ATLANTIS PRESS

Advances in Economics, Business and Management Research, volume 105

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

Regarding the issue of recognition of personal data, posted on the Internet as publicly available personal data

Vasilyeva N.V.
Baikal State University
Irkutsk, Russia
nativi@yandex.ru

Praskova S.V.
Irkutsk Institute (branch) All-Russian State University of Justice (RLA of the Ministry of Justice of Russia)
Irkutsk, Russia
savap@mail.ru

Pyatkovskaya Yu.V.
Irkutsk National Research Technical University
Irkutsk, Russia
julart@yandex.ru

***Abstract* — The article is devoted to the studying the problems of determining the degree of personal data privacy, posted on the Internet. The authors of the article note absence in legal science and legislation of a unified approach to determining degree of openness or confidentiality of such personal data, including lack of a unified approach to the recognition of such information as publicly available personal data. The article considers the position of arbitration courts, left unchanged by the Supreme Court of the Russian Federation in 2018, according to which only information contained in publicly available sources of personal data is recognized as public personal data. Taking into account the lack of written consent of users to post information about them in public sources in social networks, information of social networks was not recognized as public personal data. In this regard, the article raises questions about the basis for the processing of personal data posted on the Internet, including the situation where the subject of personal data seeks to ensure that such information becomes public, when placing personal data due to the requirements of the law, while using technologies "BIG DATE", as well as when using such data in the work of public authorities.**

Keywords — are the personal data, bases for processing, public personal data, public sources of personal data, technologies "BIG DATE".

I. INTRODUCTION

Today the digitalization of the national economy is one of the top-priority areas for the state development, contributing to the transition to a global information society. The positive aspects of such transition are indicated in the literature- the opportunity to use scientific advances for the development of social [1] and other spheres [2] of society, the involvement of public authorities and local government in digitalization processes, which contributes to the transparency of public authority and allows to fight against corruption effective [3], to deepening knowledge about new products and services [4]. In such conditions, information acquires manufacturing value and becomes an independent factor of production. In this regard, the issue of protection of personal data posted on the Internet becomes particularly acute.

Information services that aggregate information from a variety of publicly available sources about millions of citizens, systematize them by categories of citizens and presenting them to concerned parties on a subscription basis are widespread all over the world [5]. Such information, obtained mainly by using "BIG DATA" technologies, can be used to determine the financial solvency of a citizen, individualization of the terms of services offered to him, determining the occurrence of loss possibility, and for other purposes [6]. In this regard, it is important to determine the degree of confidentiality of personal data posted on the Internet and the basis for their secondary processing by various entities.

II. METHODOLOGY

The desired objectives of the research are achieved through the use of such methods of scientific research as:

1) the technical legal method, supporting logical thinking of the content of legal norms, governing the processing of personal data, as well as the practice of applying these standards;

2) method of comparative law, which allows you to consider the legal regulation of the grounds for processing personal data posted on the Internet, in the context of world practice;

3) the method of complex analysis, using which the study of the criteria for classifying one or another personal data as

public is carried out in conjunction with other legal phenomena;

4) method of forecasting that allows on the basis of the position expressed by the courts to determine the problems that the practice of using personal data posted on the Internet will encounter in the near future.

III. RESULTS OF THE RESEARCH

There is no single approach in science and in law of determining the degree of openness or confidentiality of personal data, posted on the Internet. First of all, the debate takes place, whether such information can be considered available to public personal data.

The Federal law "On personal data" (hereinafter- the Federal law), while enshrining legal definitions of the basic concepts in the field of processing the personal data, unfortunately, did not determine the content of the category "publicly available personal data". The term "publicly available personal data" was introduced only as an abbreviation when regulating the conditions of personal data processing (p. 10 part 1 article 6): it is provided that processing of personal data is carried out, access to an unlimited circle of persons to which is provided by the subject of personal data or at his request (hereinafter - personal data made publicly available by the subject of personal data). Federal law does not contain any other provisions disclosing the content of this category. However, the general concept of Article 6 of the Federal law indicates that the general availability of personal data is the basis that excludes the need to obtain written informed consent of the subject for processing of personal data. Rather than anywhere else this provision is of fundamental importance for processing of personal data posted in Internet.

At the same time, the Federal Law in Article 8 introduces a similar term in terms of sense - publicly available sources of personal data (including directories, address books). With the written consent of the subject, public sources of personal data may include his full name, year and place of birth, address, telephone line number, information about the profession and other personal data communicated by the subject of personal data.

Contents of the terms "publicly available personal data" and "publicly available sources of personal data" and their relationship in federal law are not disclosed.

In science also lacks a clear understanding of the content what is publicly available personal data. As a rule, it is explicitly recognized that publicly available personal data are the personal data located in publicly available sources of personal data. However, for the most part, scientists note that other personal information may include other information that, in accordance with the law, cannot be hidden (which is not subject to confidentiality requirements) [7, 8]. But composition of such information is not determined even through exemplary criteria.

In turn, practice of information relations proceeds from the fact that any information about citizens posted in Internet without restriction of access, or published in print media, are considered to be publicly available, unless the placement is in dispute. In such a case, it is assumed that access to such data is provided by the subject of personal data or at his request. Not only work of numerous commercial information services, but also work of many public authorities is based on this presumption.

However, at the moment there is a position of the Supreme Court of the Russian Federation, which refutes and actually prohibits such a practice.

This is a legal dispute between VKontakte LLC, on the one hand, and DABL LLC, and NATIONAL CREDIT HISTORY BUREAU JSC (hereinafter - NBKI JSC), on the other hand, which was started back in 2016 and until now has not been finally authorized by the courts. By itself, this dispute is about the presence or absence of copyright in the database consisting of personal data of persons registered in the VKontakte social network, and it will be crucial for the formation of further practice of recognition of intellectual property rights in relation to products based on the processing of information posted in social networks. Without considering this issue essentially within the framework of this article, we emphasize only that the authors support the point of view [9], according to which personal data as the content of information conceptually differs from objects of copyright. Therefore, processing of publicly available personal data should be regulated in a different - public law plane, considering the importance of this issue both for protecting the citizen's private life, and for ensuring the functioning of modern information services that are crucial for the digital economy.

In parallel with the dispute over intellectual rights to the VKontakte database, the courts resolved another dispute arising from the same life situation. The fact is that NBKI JSC, based on the use of the BIG DATE service, processed personal data posted by subjects in open sources: "VKontakte", "Odnokassniki", "My World", Instagram, Twitter, etc., in order to determine the solvency of individuals, and then offered the data obtained as a result of such processing to credit organizations. After checking this activity, Administration of Roskomnadzor for the Central Federal District issued order on eliminating the identified violation regarding the need to include these individuals in the notification of the authorized body on individuals (clients or potential clients of a financial institution) from open sources of information transmitted to a financial institution obtained using the Double Data Social Link service — a web link, the result of a search for a client or potential client, and the Double Data Social Attributes service — processing the profile of the sought individual in open sources of information. Administration of Roskomnadzor also indicated that such processing of personal data is carried out without the written consent of the subjects of personal data, which is a violation of the Federal Law requirements.

Disagreeing with the order, the NBKI JSC challenged it in the Moscow Arbitration Court, stating in support of its position that it was processing publicly available personal data and was not obliged to indicate the processing of this data in a notification sent to Roskomnadzor, as well as it has right to

carry out such processing without the written consent of the subjects of personal data.

Considering this dispute, the Moscow Arbitration Court indicated that two conditions are necessary simultaneously for recognizing personal data publicly available: 1) personal data are available to an unlimited circle of persons; 2) personal data are presented directly by the subject. Without the written consent of the subject of personal data, it is not possible to assert that they are provided by the specified subject. Personal data made publicly available by the subject of personal data only when they can be contained in publicly available sources of personal data. On the basis of which the court concluded that the information contained in social networks cannot be attributed to publicly available personal data, because social networks are not a source of publicly available personal data.

Thus, the court put an equal sign between publicly available personal data and personal data posted in publicly available personal data sources.

This position of the arbitration court was challenged in the appeal and cassational instances and was upheld, including by the Supreme Court of the Russian Federation. It is noteworthy that none of the higher authorities deemed it necessary to state their own position on this issue, adding only that, within the meaning of the Federal Law “On Personal Data”, placement of personal data in these open sources does not automatically make them publicly available. Therefore, processing of such data without the consent of the subject is not allowed.

Thus, at the moment there is an undisproved position of the Supreme Court of the Russian Federation, according to which, personal data are recognized only as publicly available personal data, placed in address books, telephone directories and other publicly available sources of personal data specially created for these purposes. The same data on citizens who are posted on the Internet or published in the print media, can be used only for the purposes for which they were posted, because in order to achieve precisely these goals the consent of the subject of personal data to their processing was given.

IV. Discussion of Results

The given position of the courts poses a number of questions to which it is not yet possible to give definite answers.

1. First of all, the question arises of the procedure for the action of the subject of personal data.

As mentioned above, the Federal Law provides as a condition for the processing of personal data a situation where access to an unlimited number of persons to such data is provided by the subject of personal data or at his request. Thus, the literal wording of the norm assumes that any subject of personal data can independently make his data publicly available, which is hardly possible when it comes to placing such data in publicly available sources of personal data. In this regard, it is unclear how subject of personal data should act, wanting to provide access to his personal data to an unlimited circle of persons. And such situations are widespread. So, the vast majority of well-known politicians, actors, people of creative professions have their own pages on social networks on which they post information about their lives. Purpose of this placement is unambiguous - to make this information available to an unlimited number of people. It is from this that both ordinary Internet users and a wide variety of subjects, including the media, use such personal information for various purposes. Is such processing of personal data lawful? And how subject the personal data himself should make it clear to Internet users that he had made his personal data publicly available? Should he inform about it every time when posting information on his page on a social network? It seems that the need to further confirm the general availability of personal data will greatly complicate the use of social networks.

2. At the same time, the question arises of the status of information posted on the Internet, by virtue of the provisions of federal law. A classic example of this kind of information is information about the head of a state body or local government, to be posted on the Internet in accordance with Part 1 of Art. 13 of the Federal Law “On providing access to information on the activities of state bodies and local authorities”. These provisions stipulate that surname, name, patronymic of the head of a state body or local government, of their structural units are subject to posting on Internet without fail, and other information - with consent of these persons Should one then consider that the surnames, names and patronymics of managers are publicly available personal data, and other information is not such? Indeed, such information is posted for one purpose - to make it available to an unlimited circle of users. Should it be only because of the difference in the grounds for placing personal data on Internet that the conditions for their processing should be distinguished?

An even more striking example in this regard is the announcement of information on income, expenses, property and property obligations provided by persons who fill state and municipal posts, service posts and a number of other posts for combating corruption. As the general meaning of the provisions of the Federal Law "On Combating Corruption" makes clear, placement of such information is aimed specifically at combating corruption, including providing the public with the opportunity to fulfilment control over individuals holding public posts. However, the common practice of using such information is to discuss, including in the media, the income level of such persons, their comparison with each other, etc. Should this discussion be considered a violation of the legislation on personal data as the use of personal data for purposes other than the purposes for which they were provided?

It seems that the position in question of the courts should not be unambiguously applied to relations of this kind. As rightly pointed out in the literature, State has repeatedly pointed out the priority of special legislation over the general conditions for the processing of personal data, recognizing the prevalence of public interests over the goals of protecting the citizen’s private life [10].

3. In the most difficult situation were various kinds of commercial information services that process personal data posted on the Internet, including using Big Data technologies. Since the considered position of the courts actually prohibits the use of Big Data technologies, all such services become

illegal. The problem is that such software products are in principle incompatible with the concept of processing personal data based on the consent of the subject of personal data. In order for consent of the subject of personal data may be called informed, specific and conscious, it is necessary that he was provided with detailed information about how his personal data will be used: purpose of use, composition of personal data and how to process it. At the same time, the use of Big Data technologies implies inability to provide an exhaustive amount of information for consent prior to processing, because a distinctive feature of these technologies is the uncertainty of the purposes of using the obtained data. Moreover, Big Data technologies offer unlimited opportunities to reap the benefits of reuse of the data, including combining them with other information [6]. So, activities of such services in the Russian Federation should be discontinued. However, firstly, it is very difficult to control, and secondly, there are no obstacles to the processing of personal data located in Russian segment of Internet, while being outside territory of Russia.

Thus, in this aspect, it is hardly possible to unambiguously use of the considered position of courts.

4. Finally, the prohibition to use without the written consent of the personal data posted on the Internet can significantly complicate the work of public authorities, including law enforcement agencies. Search for information about certain individuals on social networks is a common practice for work of bodies of inquiry and investigation. At the same time, it is known that goals of the operational-search activity are not consistent with those goals pursued by users of social networks, posting information about themselves and about other persons. As rightly noted in the literature, a person uploading information about himself to social networks does not agree that the investigator should look for information about him [11]. Does the position formed by the courts mean that such work of the authorities should be terminated?

V. CONCLUSIONS (INFERENCE)

This study allows us to conclude that at the moment, due to the uncertainty of the provisions of federal law, the interpretation of the nature and degree of confidentiality of personal data, posted on the Internet is carried out through law enforcement practice. However, due to the nature of law enforcement, posture of the courts cannot be considered as a universal rule. Questions arise about which relations the stated position is applicable to and which not. Considering the importance of processing personal data posted on the Internet, both for commercial relations and for the work of public authorities, it is required to develop a unified approach to determining their confidentiality, as well as processing conditions. This approach should be well-known and allow to all interested actors to formulate a line of their behavior in such a way that it is fully legitimate and could not subsequently entail application of sanctions by the State. It seems possible to solve this problem only by changing the provisions of the Federal Law. In this regard, the following changes can be proposed.

Firstly, to unambiguously define the concept of "publicly available personal data" through a legal definition and bring into correlation with the category of "publicly available source of personal data".

Secondly, to determine the main approaches to determining the degree of confidentiality of personal data, posted on the Internet, which are not publicly available personal data, given that it is not always possible for these purposes to obtain written consent of the informed subject personal data.

References

[1] Novikov S.P., Mikheenko O.V., Kulagina N.A., Kazakov O.D. Digital registry of professional competences of the population drawing on distributed registries and smart contracts technologies // Biznes Informatika-Business Informatics. Volume 46. Issue 4 P. 43-53. DOI: 10.17323/1998-0663.2018.4.43.53

[2] Petersen A., Tanner C., Munsie M. Citizens' use of digital media to connect with health care: Socio-ethical and regulatory implications // Health (United Kingdom). Volume 23, Issue 4, 1 July 2019, P. 367-384.

[3] Alvarez A.B. Structural transformations in french administration: ethical and technological issues // Revista general de derecho administrative. Issue 44, jan 2017.

[4] Nemtoi G., Bostan I. Digital economy and its impact over the personal data and private life protection // Innovation and knowledge management: a global competitive advantage, vols 1-4, 2011. P. 374-377.

[5] A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Date for Marketing Purposes. Committee on Commerce, Science and Transportation. Staff Report for Chairman Rockefeller. US Senate. December 18, 2013. P. ii. URL: https://www.commerce.senate.gov/2013/12/data-brokers-report.

[6] Savel'yev A.I. Problemy primeneniya zakonodatel'stva o personal'nykh dannykh v epokhu «Bol'shikh dannykh» (Big Data) // Pravo. Zhurnal Vysshey shkoly ekonomiki. 2015. № 1. P. 43-66.

[7] Gladkikh E.L. Problema obrabotki i zashchity personal'nykh dannykh v Internete // Rostovskiy nauchnyy zhurnal. 2016. № 4. P. 44;

[8] Gogaeva A.L. Personal'nye dannye kak ob'ekt informatsionno-pravovogo regulirovaniya // Perspektivy razvitiya APK v sovremennykh usloviyakh. Materialy 7-y Mezhdunarodnoy nauchno-prakticheskoy konferentsii. 2017. P. 442.Determann, L. No One Owns Data // Hastings law journal. 2018 V. 70. № 1. P. 1-43.

[9] Talapina E.V. Zashchita personal'nykh dannykh v tsifrovuyu epokhu: rossiyskoe pravo v evropeyskom kontekste // Trudy Instituta gosudarstva i prava Rossiyskoy akademii nauk. 2018. V. 13. № 5. P. 117-150.

[10] Mo, J.Y.C. Privacy and publicly available information: An analysis of the common law and statutory protection in Hong Kong// Statute Law ReviewVolume 40, Issue 2, June 2019, Pages 188-205.