mason and Daniel Sen.

3.RESULTS AND DISCUSSION

A digital signature is an information in electronic form that is attached to other information in electronic form (signed information) or otherwise associated with such information, and which is used to identify the person signing the information.

There are the following types of digital signatures: simple digital and enhanced digital signatures. There are also distinguished an enhanced non-qualified (encrypted non-certified) digital signature (hereinafter - non-qualified digital signature) and an enhanced qualified (encrypted certified) digital signature (hereinafter - qualified digital signature).

A simple digital signature is a signature that, through the use of codes, passwords or other means, confirms the fact that the digital signature has been created by a certain person.

Non-qualified digital is a signature that: is obtained as a result of a cryptographic transformation of information using a digital signature key. It allows the person who signed the electronic document to identify, and also to detect the fact of making changes to the electronic document after its signing. A non-qualified digital signature is created using digital signature tools.

Qualified digital is a signature that matches all the characteristics of a non-qualified digital signature and the following additional characteristics: the key for verifying the digital signature is specified in a qualified certificate; those means are used to create and verify digital signatures, that have received confirmation of compliance with the requirements established in accordance with the Federal Law On Digital signature. When using a non-qualified digital signature, a digital signature verification key certificate may not be created if the compliance of the digital signature with the characteristics of the non-qualified digital signature can be provided without using the digital signature verification key certificate (Article 5 of the Act). [Smolensky, 2018]

Also interesting is the example: is it possible to sign a statement containing the testimony of a witness, with a digital signature, so that the witness may not appear in court. This case was reviewed by a District Judge Jenkinson in the Fitzpatrick County.

The applicants filed a claim for damages. The defence was that the collision between vehicles was too weak to cause injury. In addition, a dispute arose regarding the number of people in the applicants' vehicle. The court issued an imperative ruling in relation to disclosing information along with the imperative ruling that applicants should file testimony explaining which documents were missing. When sending the applications, the defendants noted obvious discrepancies in the signatures. After the inquiry, it turned out that the signatures were digital signatures using a method known as Echosign. The defendant submitted that the applicants had failed to comply with the imperative ruling. The defendant made it on the grounds that the testimony of the witnesses had not been properly signed. The defendant argued that the very definition of the witness statement included the personal signature of the witness. CPR 32.4 (1) of the act states: (1) ... A testimony is a written testimony *signed by some person* and containing evidence that this person would be allowed to give orally.

The defendant argued that the requirement that the statement should be signed by a person cancels the more general rule stated in UK CPR 5.3:

If any of these Rules or any other Practice Direction requires the signing of a document, this requirement is met if the signature is printed using a computer or other mechanical means.

The 2015 commentaries discuss the question of what a document is, noting that:

The question of what a document is and what it is not for some purpose is not free from doubt. There are many documents that must be signed in accordance with the provisions of the CPR. They include the following... statements of truth (corroborating statements in the case; statements from witnesses, and statements in the case). [Stephen, 2009]

The district judge has ruled that the digital signature of the testimony complied with the rules.

The judge postponed the decision for a while and then stated:

(1) The starting point was CPR 5.3 which states that the digital signature is sufficient.

(2) The next question was whether the witness statement has been a document.

(3) There is no definition in the rules, but in the notes, to CPR 5.3 a statement of a witness is referred to as a document. The judge indicated to himself that this is an Editorial Comment.

(4) The next question was whether the specific wording of CPR 32.4 (1) was moved to CPR 5.3.

(5) As a general principle, it was recognized that specific wording replaces the general rule.

(6) The rule went that a statement of a witness must be signed by a person.

(7) The question was whether the words signed by a person are displaced in accordance with paragraph 5.3.

(8) The defendant argued that achievement of the main goal has led to such significant factors which determine why the rule should be interpreted as requiring a personal signature to achieve the main goal.

(9) However, if the authors of the rule wanted the testimony of witnesses to replace the general provisions, the rule could state this directly and clearly indicate that the testimonies of witnesses are an exception.

(10) The system used by the applicants had the means to track them. There is an equal opportunity for a handwritten signature to be false.

(11) At a time when the need for compliance is of paramount importance, the fact of a digital signature is appropriate. This in itself facilitated the use of digital signatures.

(12) If a digital signature of testimony is a widespread problem, the solution is to contact the Rules Committee.

Thus, in the UK it is possible to use a digital signature to certify testimony.

4.CONCLUSIONS

Public documents, such as birth and death registers, baptism and marriage registers, acts of parliament, royal proclamations, resolutions of the Council, statutory tools and journals of any house of parliament, can be proved as proof by simply making an appropriate copy stamped where appropriate. Proof of their performance is also not required. But the court requires for proof of registration of a private document if its proper storage lasts no more than 20 years.

Thus, Regulation No. 910/2014 of the European Parliament dated July 23, 2014, 3.75 Section 7 (1) of the Law provides for the admissibility of a digital signature in two ways: 7 (1) [Mason, 2018]:

(a) A digital signature included or logically associated with a specific electronic message or specific electronic data.

(b) The assurance by any person of such a signature, which must be admissible as evidence in relation to any matter relating to the authenticity of the communication.

To date, it does not appear that complex electronic documents are subject to legal proceedings. This does not mean that electronic documents are disputed because they are in electronic form. It is doubtful that any judge would willingly hear the false argument of a lawyer who claims that documents in electronic form are not allowed. Current legislation clearly stipulates the possibility of the use of digital documents, although in practice digital documents are not always accepted by courts at the present time. Some examples are given below:

(i) The Companies Act 2006 provides for the submission of electronic documents: Section 1146 provides for the authentication of documents in printed and electronic form; Section 1168 provides for printed and electronic copies of documents; Part 4 of Annex 4 provides that the document or information are correctly sent or provided to the company, if they are sent or provided in electronic form in accordance with this clause.

It seems that in the future, with the further development of electronic means of interaction between business entities, their direct participation in court hearings will be significantly reduced. It will be due to the need to establish certain circumstances of the cases related to verifying the validity of a particular person's will, investigation of evidence, during which additional explanations are needed both from those who submitted them and from experts (specialists) on the results of their investigation.

REFERENCES

1. Nakhova E.A. (2018). Problems of electronic evidence application in civil procedure and administrative proceedings // Law.2018. No. 4. Pp. 81 - 90.
2. Kirillov A.E. (2018). Procedural foundations of e-justice // Bulletin of the civil process. 2018. N 1. Pp. 220-228.
3. Smolensky I.N. (2018). Identification of a person (the subject of the arbitration process) in electronic justice // Bulletin of the civil process. 2018. No. 1. P. 248 - 255.

4. Stephen M. (2009). 'Electronic evidence and the meaning of 'original'' Amicus Curiae. The Journal of the Society for Advanced Legal Studies Issue 79 Autumn 2009 26–28.
5. Mason, S. (2018). Documents signed or executed with electronic signatures in English law. Computer Law & Security Review, 34(4), 933–945.doi:10.1016/j.clsr.2018.05.023