LEGAL REGIME OF BIG DATA IN FOREIGN LEGAL ORDER

Tojiboyev Sarvar Zafarovich
Lecturer of Civil Law Department at
Tashkent State University of Law, Uzbekistan
Email: szafarovic@gmail.com

Abstract

Most states, realizing the growing importance of global digitalization, one way or another embarked on the path of legal regulation of the virtual world by defining the main institutions, their legal principles and protection mechanisms. Surely, the active development of the legal framework is also taking place in relation to Big Data, being a key link in the digital chain, however, since its inception; it has not yet acquired an adequate legal regime.

Going beyond the scope of national regulation and the need to study foreign experience in the legal regulation of the analyzed phenomenon is determined by the presence of its extraterritorial nature. The turnover of a huge amount of data goes beyond the boundaries of one country, which requires unified regulation both at the international and national levels, ignoring which leads to legal uncertainty for all participants in the market turnover and inhibition of the development of the digital economy. Therefore, instead of introducing local norms within the framework of one legal system, it should take into account the experience of international lawmaking in the area under study, using uniform provisions and include universal norms in domestic legislation. It is preferable to create effective digital legislation harmonized with the world community, otherwise, Uzbekistan risks falling out of international economic turnovers.

Keywords: *Big Data, legal regime, digitalization, foreign law, data law, database, domestic legislation, virtual world.*

The UK model of regulating Big Data

For the analysis of foreign practice, some countries have been taken that use two different legal approaches in the legal regulation of Big Data: 1) a restrictive regulation model within the framework of personal data legislation (Great Britain), 2) and a free regulation model (USA). The first country that follows the path of establishing legal regulation and introducing Big Data into the national system is the United Kingdom. Preparations for the formation of legal norms for the regulation of Big Data began in 2013, when the UK Government declared Big Data to be a key technology of critical importance for the United Kingdom[1]. Consideration of the legal regulation of this area should start with the United Kingdom Report[2] in which it was pointed out that the British legislators have the goal of amending the clarification of the legal regulation of Big Data in data protection legislation. It would reflect the general trend in the development of this area precisely within the framework of data privacy legislation, giving priority to the principle of privacy. In the absence of special rules or regulations that would directly regulate activities in the field of Big Data, the UK, today, implies an indirect approach to the legal regulation of this area through existing legislation, which in one way or another affects the use of a certain category of information.

The first category includes personal data that is governed by the General Data Protection Regulation (hereinafter GDPR)[3], as well as the Data Protection Act 2018[4], which supplements the main provisions of the GDPR and regulates areas that are outside the jurisdiction of this document (for example, national safety). Both acts quite strictly regulate the process of collecting and processing personal

[1] Bart van der Sloot, Sascha van Schendel. International and comparative legal study on Big Data // The Netherlands Scientific Council for Government Policy. P.57. URL: https://www.wrr.nl/binaries/wrr/documenten/working-papers/2016/04/28/international-and-comparative-legal-study-on-big-data/WP020-International-Comparative-Legal-Study-Big-Data.pdf

[2] Bennett Moses L;De Koker L;Mendelson D. Big Data Technology and National Security: Comparative International Perspectives on Strategy, Policy and Law – United Kingdom Report. June 2018. URL: https://www.d2dcrc.com.au/m/u/2018/08/30/uk-report-june-2018.pdf

[3] 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). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[4] Data Protection Act 2018. URL: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

data, setting high standards of protection, as well as serious sanctions for violation as of provisions prohibiting the sale or offer for sale of illegally collected personal data without the consent of the subject.

The next category of information is anonymized data. The introduction of this category of data is determined by the need to meet the needs of the subjects of information circulation, as well as its general development. However, in order to maintain a balance of interests of each stakeholder in the era of Big Data, anonymized data was classified into two groups: 1) anonymized data and 2) pseudonymized data. The first group includes data that suggest such a degree of depersonalization, in which it is impossible to depersonalize them using the available methods. Due to the high degree of anonymity, such data does not fall under the category of personal data, and, accordingly, under the provisions of the GDPR, which implies their free collection and processing. A different situation develops with pseudonymized data, which means such data that does not contain "personal" identifiers of a particular subject; however, when processed with additional data, depersonalization of anonymized data is possible[5].

Further, as part of the consideration of the legal experience of the UK, it is impossible to ignore the significant document of the European Commission from 2017 - "Building the European Data Economy"[6], where two significant conclusions were made. First, the paper presented for the first time touched upon the issue of the legal regime of machine-generated industrial data. Hence, it was proposed to introduce a new subject - the "creator of industrial data", which is the owner of the equipment that generates data, or owns the equipment on a different basis. As a result, it was proposed to assign a new "data producer right" to such a subject, which would establish the possibility of using raw information, as well as granting others access to use the data. Second, the proposal on the possibility of granting access to any person to the personal data of third parties in return for the specified remuneration, based on the principles of reasonableness, fairness and

[5] General Data Protection Regulation. Art. 4 (5).
[6] Communication on Building a European Data Economy // European Comission. 2017, p.13.

proportionality, by analogy with the free use of an intellectual property object without the consent of the copyright holder, but with the payment of a certain remuneration[7].

The US model of regulating Big Data

The specifics of the US information legislation is that, by and large, there are no rules when using any information, which is caused by the free collection and processing of any information, with the exception of restrictions established by industry legislation. In this regard, it is supposed to be appropriate to divide the consideration of American legal regulation into different categories of information, which individual form of Big Data, by analogy with the legal analysis of the UK experience.

Thus, starting with the consideration of the category of industrial data, the United States is currently refraining from adopting specialized acts that would regulate the area under study. However, within the framework of the issue under study, the Misuse and Computer Fraud Act deserves attention[8]. However, due to the emergence of digital phenomena such as Big Data, as well as the increasing cases of leakage of confidential information about the subject, American citizens increasingly feel the need to protect their personal data, which gives impetus to the regional development of relevant legislation, an example of which is the Law on California Consumer Privacy Policy 2018. Particular attention is drawn to the fact that the concept of personal data, according to this Law, includes not only traditional personal identifiers, as well as data from cookies and network activity, but also the results obtained from the processing of such data, which significantly expands the boundaries of this term[9].

Since information is considered as a commodity in the United States, it is possible for the personal data of subjects to be sold. However, due to the

[7] Ibid p.14
[8] The Code of Laws of the United States of America (18 U.S.C. § 1030). URL: https://www.law.cornell.edu/uscode/text/18/1030
[9] The Children's Online Privacy Protection Rule of 2013. §312.2. URL: http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim

unregulated nature of this area, the issue of abuse in the activities of information brokers, organizations that collect personal data for subsequent resale to another person, has become acute in the United States. Unfortunately, this issue has not yet been resolved at the federal level; however, individual states have attempted legally regulate this issue. Thus, in 2018, the State of Vermont passed the Law on Information Brokers, fixing their legal definition, as well as establishing certain rules for their activities, namely, registration with the authorized body of the state, a periodic report on their activities, the creation of an effective security system, a ban on the use data contrary to the purpose of collection[10]. Almost complete independence from the regulation by the provisions of this or that information legislation (with the exception of restrictions on special categories of information) is anonymized, as well as publicly available data that can be freely collected and analyzed without any notification of such activities. However, some authors state that there is a practice where technology startups have to pay for access to Big Data.

Conclusion

Based on the analysis of foreign legislation, we can come to the following conclusions.

First, there is no special law in foreign legislation that would regulate

[10] Information broker Act 2018. § 2430 (4)(A). URL: https://legislature.vermont.gov/assets/Documents/2018/Docs/BILLS/H-0764/H-0764%20As%20Passed%20by%20Both%20House%20and%20Senate%20Official.pdf

activities related to Big Data. Considering Big Data as a special commodity (USA) with commercial value seems to be successful theory. Second, there is a difference in the legal model of Big Data regulation between countries. As saying so, the UK builds the management of this area around privacy legislation, giving priority to the need to go through the procedure of "legalization" of the collection and processing of such data. However, in the US, due to the lack of a unified data privacy regulation, there is a free collection and analysis of any information, giving priority to commercial potential data. In the literature, the heterogeneous approach of countries to the same phenomena has been explained by the fact that the United States considers information as a special commodity, while the UK points to a continuous relationship between an individual and personal data related to him.

Third, the analysis of foreign doctrine did not reveal an urgent need for countries to determine a unified approach to the legal nature of Big Data, which may be due to the presence of data transfer structures. For example, in the UK, there is an agreement on data exchange, or in the USA, there is information broker who meets the main needs of the business sector and smooth existing gaps in the current legislation.

REFERENCES

1. Bart van der Sloot, Sascha van Schendel. International and comparative legal study on Big Data // The Netherlands Scientific Council for Government Policy. P.57. URL: https://www.wrr.nl/binaries/wrr/documenten/working-

papers/2016/04/28/international-and-comparative-legal-study-on-big-data/WP020-International-Comparative-Legal-Study-Big-Data.pdf

2. Bennett Moses L;De Koker L;Mendelson D. Big Data Technology and National Security: Comparative International Perspectives on Strategy, Policy and Law – United Kingdom Report. June 2018. URL: https://www.d2dcrc.com.au/m/u/2018/08/30/uk-report-june-2018.pdf

3. Tojiboev, A., Sharakhmetova, U., & Tojjiboyev, S. (2020). Between public and private-state entity as a party to international commercial arbitration: Lessons for the Republic of Uzbekistan. International Journal of Psychosocial Rehabilitation, 24(6), 581-591.

4. Tojiboyev, S. Z. (2022, August). THE PROSPECT OF TOBACCO CONTROL REGIME IN UZBEKISTAN IN LIGHT OF POTENTIAL DISPUTE UNDER THE UK-UZBEKISTAN BIT. In INTERNATIONAL CONFERENCES (Vol. 1, No. 7, pp. 46-51).

5. Zafarovich, T. S. (2022). Different Approaches in Enforcement of Arbitral Award Annulled at the Place of Arbitration. Miasto Przyszłości, 25, 320-323.

6. Tojiboyev, S. Z. (2022). TAXATION POLICY OF HOST STATE IN INVESTOR-STATE DISPUTE SETTLEMENT. Oriental renaissance: Innovative, educational, natural and social sciences, 2(8), 232-238.

7. Zafarovich, T. S. (2022). TAXATION POLICY OF HOST STATE IN INVESTOR-STATE DISPUTE SETTLEMENT.

8. Akbar, Z. (2020). The Activity of startups as an object of civil law. Review of law sciences, 4(1), 5.

9. Тожибоев, А. З. У. (2020). ДЕЯТЕЛЬНОСТЬ СТАРТАПОВ КАК ОБЪЕКТ ГРАЖДАНСКОГО ПРАВА. Review of law sciences, (1), 79-87.

10. ТОЖИБОЕВ, А. (2018). THE ROLE OF STABILIZATION CLAUSE IN INVESTMENT CONTRACT. Юридик фанлар аҳборотномаси, (2), 37-41.

11. Tojiboev, A. (2018). The role of stabilization clause in investment contract. Review of law sciences, 2(2), 8.

12. Тожибоев, А. (2020). ПРИМЕНЕНИЕ НЕКОТОРЫХ СТАРТАП-КОНТРАКТОВ И ЕГО ВАЖНОСТЬ В УСЛОВИЯХ ОНЛАЙН-РЕЖИМА. Review of law sciences, (2), 119-123.