Approaches Determining the Applicable Law Using Internet Technologies in the Digital Economy

K. K. Taran(✉)

Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs, Moscow, Russia
taran.kira@yndex.ru

Abstract. In the era of intensive development and growth of information technologies, new legal norms controlling legal relations when using new Internet technologies are formed. Moreover, digitization of economic relations accelerates the civilian turnover, and transactions are made much faster and more convenient for the parties. The forms of interaction between foreign counterparties are changing. The study considers current approaches that are used in Russia, the United States and the EU countries to determine the applicable law to legal relations when using the Internet. The author highlights restrictions on the choice of the applicable law in the states under consideration. On the basis of the studied approaches, their advantages and disadvantages, we can assume further trends in the norms of private international law.

Keywords: Conflict of laws · Legal relations on the Internet · International private law and the Internet · Internet technologies · User rights

1 Introduction

Relationships that develop on the Internet are often cross-border in nature. This is explained, firstly, by the fact that the parties to the contract may belong to different states, and, secondly, the server that serves the Internet resource may be located in the third state or in neutral space, and in this connection there will be difficulties in determining the nationality of the server (for example, if the server is located in space on a private satellite or on an abandoned ship in neutral waters). Also, taking into account the change in information transfer, it is difficult to determine its initial and final source. The implementation of the state's ability to subordinate websites to its rule of law, which can be accessed from the territory of this state, is not always effective, and can cause both legal uncertainty and lead to unfair legal consequences.

Digitization of the economic turnover and cross-border transactions need to revise and improve the rules of private international law. Classical conflict rules adapt to new legal relationships, but we need to know how effective they are. The study considers approaches of Russia, the United States and the EU countries, which have a number of similarities and differences related both to the development of the legal system of states and the introduction of Internet technologies.

S. I. Ashmarina et al. (Eds.): ISCDTE 2019, LNNS 84, pp. 622–629, 2020.
https://doi.org/10.1007/978-3-030-27015-5_74

Collision bindings that determine the applicable law to the contract concluded on the Internet, if such the right is not determined by the parties themselves, should help determine the rule of law that is most associated with relevant legal relations and suggests a suitable and most fair regulatory mechanism.

2 Methodology

In the course of the study, the author used the following general scientific methods: analysis - the study of key components of legal relations to determine the applicable law to legal relations when using Internet technologies; inductive and deductive methods; modeling methods and others. Special methods were also used: a comparative legal method for comparing approaches to the definition of the applicable law to legal relations when using Internet technologies in Russia, the United States and the EU, which made it possible to identify regulatory features of these states; logical and legal methods; methods of systematic interpretation of legal norms; synergistic method; systematization; and etc.

3 Results

The study will consider only the issues determining the applicable law to legal relations, despite the fact that the definition of judicial jurisdiction is very closely related to this issue.

Relations on the Internet can be divided into two groups: (1) Relations that are made through the Internet, i.e. which can be implemented without the Internet, for example, to conclude a contract of sale. The structure and characteristics of such relationships undergo changes (the type, time of receipt of the offer and acceptance, time of conclusion of the contract, and other issues), but the essence and purpose of legal relationship remains unchanged. An example would be legal relations in the field of e-commerce. (2) Relations that cannot be realized without the Internet. This group can include relations when using cloud storage of information, downloading music and other files from the Internet, and so on. Often legal relations on the Internet imply the transfer of information to the server/s, where it is not excluded that it is transferred (sorted) to another server.

Due to the fact that legal norms regulating relations, which can be implemented using the Internet, are only being formed, new legal relations are emerging, and the possibility of applying legal norms by analogy cannot be excluded.

The Civil Code of the Russian Federation and the EU Regulation Rome 1 allow the parties to independently choose the applicable law [1, 4]. It is assumed that this right will be applicable to the entire contract, and not to its specific part, including relations when using Internet technologies. In particular, this approach is peculiar to the United States, where legal relations can often be brought under the jurisdiction of a certain state and under the law of that state. In the US, attempts were made to summarize legal relations arising and implemented on the Internet under the principle of territoriality: the administration of the Attorney General of Minnesota in the mid-1990s was asked to

subordinate disputes arising in cases of violations of criminal and civil law when people know that information will be distributed including through the state of Minnesota [6].

Russia and the EU use a similar approach: if all elements of legal relations are located in another country than the one whose right is chosen, the choice of the parties should not prejudice the provisions of the law of this other country, which are not allowed to retreat by agreement.

However, this free approach to the choice of the law has its own limitations: in Russia and the EU countries legal mechanisms are used to counter the circumvention of the law, requirements for compliance with the norms of direct application and non-contradiction to the rules of public law and order. In the United States, the chosen applicable law to contracts in which the consumer is a party must have a substantial connection with the contract. In Russia and the EU countries there are no requirements that the choice of the applicable law by the parties should be based on the substantial connection of the contract with the chosen law.

In all the legal procedures under consideration, the chosen applicable law cannot conflict with the rules of judicial jurisdiction.

In determining the applicable law in most countries, the status of the parties is taken into account. That is, if legal relations are formed between a merchant and a consumer, then legal mechanisms will be used that provide the greatest protection to the weaker consumer.

Article 6 of the EU Regulation Rome 1 [4] enshrines the application of the law of the country of the consumer's residence. Moreover, it is prohibited to reduce the level of consumer protection in the absence of the applicable law. This implies that, for example, in the case of a contract for downloading music or software, the relationship took place in the country of the consumer's residence, that is, the site offered to enter into an agreement, and the site should be active (i.e., to function in the territory given state and have feedback with the consumer).

Russia also has a special regulation of legal relations to which the consumer is a party, namely Art. 1212 of the Civil Code of the Russian Federation [1] guarantees compliance with peremptory norms of law aimed at protecting the consumer's rights. Russian law permits the choice of the applicable law to a contract to which the consumer is a party, however, if such a right is not chosen and if circumstances are established by the Civil Code of the Russian Federation, the law of the country of the consumer's residence is applied.

In the US, the situation is different: the official documents establish that the law chosen by the parties cannot be applied if its application contradicts the fundamental order of the state, which has substantially more interest than the right of the chosen state in relation to a particular issue; this right would also be applied if there is no choice of the parties. The US approach is interesting because it determines in advance that a particular state has an interest in a particular legal relationship in order to determine whether the law of that state will be applied. Judicial practice in cases involving consumers in the United States is very diverse. The law of the EU countries, on the contrary, chooses the applicable law to the contract, with the exception of provisions that harm the consumer.

In the US, legal relations on the creation/development of computer information, transactions related to computer programs, Internet contracts, data processing transactions, etc. are governed by the Uniform Computer Information Transactions Act 2000 (English UCITA, adopted in only two states: Maryland and Virginia). This law also allows the parties to choose the applicable law, with the exception of the provisions that relate to the consumer [7].

Despite the fact that conflict rights to consumer relations are fairly developed, difficulties may arise when it is not possible to determine the place of residence/location of the consumer, as he can make a transaction in one state, transfer funds from the accounts of the bank that is located in another state, and he himself moved to the third state - the place of the transaction.

In the EU Regulation Rome 1, as well as in Russian legislation, the applicable law is generally determined according to the law of residence of the party performing decisive execution under an agreement; in other cases the principle of the closest connection is used.

The EU Regulation Rome 2 [3] establishes legal approaches to the definition of the applicable law, to non-contractual obligations. The provisions of the EU Regulation Rome 2 also have many similarities with the regulation in Russia.

The Russian Federation is characterized by the approaches lex loci damni (the law of the place of harm) and lex loci delicti commissi (the law of the place of the unlawful action). Such approaches are used in the European Union: the first is common in many states; the second is rarely used. These approaches are enshrined in the Civil Code of the Russian Federation in Art. 1219: obligations arising from caused harm, the law of the country where the action or other circumstance took place that served as the basis for the claim for damages; if harm occurred in another country, the law of that country could be applied, if the injurer foresaw or should have foreseen the occurrence of harm in that country [1].

Taking into account the peculiarities of information transmission via the Internet, the place of committing unlawful actions that may cause adverse consequences will be considered the place where information is entered into the network. If we take as an example cloud storage of information, then information can be uploaded to the cloud storage, which will not be malicious or will not contain a virus, but entering it can reduce the value of the stored information (this can be fraudulent actions and actions aimed at causing harm to the party), for example, the substitution of data regarding concluded contracts and the order of obligations, the substitution of data associated with the invention, leveling its novelty. And the location of the server through which information is transmitted will not be considered the place of unlawful actions that may cause adverse consequences for the party (then, for example, if the virus is downloaded to the cloud storage, the law of the state from which the virus was downloaded will be applied). However, there are significant difficulties in determining where to download information, as the offender may use various programs that hide the place of loading, or download information from the territory of the state where the issue is not settled or insufficiently resolved. To solve this problem, it is possible to shift the downloading information/virus to the affected party while justifying their requirements, then this side has the advantage of choosing the most convenient material right. In this case, there will be a dilemma before the violator: continue to hide information about the place of

downloading information, which may be beneficial for the affected party, or record and submit to the court the place of downloading the malicious program.

Such an approach is interesting and quite convenient for the parties and the court, but taking into account the scientific and technological progress, it may not be possible to establish the loading site. It may be practical in case of violation of the user's rights by a cloud company or another person to resort to the presumption used in Swiss law. It indicates the coincidence of the usual location of the offender's administrative center (or residence, if it is an individual) with the place of entry data to the network. But this presumption also does not exclude the deliberate choice of the place of the tort. And the choice is very difficult.

As for binding at the place of occurrence of harm, in this case there are difficulties concerning the parties: (1) A company operating on the Internet must foresee the possibility of such situations, the result of its actions and the possible effect in countries; (2) A user may face the consequences not in the country of citizenship/domicile, but in another state (since many technologies are cross-border). Such an approach implies a high level of responsibility of companies that operate on the Internet, for ensuring a high level of security for the user, but it is difficult for practical application, despite the fact that binding at the place of occurrence of harm is quite widely used.

When a virus is infected with data, the applicable law will usually be determined by the location of damaged databases and software.

In determining the applicable law, it is still necessary to consider what consequences the offender wanted. If the goal was data destruction and hacking, then the right of the place where the data owner is located should be applied. If the purpose of the offender was to obtain data for maintaining unfair competition and obtaining benefits, then in accordance with Art. 1222 of the Civil Code of the Russian Federation to obligations arising from unfair competition, the law of the country whose market is affected or may be affected by such competition is applied. However, Art. 1223.1 of the Civil Code of the Russian Federation, after committing an act or other circumstance that entailed harm or unjust enrichment, allows choosing the applicable law by the parties, but if all the circumstances relating to relations of the parties are connected with one country, the choice of the applicable law should not affect the imperative norms of this country. In the EU as a whole, a similar approach is used [1].

When determining the applicable law in transferring information, this is unlikely to be crucial in the event of a legal dispute, since this process is instantaneous.

It is necessary to pay attention to the fact that Art. 1219 of the Civil Code of the Russian Federation also indicates the possibility of applying the law, to which the parties have subordinated the contract, in case it was concluded by the parties in carrying out business activities [1].

Russian companies that offer a cloud storage service usually specify in their agreements with users the applicable law is the law of the Russian Federation, and the courts authorized to consider the dispute are the courts of the Russian Federation.

In the US, there is a slightly different tendency associated with the determination of the applicable law: the law largely depends on which court will be recognized as authorized to consider the dispute. In the USA, a number of approaches and presumptions are used, which allow, first of all, subordinating the proceedings in the case to US courts, which later may also have an impact on the definition of the applicable

law. In the USA, the following approaches are used both individually and in combination, if the parties have not chosen the applicable law and, if the party is not a consumer.

- The place of conclusion of the contract. For example, in the case of Bodreau v. Scitex the court determined that the law of the State of Massachusetts is applicable, as e-mails about the contract were received in this state.
- The "best" right for a legal relationship.
- The public interest approach.
- The law of the place of execution.
- Minimum contact test (long arm rule).
- Purposeful submission (or the goal criterion). The courts in Europe are much less likely to apply this criterion compared to US courts, and they mainly use criteria related to the harmfulness of the act and the place of its occurrence. The goal criterion may soon be included in the legal system of the Russian Federation, which may be very promising for the development of the judicial system.
- Theory of loading and unloading information.
- Location of data processing and storage center. In the United States, the definition of the applicable law will also vary depending on the location of the data processing center and the location of the user. For example, if the data center of an American company of the relevant specialization is located in Singapore, then for a user from Australia, the applicable law will be Singapore's law, and Singapore's courts will have exclusive authority to deal with disputes between a user from Australia and a US company. If the user lives in the United States, then the applicable law will be the law of the United States, and the relevant courts of the given state will consider the dispute [4, 8].
- The place of operation. This criterion is preferred by companies that have a presence in different countries.

The European Union Regulation (EC) 2016/679 [5] has expanded its rights in the field of personal data processing, i.e. it is applied to the processing of personal data at the place of business, regardless of whether processing is carried out in the union or not. The conflict rules discussed indicate a closer approximation of conflict rules of the Russian Federation and the EU countries in determining the applicable law to legal relations when using Internet technologies. The US approaches are of great interest both for Russia and for the EU, since they began developing legal regulation of Internet technologies earlier than in other states, therefore these approaches are more diverse. But despite this there is no established practice that should be guided in most cases.

4 Discussion

The Russian and EU countries' approaches have much in common, the structure of conflict-of-law regulation largely coincides, new conflict-of-laws rules to resolve situations when the parties have not chosen the applicable law to the contract are underway.

In Europe, according to Czigler [2], greater attention is paid to commercial situations where the consumer is a party to a contract. And since most of transactions on the Internet are carried out by consumers, the rules of law on consumer protection will be guiding principles for determining the jurisdiction of the court and the applicable law. Moreover, when concluding a contract, the consumer should take into account both the activity/passivity of the site in the state (the passivity of the site does not prevent the consumer from contacting the company if he wants to place an order), as well as all circumstances related to the contract: advertising the company's offer with worldwide delivery, place of conclusion of the contract, location of the parties, place of the computer from which the transaction was made; place of payment, place of breach of contract, etc.

In the United States, an integrated approach is used, in which various collision bindings can be used and all the circumstances of a particular legal relationship are taken into account.

Svantesson (USA) [6] believes that in order to develop new legal norms in the field of private international law, it is necessary first of all to rethink the classical and established norms, since the current changes are a slight deviation from the well-established approaches. In fact, the regulation of relations when using Internet technologies is proceeding very slowly.

In the Russian Federation, adapting legal norms to new legal relations is under way. The Digital Code is being developed, which will probably lead to a whole new level of regulation of legal relations when using Internet technologies.

5 Conclusion

Legislation of different states regulates differently legal relations when using Internet technologies. In the event of a dispute, the parties have the advantage of choosing the state with the most advantageous material and procedural rules for court proceedings taking into account the future place of recognition and enforcement of the decision court. This possibility of choosing the law suggests the need to create a model law, which would include the procedural, material and conflict-of-law regulation of relations when using Internet technologies. Perhaps the best option for the most effective regulation of legal relations on the Internet, the definition of the applicable law would be to create a multilateral model convention that would reinforce dominant approaches of states. Most likely, such a document will be created, and the states will be able to come to a common denominator, as the relations arising when using Internet technologies are the same in most states.

Acknowledgements. The research was conducted by the authors with the financial support of the Russian Foundation for Basic Research, Project no. 19-011-20091.

References

1. Civil Code of the Russian Federation. Part 3rd no. 146, adopted on 26 November 2001. http://www.consultant.ru/document/cons_doc_LAW_34154/. Accessed 3 June 2019. (in Russian)
2. Czigler, T.D.: Choice-of-law in the internet age-US and European rules. Acta Juridica Hungarica **53**(3), 193–203 (2012). https://doi.org/10.1556/AJur.53.2012.3.2
3. Regulation (EC) No. 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007R0864&from=enU.C.C. Accessed 3 June 2019
4. Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008R0593&from=EN. Accessed 3 June 2019
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679. Accessed 19 June 2019
6. Svantesson, D.J.B.: Jurisdictional issues and the internet – a brief overview 2.0. Comput. Law Secur. Rev. **34**(4), 715–722 (2018). https://doi.org/10.1016/j.clsr.2018.05.004
7. Uniform computer information transactions act. https://www.steptoe.com/images/content/1/4/v1/1468/2359.pdf. Accessed 3 June 2019
8. Vincent, M., Hart, N., Morton, K.: Cloud computing contracts white paper a survey of terms and conditions. Truman Hoyle (2011). https://ficpi.org.au/articles/White_Paper_June2011.pdf. Accessed 19 June 2019