BIG DATA AS THE SUBJECT OF A TRANSACTION IN CIVIL TURNOVER UNDER THE LAW OF THE RUSSIAN FEDERATION

BIG DATA COMO OBJETO DE UNA TRANSACCIÓN EN VOLUMEN DE NEGOCIOS CIVIL BAJO LA LEY DE LA FEDERACIÓN RUSA

Artur G. Kravchenko[1]*; Aleksey I. Ovchinnikov[2]; Anna P. Rabets[3]; Sergey S. Chekulaev[4].

1. Far Eastern Federal University, Russia. kravchenko_artur@mail.ru
2. South Federal University, Russia. k_fp3@mail.ru
3. Far Eastern Federal University, Russia. rabets.ap@dvfu.ru
4. Far Eastern Federal University, Russia. chekulaev_ss@dvfu.ru

*corresponding author:Artur G. Kravchenko email: kravchenko_artur@mail.ru

ABSTRACT

The article aims to investigate the issues concerning the definition of the big data concept, as well as the problem of civil turnover of big data in the legislation of the Russian Federation. Approaches to this definition enshrined in doctrinal legal acts and investigated in the legal literature are analyzed. The features and peculiarities of big data are considered. The conclusion about the need to legislate the basic categories in the field of big data to clarify the place of this object in the system of objects of civil rights is made. The study has also analyzed the risks of including big data in civil law turnover. Given the results, substantially practical approaches to regulating civilized forms of big data circulation should be the established mechanisms of civil liability for the use of big data that have resulted in derogation or limitation of the rights of citizens.

Keywords: big data; objects of civil rights; digital assets; intellectual property; information.

Revista de Investigaciones Universidad del Quindío,
34(S3), 256-264; 2022.
ISSN: 1794-631X e-ISSN: 2500-5782

RESUMEN

El artículo tiene como objetivo investigar las cuestiones relativas a la definición del concepto de big data, así como el problema de la transferencia civil de big data en la legislación de la Federación Rusa. Se analizan aproximaciones a esta definición consagradas en actos jurídicos doctrinales, así como investigadas en la literatura jurídica. Se consideran las características y peculiaridades de los grandes datos. Se concluye sobre la necesidad de legislar las categorías básicas en el campo del big data con el fin de aclarar el lugar de este objeto en el sistema de objetos de derechos civiles. El estudio también ha analizado los riesgos de la inclusión de big data en la facturación del derecho civil. Dados los resultados, un enfoque sustancialmente efectivo para regular las formas civilizadas de circulación de big data deberían ser los mecanismos establecidos de responsabilidad civil por el uso de big data que ha resultado en la derogación o limitación de los derechos de los ciudadanos.

Palabras clave: grandes datos; objetos de los derechos civiles; recursos digitales; propiedad intelectual; información.

INTRODUCTION

Among most important government tasks in the digital economy era is to create a legal regime to ensure the effectiveness of the system for collecting, processing, storing and providing reliable and relevant information to data consumers (the state, businesses and citizens). Technologies such as blockchain, neural networks, smart cities, and Internet of Things are developing through the collection and analysis of system (big) data. In addition, the "big data" technology can be effectively used in the management of intellectual property, in health care, and in other areas thus significantly increasing the economic efficiency of human activities. Therefore, both unstructured "big data" and the results of their processing often become the subject of civil law transactions.

According to expert estimates, at the end of 2019 the data market in Russia was estimated at 45 billion roubles, and by 2024 it will grow to 100 billion roubles (Popkova & Sergi, 2020). Therefore, information corporations and industrial companies are investing heavily in this technology.

At first sight, "big data" is an effective tool for ensuring biological security of the population during pandemics period (Chudinovskikh & Sevryugin, 2019), information predictive security for corporations, effective regulation of road traffic, etc. At the same time, the practice of using "big data" raises a lot of questions both in terms of restricting competition (Hilbert, 2016), information security, and observance of property and personal non-property rights of citizens. For example, the results of "big data" processing are used for targeting the advertising (determining consumer preferences); in fact, they provide reliable data on legally protected information.

In particular, the collection and subsequent analysis of consumer preferences affect the rights to privacy and family life; they also violate medical confidentiality, the secrecy of correspondence, and others. Using both documented and undocumented capabilities of Internet assistants, developers of software based on "Big Data" technology actually perform a total surveillance of a user, and the processed results of this surveillance become the subject of transactions. At the same time, the format of big data collection can be different, which does not reduce the potential risks of violation

of civil public and state interests. For example, camera data allows to identify the personnel of closed institutions, to assess their security system (e.g. banks), to conduct automated analysis of digital traces in the Internet of the user, they also allow to establish with high probability the race, sex, political views, biological state (disease, pregnancy, mania, phobias, etc. (Petrenko, 2018). At the same time, the technology of depersonalization embedded in the legislation of many countries is not an absolute barrier to the effective use of personal data. Automated analytical processing of the "big data" by neural networks allows the restoration of personal attachments to initially depersonalized subjects due to a unique combination of information. For example, databases storing depersonalized readings of tracker bracelets recording both geodata and biological states of a person (heart rate, blood pressure, step frequency, temporal activity, ECG) allow with high probability to detect and define a specific person and conduct effective untraceable observation of him/her. Moreover, a number of precedents suggest the possibility of a big date to use for "analytical hacking" of state secrets (Hilbert, 2016).

On the other hand, the needs of a digital infrastructure increasingly dependent on "big data" are objectively growing, reinforcing the contradictions between the legal concept of personal data protection and the economic need for its non-destructive use. In particular, the validity of interpretive processing results is highly dependent on the mass collection of big data. For example, the correct management of public transport requires maximum coverage of passenger geodata. The more users prohibit the use of geodata to maintain a smart city, the greater will be the error in the public transport management. At the same time, the problem concerning the technological overcoming of the personal data legal protection system grows. Meanwhile, this contradiction increasingly brings the classical legislative concept of absolute protection of personal data to a nonplus. The problem in the state regulation of big data technologies lies in the tossing of legislators and civil society between the minimization of excessive legislative barriers and restrictions in the digital ecosystem and the growing need for personal data protection" (Popkova & Sergi, 2020). The very definition of "big data" in its legal meaning also deserves a separate question.

The multidimensionality and complexity of the "big data" concept are pointed out by both domestic and foreign researchers describing the concept as a set of information on the activities of subjects of the digital economy, and the results of their processing as the identification of "unidentified patterns, relationships, behaviour patterns, trends, identities, and practical knowledge" (Schneider, 2018).

In Russian law, the concept of "big data" can only be derived from doctrinal legal acts. Thus, it follows from the content of subparagraph "k" of paragraph 4 included in the Strategy for the Information Society Development in Russia for 2017-2030 approved by Presidential Decree No. 203 dated May 9, 2017, that big data is structured and unstructured information coming from a large number of different, including disparate or weakly connected, information sources (Sidorenko & von Arx, 2020).

Analysing the above definition, we highlight the following features of big data.

Firstly, big data is a huge amount of information continuously coming from a variety of sources. At the same time, this volume of information is not static, that is, it is constantly increasing. The criterion of "huge volume" is the objective impossibility to process an array of data in a reasonable period of time (a time interval during which the result of such processing would not lose its meaning and value).

Secondly, this information is not single-format, representing both structured and unstructured data. Structured (processed) data refers to ordered information contained, for example, in information

systems. Unstructured data is information contained in audio and video recordings, as well as representing data from social networks, servers, satellite images, etc.

In the meanwhile, big data can also be considered as a digital technology used to collect, accumulate, store and process data (Iasechko et al., 2020).

In turn, the doctrine notes that from a technical point of view, big data is seen as a new technology used to collect, accumulate, store and process data (Kalinina et al., 2019).

Thus, big data is a multidimensional category, including the information itself, as well as methods of its collection, processing, storage and analysing, requiring special algorithms and software tools to use.

It should be noted that on February 14, 2020, the Ministry of Digital Development, Communications and Mass Media of the Russian Federation (Ministry of Communications) has posted on the federal portal of the draft federal law on the regulation of big data circulation (Popkova & Sergi, 2020). The purpose of the legislative proposal is to unify approaches to big data processing activities as well as to create legal conditions for big data to become a resource for social and economic development.

According to the said legislative proposal, big data is a set of non-personalized data classified according to group characteristics, including statistical reports, and information, data on the location of immovable and movable objects, qualitative and quantitative activities' characteristics, behavioural features of immovable and movable objects acquired from various data owners or from unstructured or structured data sources, via data collection utilizing methods and technologies of processing data, as well as technical approaches guaranteeing the consolidation of the specific data set, systematic updating, repeated utilization, the form of presentation of which doesn't mean their attribution to a specific individual (Novruzova et al., 2019).

A study of this big data definition leads to the conclusion that it mainly refers to a qualitative characteristic of information. It does not take into account the fact that big data is a type of digital technology that involves the analysis of big data with the help of special algorithms. Thus, the legislative proposal initially provided for a distinction between, on the one hand, big data as information and, on the other hand, big data processing as actions with big data, including, among other things, analysis of processed data (Zharova & Lloyd, 2018).

In addition, the reference in the definition to the "totality of non-personalized data" that does not refer to a specific individual excludes personal data from big data. This approach is not consistent with international practice. At the same time, this legislative clarification will help solve the problem of obtaining consent for the use of personal data in the processing of big data.

Other methods are used in storing and processing large quantities of information. Therefore, the issue of correlation between the concept of "big data" and the related definition of "database", which are often referred to as synonymous concepts, is quite relevant (Boltanova & Imekova, 2019).

METHODS

According to item 2, article 1260 of the Civil Code of the Russian Federation, a database is a set of

independent materials, presented in an objective form, and systematized in such a way that these materials could be found and processed by means of a computer (information legal and reference systems, databases of mobile operators, etc.). Databases are protected as objects of copyright and are considered as composite works.

Legal protection of the content of databases, which does not depend on the creative nature of its creation, is carried out according to the rules of Paragraph 5, Chapter 71 of the Civil Code of the Russian Federation "Rights related to copyrights". A database becomes an object of related rights provided that its creation (including processing or presentation of corresponding materials) requires substantial financial, material or other expenses (Hilbert, 2016).

Speaking about the relationship between the definitions under study, it can be noted that the regime of legal protection applicable to databases cannot extend to relations related to the collection, processing and storage of big data.

First of all, big data is not an object of intellectual rights.

Secondly, big data includes, in addition to structured information, a large amount of the unstructured one, and, accordingly, big data do not have the attributes of databases protected by copyright.

Third, due to the fact that many entities can simultaneously collect and store data obtained from the same public sources, the provisions of the exclusive right (monopoly of the holder of copyright or related rights) do not apply to the sphere of big data.

Summarizing the above, we can assume that the norms of the fourth part of the Civil Code of the Russian Federation on intellectual property rights cannot be applied to regulate relations in the sphere of big data, where special regulation is required. According to Clause 39 of the National Strategy for the Artificial Intelligence Development for the period until 2030, approved by Presidential Decree No. 490 dated October 10, 2019, the implementation of this Strategy requires the creation of a regulatory and legal framework to ensure the protection of data obtained during economic and scientific activities (Boltanova & Imekova, 2019).

In the legal literature, there is an opinion that big data should be classified as a type of digital assets (Chudinovskikh & Sevryugin, 2019). At the same time, the legislation regulating the legal regime of digital rights does not classify big data as a type of digital assets, primarily due to the presence in the category under study of such a generic feature as information (Fondahl et al., 2019).

Thus, the theoretical and methodological complexity of defining "big data", as well as the definition of specific restrictions and rules of civil turnover of "big data" as an object of civil rights is caused by their complex nature, which includes multidimensional information, among other things, including information subject to protection through intellectual law, contract law. On the other hand, the structure of "big data" contains fragments of information themselves not protected by the current legislation, but in the course of their systematic analytical processing, the effect of "hacking" of legally protected interests and, consequently, violation of civil rights arises. At the same time, it should be noted that limiting the circulation of "big data" may have a significant adverse economic effect, since this technology is becoming a key tool of the digital economy, opening up fundamentally new opportunities in the effective organization of society and the state.

RESULTS AND DISCUSSION

There is another opinion with regard to the legal nature of the category under study; this opinion is, in our view, of certain interest. Big data is a property complex, which includes a set of objects with different legal nature, which have a common purpose. In this case, big data as a type of property complex may include: 1) information consisting of raw data and the results of processing (including in embodied form); 2) property rights (in particular, exclusive rights to the results of intellectual activity) (Petrenko, 2018).

“Big data“ is also considered through the construct of a service, since by itself, without its analytical processing, it is of no economic interest (Schneider. 2018).

However, many experts believe that relations in the sphere of big data do not need detailed legal regulation. For example, members of the Big Data Association, which unites major corporations in this area (Megafon PJSC, Rostelecom PJSC, Sberbank PJSC, etc.) consider the introduction of a single term "big data" inexpedient, because the category of processed information is constantly changing, and the term itself serves as a kind of metaphor, which does not allow giving it a clear legal definition (Iasechko et al., 2020).

The second no less important aspect that determines the legal regime of the use of "big data" is the establishment of limits of their defensibility in civil turnover.

Obviously, for effective legal regulation, it is necessary to understand the very essence of "big data", which can be represented not only by an array of publicly available information, a set of personal data of Internet users (from a primary source), but also a complex of information collected by independent software and hardware products united by a data collection program. An example of such big data can be neural networks combining software for Internet of Things developed by different manufacturers.

To define the construction of the right regulation it seems necessary to determine: 1. Categories of "big data" allowed for free and restricted circulation; 2. "Big data" as an independent object of property rights; 3. Limits to restriction of "big data" circulation for reasons of: violation of personal non-property rights of citizens, state, investigation, commercial, personal and family secrets; violation of antitrust laws; 4. Civil rights protection framework for the person collecting "big data".

First of all, let us note that it is necessary to take into account the nature of the information contained in "big data", which may differ, in fact, only even in its name. For example, genetic information in the structure of "big data" obtained in the course of medical studies of patients (Novruzova et al., 2019), studies of natural objects, should be separated from genetic information obtained in the course of research and development of a unique sequence of genomic structures, which can be the subject of intellectual law (Kalinina et al., 2019).

Secondly, it is necessary to take into account the close relationship between Big Data and its subsequent analytical processing, which itself can create legal consequences. For example, a misinterpretation of Big Data that caused reputational costs to a corporation or an individual may also be the basis of a legal dispute aimed at protecting honour, dignity and business reputation. And it is not about the intentional infliction of moral harm by the subject who processes the data, but about the fact that "a person behaves differently depending on the situation, so it is inadmissible to use a personal data in

isolation from the context" (Chudinovskikh & Sevryugin, 2019).

Finally, there are several principles of legal protection of personal data included in the structure of "big data". First of all, these are the norms aimed at the "legal clarity" of the data, establishing the requirements for its collection and storage in the "big data" array. Thus, the paragraph b, point 1, Article 6 of Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals concerning the process of personal data and on the free movement of that kind of data concludes that they are gathered for specific, legitimate and explicit aims and not more processed in a way incompatible with these aims. More data processing for statistical, historical, or scientific objectives should not be deemed as incompatible providing that Member States provide proper safeguards. The same Directive defines the requirement of proportionality of the collection and processing of the established purposes, the reliability of the data and their completeness, the storage of the data in a personalized form only within the time necessary for the processing of the data (Popkova & Sergi, 2020).

Moreover, in addition to technical limitations to close "big data", lawmakers encounter fundamentally new properties of "big data" automated processing which allows to "uncover" information about an object, phenomenon, process, subject, that is not accessible to third parties in the usual manner. Thus, based on the unique data of digital traces (characteristic interaction with the interface, a unique profile of preferences, etc.), identification of impersonal users, tracking of their lives is possible and this information cannot be effectively legally protected (Sidorenko & von Arx, 2020).

On the other hand, the civil turnover of big data must still be limited in certain cases defined by law. For example, the circulation of personalized big data, including with the consent of the user, may have consequences that are not foreseeable for a user. For example, after consenting to the commercial circulation of their biodata, users of "smart bracelets" may suddenly discover the discriminatory policies of insurance companies. In particular, the biodata of "smart bracelets" may become the subject of a deal with insurance companies that "can use Big Data to assess the risk of developing a particular disease or getting injured" of their clients (Boltanova & Imekova, 2019). A similar situation is occurring in the banking sector, where there is virtually no civil law protection against wrongful refusal of bank credit. It is obvious that the use of "big data" by private companies in order to reduce costs and maximize profits may be associated with legal discrimination. Hence, the idea of administrative control over the circulation of "big data" is suggested as a consequence. However, in this regard, we note that not every restrictive model of the legal regime of "big data" circulation can be implemented both legally and technically, and also economically. For example, the legislative initiative on the draft law No. 571124-7 “On Amendments to the Federal Law "On Information, Information Technologies and Information Protection" was rejected namely on the grounds of the need for budgetary expenditures.

The scientific literature also raises the problem of protecting the rights of those people who carry out the formation of "big data" associated with the impossibility of recognizing their automated analytical processing with the use of creative work and the spread of the norms of intellectual property on these results. Nevertheless, currently the civil law protection of the interests of persons engaged in the collection and automated processing of "big data" is carried out through the construction of trade secrets (Shackelford, 2016; Iasechko et al., 2020), which demonstrates its effectiveness in world practice.

CONCLUSION

Thus, to summarize, it should be noted that:

Firstly, the phenomenon of "big data" as a subject of a civil law transaction, like many other digital phenomena of social relations, exists being objectively independent of the will of the legislator and the legal doctrine. Therefore, the non-recognition of "big data" (information) as an object of civil rights only forms a fertile ground for abusing contract law and legal gaps. As a consequence, the legitimate interests of participants in civil turnover suffer. On the other hand, when establishing legal regulation of "big data", it is necessary to be guided by the principle of reasonable degree of legal regulation to avoid negative economic consequences of unreasonable or disproportionate restrictions on circulation of "big data" in relation to the potential risks of civil rights violation. At the same time, considering the importance of applying the analysis results of "big data" for the state needs and the needs of business community, it is definitely necessary to legislate the basic categories in the field of big data in Federal Law No. 149-FZ dated 27.07.2006 "On Information, Information Technologies, and Information Security". We believe that this will allow eliminating ambiguity in the construction of the "big data" concept and, in the absence of such an object as information in Article 128 of the Civil Code of the Russian Federation, to determine the place of "big data" in the system of civil rights objects.

Secondly, the introduction of "big data" to the list of objects of civil rights requires a clear distinction in the civil law category of information that cannot be the subject of transactions involving commercial organizations and purposes aimed at making a profit, because the results of their processing can be used for purposes of legal discrimination.

Thirdly, controlling the circulation of big data is objectively still technically impossible or difficult to implement. Therefore, an important effective means of regulating civilized forms of "big data" circulation should be the established mechanisms of civil liability for the use of "big data" that have caused derogation or limitation of rights of citizens, as well as damage to the business reputation of digital economy participants.

ACKNOWLEDGEMENTS

The current study was carried out with the financial support of the RFBR grant No. 19-011-00820 (a) “The legal policy of the Russian State, its priorities and principles in the digital economy and the digital technological structure: conceptual, methodological, sectoral aspects of digitalization of law and legal regulation”.

REFERENCES

Boltanova, E. S., & Imekova, M. P. (2019). Genetic information in the system of objects of civil rights. Lex russica, (6), 110-121.

Chudinovskikh, M., & Sevryugin, V. (2019). Cryptocurrency regulation in the BRICS countries and the Eurasian Economic Union. BRICS law journal, 6(1), 63-81.

Fondahl, G., Filippova, V., Savvinova, A., Ivanova, A., Stammler, F., & Hoogensen Gjørv, G. (2019). Niches

of agency: Managing state-region relations through law in Russia. Space and Polity, 23(1), 49-66.
Hilbert, M. (2016). Big data for development: A review of promises and challenges. Development Policy Review, 34(1), 135-174.
Iasechko, S., Puzyrnyi, V., Puzyrna, N., Kostiuk, N., Bakhnovska, I., & Litvinova, I. (2020). The investigation of peculiarities of the occurrence of subjective civil rights in registration of a patent. J. Advanced Res. L. & Econ., 11, 844.
Kalinina, O., Alekseeva, L., Varlamova, D., Barykin, S., & Kapustina, I. (2019). Logistic approach to intellectual property. In E3S Web of Conferences (Vol. 110, p. 02103). EDP Sciences.
Novruzova, O. B., Pronina, Y. O., Shergunova, E. A., & Gorevoy, E. D. (2019, December). The contract of power supply during the era of the digital law: civil bases. In Institute of Scientific Communications Conference (pp. 553-560). Springer, Cham.
Petrenko, S. (2018). Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation (pp. 1-249). Springer International Publishing.
Popkova, E. G., & Sergi, B. S. (2020). Human capital and AI in industry 4.0. Convergence and divergence in social entrepreneurship in Russia. Journal of Intellectual Capital.
Schneider, I. (2018). Bringing the state back in: Big Data-based capitalism, disruption, and novel regulatory approaches in Europe. In The Politics of Big Data (pp. 129-175). Routledge.
Shackelford, S. J. (2016). Protecting intellectual property and privacy in the digital age: the use of national cybersecurity strategies to mitigate cyber risk. Chap. L. Rev., 19, 445.
Sidorenko, E. L., & von Arx, P. (2020). Transformation of law in the context of digitalization: Defining the correct priorities. Digital Law Journal, 1(1), 24-38.
Zharova, A., & Lloyd, I. (2018). An examination of the experience of cryptocurrency use in Russia. In search of better practice. Computer Law & Security Review, 34(6), 1300-1313.