Social Media Users Data Access: Russian Legal Approach

Juliya Kharitonova, Larissa Sannikova

Abstract: The article is devoted to the problem of the legal protection of data of users of social networks. Businesses are interested in the data posted by users on their social media pages. Big data from social media users have a high potential commercial value. However, at present, Russian legislation does not provide for the legal possibility of processing data for transferring it to third parties. For the development of digital markets, it is important to find a balance between the personal data protection of social media users and data processing companies. For this purpose, a legal regime for open-access personal data is being introduced in the Russian jurisdiction.

Keywords: personal data protection, sensitive personal data, personal data in the public domain, Big data.

Chapter 1. Introduction

The issue of personal data control in social media networks is directly connected to those legal restrictions regulating the level of privacy given to the data in question[1]. The processing of a users personal data is regulated by Russian legislation, and disclosure of the information provided by the user, including personal data, is only possible at the request of a court, law enforcement agency and in other cases as prescribed by law. However, the interests of these vital companies that analyze and process the vast amounts of data that is acquired by such social networks remain unprotected. This paper analyzes one such case, VKontakte LLC vs DABL LLC, which aims at protecting small businesses (companies) when using publicly available data from open social networking pages for commercial purposes. In the next part of the paper, we explore the legal treatment of user data on social

1 Katharine Sarikakis and Lisa Winter, "Social Media Users' Legal Consciousness About Privacy", *Social Media + Society,* February 2017. https://journals.sagepub.com/doi/pdf/10.1177/2056305117695325

media under Russian law. Particular attention is paid to the new legal concept "personal data, which the personal data subject has permitted to disclose".

Chapter 2. VKontakte Case Study

A key case in Russian law was VKontakte LLC vs DABL LLC (No. 40-18827/17-110-180).

VKontakte LLC, the VKontakte social network (VK.com) operator, brought a claim against DABL LLC, claiming that the defendant's actions violated its exclusive rights. DABL extracted and then used user information from the VK.com Database. According to the plaintiff, the Database producer's rights were violated. The parties' attention in the lawsuit was focused on the protection of IP rights. However, the legal community also saw in this dispute a more profound problem about the nature of the existing legal regimes regarding users data in online social networks.

The court concluded that DABL had created Double Search, Social Link, and Social Attributes software. This software is based on its unique technological search methods and algorithms for storing and analyzing social networks data, including VKontakte. As the copyright holder of the above mentioned software, DABL offers to collect and automatically process social network users data on behalf of its clients, in order to assess the creditworthiness of potential and existing debtors who are users of such social networks. Thus, for the first time, Russian litigation has addressed the possibility of manipulating social network user data for commercial purposes.

According to the general idea, the social network consists of hardware, software, and information parts. The social network information part comprises several automated databases, each of which consists of independent elements (materials), systematized in a certain way, allowing finding and processing the elements using the software. One of such databases is a database of social network users, which contains a set of independent elements (user cards) with information about each registered user in the social network. The database is updated with a new standalone element through a given data collection algorithm as a new user registers through the social networking site.

According to the experts who conducted a study of Double Search software, a set of independent elements, presented in the form of individual user cards, was studied for the purpose of analytical processing of informa-

tion resulting from viewing and indexing by the search engine Double Search[2] of VK.com users` publicly available pages.

The defendant's software explored the pages of users who had set suitable privacy settings in the social network for search engines to index their pages. In the system of VK.com settings in the Data Management Rules of the website there is an opportunity for users to set the option "The page is available for indexing by search engines." [3]

The courts disagreed on this point at various stages of the proceedings.

The court of the first instance dismissed VKontakte's claim because the plaintiff had not proved that the database had been created. The defendant was searching for publicly available information. The owners of information presented in the profiles are the users themselves and the information published by them is, by setting the appropriate access mode by the user, closed or public, i.e. open for use by any persons following part 2 of Article 7 of the Federal Law "On Information, Information Technologies, and Information Protection", No. 149-FZ, July 27, 2006.

The court of appeal reviewed the decision in favor of VKontakte LLC, noting that the extraction of content from the database DABL LLC violated social media users' rights. Since the plaintiff had assumed obligations to ensure the protection of data from unauthorized copying, distribution, and reproduction, collection and other actions performed with information from the social network, for commercial purposes or its use in whole or in any part in any way are not permitted without the licensor's (social media user's) consent.

---

2 The defendant is the copyright holder of the following software:
Double Search - a specialized search engine for finding information about people, including social networks;
Social Link - a program for viewing the results of clicking on the links uploaded to it by reflecting on the user's screen the contents of the page/pages to which the links uploaded to Social Link lead. This program can handle any links, both those received from Double Search and those received from other search engines or other sources.
Social Attributes is a program designed to follow the links uploaded to it and display the results of the content analysis of the linked pages on the user's screen, in the form of a system of numerical coefficients assigned to specific groups of information.

3 You can choose who can visit your page, contact you and see what you post on your page. You can even make your profile completely private and protect your personal space from unknown people, leaving your page fully visible only to your friends.

The court of appeal emphasized that "the plaintiff guaranteed users the protection of information about them from outsiders who were not users of the social media network, regardless of whether the information was public or private. At the same time, a disclaimer from the VK.com Privacy Policy stated that they did not apply to third parties' actions and internet resources. Also, The Site Administration bears no liability for the actions of third parties which as the result of using the Internet or the Site Services obtained access to the User information in accordance with the confidentiality level selected by the User, for the consequences of use of the information which, due to the Site nature, is available to any Internet user. (clause 8). The VK.com Privacy Policy stipulates that The Site Administration takes technical, organizational, and legal measures to ensure that the User's personal data are protected from unauthorized or accidental access, deletion, modification, blocking, copying, dissemination, as well as from other unauthorized actions. (clause 7.1).

The VK.com License Agreement8 prohibits any actions (Reproduction, copying, collection, arrangement, storage, and transfer of information from the Social Network for commercial purposes) with the Social Network content without the licensor's consent (clause 5.16). In doing so, it stipulates that the licensee, i.e., the user, consents to the reflection of his data on the Personal page within the SNS functionality and that such data will be considered publicly available unless another mode of access is chosen by the subject (point 5.3).

It is the user who chooses the level of visibility of his/her profile per the VK.com Privacy Policy and accepts the responsibility that the information specified by him/her may be accessed by other users of the website, taking into account the specifics of the website architecture and functionality (point 5.2). Consequently, when a data subject decides to apply any privacy settings, he or she also determines the personal data regime, including its public accessibility, by his or her conclusive actions.

The VKontakte License Agreement applies to all Internet users who may not be users of the social network but access the VKontakte user page.

It is worth mentioning that since August 31, 2018, VKontakte has introduced fully private profiles, information from which is only available to those whom the person has added as "friends." [4] However, even if a user has a "closed" profile type, it can still be visible to all users of the

4 Sultan Suleymanov, "VK users can now close profiles from strangers", *Meduza*, August 31, 2018, https://meduza.io/feature/2018/08/31/vkontakte-pozvolila-zakryvat-profili-ot-postoronnih-v-tom-chisle-ot-politseyskih-kotorye-ischut-ekstremizm

"Internet," or to everyone except search services, or only to users of the social network VKontakte. However, a closed profile shows a small image of the person, name, date of birth, workplace, and city if they fill in the relevant fields. Thus, it seems that public accessibility is determined first by profile visibility and then by the categories of information that the user reveals depending on the type of profile. The presence of Public post or Friends only ("Visible to all" or "Visible to all except search sites") options in the visibility settings suggests that the profile is unambiguously accessible to all, as it is not restricted to social network members.

DABL Ltd.'s appeal reasonably stresses that the software processes the publicly available information of the social network profiles, originally intended to be accessible to all users. It is up to the subject to consciously dispose of its data and be aware of the consequences of publishing information in public social network profiles.

If the intellectual property regime is extended to the data published by users, the subject would be deprived of the right to dispose of the information about him/herself (Article 20.2 of the cassation appeal).

In rendering its final judgment in the case on March 22, 2021, the court expressed its opinion that the Respondent's software browses the pages of users expressly authorized for everyone to view them by clicking on links to those pages, the experts involved in the case agreed that Double Search was a specialized search engine. Defendant's customers do not use the information in the index (do not read it, do not analyze it, do not search for something in it, etc.) when they work with Double Search and search information for a user. They receive the results they need from the program in the form of links to users' webpages. The Respondent's software indexes only the pages of those users who have consented to this by using the appropriate privacy settings offered by VKontakte and have set the page to be open to all, and information from pages with other access settings is not indexed. Defendant's software interacts with the VKontakte site only within the rules and for the purposes set by the rights holder itself and only with those user pages that have explicitly expressed their consent (using the VKontakte site functionality) for their pages to be indexed by search engines.

These circumstances enabled the court to reject the plaintiff's claims and, in effect, to allow the disputed software to process, in algorithmic ways, open user data from social networks for commercial purposes.

Chapter 3. Legal treatment of user data on social media under Russian law

The users themselves mainly provide the data that comes in and is stored in the social media information base. However, the set of such data can be particular in each case.

For example, VK.com has and makes it possible to upload user data to the following extent:

- location;
- registration data (name, surname, date of birth, gender, mobile number, email if provided);
- support service contacts;
- profile details (marital status, place of residence and hometown, education, career, and military service);
- history of visits to VKontakte and data about the device from which you are logged in;
- the automatically obtained information (e.g., when the user has logged in to third-party sites through VK.com and has given access to any information);
- the history of posts and subscriptions;
- messages;
- media files in which the user has been marked;
- payment data;
- information from third parties.

Legally, data collected by a social network is subject to different legal regimes.

Chapter 3.a. Personal data

Article 3, paragraph 1 of the Federal Law of 27.07.2006 No. 152-FZ (rev. 30.12.2020) "On Personal Data" states that personal data includes any information that directly or indirectly concerns a defined or identifiable natural person. The law represents the latter as the subject of personal data.

Russia has adopted the broadest approach, according to which personal data is any information: name, surname, patronymic, year, month, date of birth, place of birth, address, marital status, social status, property status, education, profession, income, other information relating to the subject of personal data (paragraph 2.5 of Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) Order No 94 dated 30.05.2017 (revised on 30.10.2018) "On approval of

methodological recommendations for notifying the competent authority on the beginning of personal data processing and on changes in previously submitted. "

The main legal attributes of personal data are distinguished:

1. information (information, data, reports, etc., following the Information Act).
2. relating directly or indirectly to an individual. Personal data containing direct information about a person (passport series and number, DNA, etc.) can be accurately identified. With indirect information about the person, he or she becomes "identifiable" (e.g., such information includes information about the education received). (Article 6 of the Information Act).
3. the subject of personal data is a human being.
4. the purpose of collecting, storing, and using personal data is to identify a data subject based on specific characteristics.
5. to be legally protected, personal data has to be recorded in a specific storage medium. This is information coming from any source and in any form. The Model Law on Personal Data of October 16, 1999, adopted to unify and harmonize the legislation of the countries of the former USSR, states that the information recorded on a tangible medium is subject to legal protection.

Personal data may be permissible for dissemination (Article 3 of the Federal Act of 27.07.2006 No. 152-FZ "On Personal Data").

The law divides personal data into groups:

1. general: 1) basic, 2) additional
2. special;
3. biometric: 1) physiological, 2) physical, 3) behavioral.

General personal data is data that can be identified with the highest degree of certainty.

General personal data includes basic and supplementary data. General basic data directly refers to a specific person: Full name and other passport details, date of birth, place of registration, and actual residence.

General additional data is, for example, information on education, profession, marital status, telephone number, etc. With the available general basic data, this type of information makes it possible to identify a person with almost absolute certainty.

Special categories of personal data include race, nationality, political views, religious or philosophical beliefs, health conditions, intimate life (clause 2.6 of Roskomnadzor Order No 94 dated 30.05.2017).

Biometric personal data characterizes a person's physiological and biological characteristics that can be used to identify the person. (clause 2.7 of Order of Roskomnadzor of 30.05.2017 N 94). An image of a person (photograph and video recording) that allows identification and is used by the operator for this purpose is considered personal biometric data (Clarifications by Roskomnadzor "On the issues of attributing photo and video images, fingerprints, and other information to personal biometric data and the specifics of their processing").

All of this data is used by the operator (the person who organizes and/or carries out personal data processing and determines the purposes and content of personal data processing) to establish the personal data subjects identity.

The law does not single out the so-called personal sensitive data of a citizen - one of the personal data types - but it does have increased importance to the individual. Personal data, the disclosure of which may cause substantial non-pecuniary damage to an individual. For example, information on race, sexual orientation, religious and political beliefs, criminal record, etc. Article 6 of the Convention for the Protection of Individuals concerning Automatic Processing of Personal Data states that it is unlawful to subject such data to automatic processing. The latter is possible only if the domestic law of the state provides appropriate safeguards (Convention for the Protection of Individuals concerning Automatic Processing of Personal Data. ETS No.108. Strasbourg, 28/01/1981).

In Russia, the principle of indirect identification of the data subject is enshrined, which allows an individual to claim data protection rights in many contentious situations. There is information that can, to a certain extent, identify an individual or a specific range of data subjects or, in conjunction with other personal data, identify a person. This approach is recognized in the doctrine and is also confirmed by international law-making practice. For example, the EU Directive 95/46/EC on personal data protection (GDPR) contains a similar approach.

The approach to understanding personal data established by Russian law is called context-oriented and has formal ambiguity. It is not easy to define precisely what information should be classified as personal data.

Chapter 3.b. Sensitive personal data

However, in general, the business model of most major social networks is built around personal data. The accumulation of personal, susceptible

information about the user and encouraging the user to disclose relevant information continuously is at the core of social media functioning.

Russian law does not distinguish a separate concept of sensitive personal data, unlike the GDPR rules, which qualify personal data as "sensitive" on a par with health, political and religious beliefs.

Centrally, it argues that scholars and regulators need to pay attention to the principle of intimacy[5].

M.A. Rozhkova[6] also notes that personal data, in general, is understood instead as data about citizens processed by public authorities. The researcher refers to them as:

1. unique identifiers of a person;
2. an image of a citizen;
3. unique identification numbers (TIN, Insurance Number of Individual Ledger Account);
4. publicly available information about a citizen that is self-published on the internet.

Regarding personal information that an individual puts in the public domain, by Article 152.2.1 of the Russian Civil Code, the subject of such information has no right to prevent its further use without his or her consent. As we can see, the legislator provides for the possibility of processing such information. That requires the subject of such information to place it in the public domain independently. Such information is regulated as publicly accessible.

Part 1 Article 7 of the Information Act determines that publicly accessible information is the information the access to which is unlimited. That establishes the presumption of openness of information, as it is any information to which access is open to everyone. As Article 7 (2) of the Information Act establishes, such information may be used without restrictions, but there are restrictions regarding dissemination.

A particular case of the above rule is the provision in point 2 of paragraph 1 of Article 152.2 of the Russian Civil Code which states that in a situation where information about a citizen's private life has previously been made publicly available or has been disclosed by the individual him-

---

5 Andrew McStay, "Empathic media and advertising: Industry, policy, legal and citizen perspectives (the case for intimacy)", *Big data & society* (December 2016), https://doi.org/10.1177/2053951716666868.

6 Marina Rozhkova, "Personal data: can they be classified as property? (view of a civilist)", Zakon.ru, February 28, 2019, https://zakon.ru/blog/2019/02/28/personalnye_dannye_mozhno_li_otnosit_ih_k_imuschestvu_vzglyad_civilista

self or by his will, it will not be considered a violation to collect, store, distribute or otherwise use such information without the citizen's consent. In other words, federal law here enshrines the rule that it is permissible to disseminate the designated publicly available information without the consent of the data subject.

It can be concluded that the posting of personal information on an internet site makes it publicly available. However, to disseminate such information, the procedure set out in Article 9 of the Law on Information must be followed.

Thus, personal data is any information that directly or indirectly relates to an identified or identifiable natural person. Personal data (or "personal sensitive data"), on the other hand, is understood as a particular type of personal data, which implies mainly personal information about an individual.

Chapter 3.c. Personal data in the public domain

Amendments to the Personal Data Law came into force on March 1, 2020, introducing the term "personal data, which the personal data subject has permitted to disclose" and establishing a special legal regime. Essentially, this refers to personal data that is publicly available and that users themselves post via geolocation tags, photos, audio, and video recordings, comments, reposts, participation in groups, polls, etc[7].

According to Article 10.1 of the Personal Data Law, users must expressly consent to the processing of personal data that is publicly available. Social networks and other digital platforms shall provide the user with the possibility to determine the list of personal data for each category of personal data specified in such consent. Consent can be executed directly on the digital platform's website or using a unique information system of the authorized body to protect personal data subjects' rights. Silence or inaction of the user under no circumstances can be considered as consent.

The consent must clearly express the user's will to disseminate the personal data to which the user has access. Otherwise, the user will be deemed not to have consented to the dissemination of their data. In the consent,

---

7 David Hiatt and Young B. Choi, "Role of Security in Social Networking", *(IJACSA) International Journal of Advanced Computer Science and Applications* 7, no. 2 (2016): 12, https://thesai.org/Downloads/Volume7No2/Paper_2-Role_of_Security_in_Social_Networking.pdf

the user can establish prohibitions and conditions for the processing of the data, except for access to it. Thus, the law establishes a rather strict legal regime for publicly available personal data.

However, at present, social networks have not responded to the legislation changes on personal data. For example, not a single social network has offered its users consent to the processing of publicly available personal data with a list for each category of personal data. It appears that some social networks operating in Russia will be unable to meet these requirements due to their algorithm. For example, the algorithm of the well-known dating network Tinder.com is set up to provide information on the user's age and allow access to geolocation. The availability of this data allows for a more accurate matchmaking process. The digital platform is required by law to ensure that the user can set a ban on sharing personal data about them, but this cannot be easy to implement due to the algorithm in place.

User agreements with social media platforms usually specify that the user also bears third parties' risk using this information. Thus, point 2.1 of "Rules of Protection of Information about Users of VK.com" states directly that the user "understands that the information on the Site posted by the User about himself can become available to other users of the Site and Internet users and can be copied and distributed by such users." The Odnoklassniki social network followed the path of limiting its liability by explicitly stating that it "shall not be held liable for the actions of third parties that gain access to information about the User following the User's chosen level of privacy as a result of using the Internet or the Social Network, for the consequences of using information that, due to the nature of the Social Network, is available to any Internet user." Thus, social networks merely alert their users to the technical possibility of third parties collecting such information for further processing.

The processing of publicly available personal information using data mining systems provides insights into specific user behavior groups. This information is therefore of considerable interest for both commercial and other public purposes. Big Data is recognized as a new digital asset - BigDate - and is in high demand on the market[8].

Article 5(2) of the Personal Data Law stipulates that personal data may only be collected and processed for "specific, predetermined and legitimate purposes". Social networks (VK.com, Odnoklassniki.com, etc.) in their

8 Larisa Sannikova and Juliya Kharitonova, *Digital Assets: A Legal Analysis*, (Moscow, 2020), 58.

rules specify as such a purpose the execution of an agreement with users. There is no legal possibility of transferring (sellng) the processed data as Big Data to third parties. Based on data processing's strict purpose, social networks cannot collect data for different purposes: fulfillment of user agreements and sale to third parties. Clause 3 of Article 5 of the Personal Data Law expressly prohibits combining databases containing personal data whose processing is incompatible with one another. Thus, at present, Russian social networks are not allowed to collect and process users' information for subsequent sale to third parties.

At the same time, all market participants recognize Big Data's value as a digital asset and the need to legalize its circulation. To date, the problem of legalizing Big Data circulation is closely linked to protecting individual personal data. The law prescribes that personal data must be destroyed or depersonalized once the purpose of its processing has been achieved (Article 5(7) of the Personal Data Law). The law essentially equates depersonalization with destruction.

However, an analysis of regulatory rules shows that these categories are not identical. According to the Methodological Recommendations on the application of Roskomnadzor Order No 996 of September 5, 2013, "On Approval of Requirements and Methods of Personal Data Depersonalisation," depersonalized data refers to data stored in information systems in electronic form that cannot be identified as belonging to a specific personal data subject without additional information.

This recommendation also contains a non-exhaustive list of methods of depersonalization:

> the method of introducing identifiers (replacement of the part of the information (personal data values) with identifiers with the creation of a table (reference book) of identifiers compliance with the original data);
> the method of composition or semantics modification (change of personal data composition or semantics using statistical processing results replacement, summarization, or deletion of part of the data);
> the decomposition method (splitting the set (array) of personal data into several subsets (parts) and then storing the subsets separately);
> shuffling (shuffling of individual records or groups of records in a personal data file).

It should be noted explicitly that Roskomnadzor Order No 996 of September 5, 2013, "On Approval of Requirements and Methods for Personal Data De-identification," makes reversibility a mandatory requirement for the properties of the de-identification method. Reversibility refers to the

possibility of de-anonymization, whereby anonymised data can be reduced to its original form, making it possible to determine whether the personal data belongs to a specific subject and eliminate anonymity.

Thus, in depersonalization, as opposed to destruction, the possibility of extracting information about a particular user as a whole is retained, and hence the risk of disclosure of user information is also retained[9].

When choosing a technique, it is crucial to maintain a balance between confidentiality and the data's usefulness[10]. The greater the anonymization of big data, the less accurate information can be gleaned from its analysis. Consequently, the value of such data decreases significantly.

According to the Russian regulator, big data can only be sold if the user has given his or her separate consent. As an additional protective measure, it is proposed to prohibit identifiers to third parties for de-identification procedures. The relevant bill is now in the Russian State Duma. However, a business has been skeptical of the bill, pointing out that the lack of an appropriate legal framework significantly hinders the digital economy's development.

Chapter 4. Conclusion

In general, it can be concluded that a legal regime for open-access personal data is being introduced in the Russian jurisdiction. If the data subject allows everyone to see his or her social media account data, personal data is considered publicly available. Any company can collect, analyse and share this information with its customers for commercial purposes.

Bibliography

Hiatt, David and Choi Young B. "Role of Security in Social Networking" *(IJACSA) International Journal of Advanced Computer Science and Applications* 7, no 2. (2016): 12-15. https://thesai.org/Downloads/Volume7No2/Paper_2-Role_of_Security_in_Social_Networking.pdf

9 Alexander Savelyev, "Problems of the application of legislation on personal data in the era of "Big Data"", *Law. Journal of the Higher School of Economics* 1 (2015).

10 Vladislav Kiselenko, "Anonymization of work in the global computer network Internet", *Vestnik Bauman MSTU Instrument making series* 1 (2005), https://cyberleninka.ru/article/n/anonimizatsiya-raboty-v-globalnoy-kompyuternoy-seti-internet

Kiselenko, Vladislav. “Anonymization of work in the global computer network Internet.” *Vestnik Bauman MSTU Instrument making series* 1 (2005): 44-51. https://cyberleninka.ru/article/n/anonimizatsiya-raboty-v-globalnoy-kompyuternoy-seti-internet

McStay, Andrew. “Empathic media and advertising: Industry, policy, legal and citizen perspectives (the case for intimacy)”, *Big data & society* (December 2016). https://doi.org/10.1177/2053951716666868.

Rozhkova, Marina. “Personal data: can they be classified as property? (view of a civilist)” Zakon.ru, February 28, 2019. https://zakon.ru/blog/2019/02/28/personalnye_dannye_mozhno_li_otnosit_ih_k_imuschestvu_vzglyad_civilista

Sannikova, Larisa, and Kharitonova Juliya. *Digital Assets: A Legal Analysis*. Moscow: 4 Print, 2020.

Sarikakis, Katharine, and Lisa Winter. “Social Media Users’ Legal Consciousness About Privacy”. *Social Media + Society*, (February 2017), https://journals.sagepub.com/doi/pdf/10.1177/2056305117695325.

Savelyev, Alexander. «Problems of the application of legislation on personal data in the era of "Big Data"» *Law. Journal of the Higher School of Economics* 1 (2015): 43-66.

Suleymanov, Sultan. “VK users can now close profiles from strangers”, *Meduza*, August 31, 2018. https://meduza.io/feature/2018/08/31/vkontakte-pozvolila-zakryvat-profili-ot-postoronnih-v-tom-chisle-ot-politseyskih-kotorye-ischut-ekstremizm