



УДК 349.681



Серебряков Кирилл Дмитриевич  
Санкт-Петербургский государственный университет

Факультет политологии

Россия, Санкт-Петербург

[serebryakovkirill35@gmail.com](mailto:serebryakovkirill35@gmail.com)

Serebryakov Kirill

St. Petersburg state university

Faculty of political science

Russia, St. Petersburg

## НЕКОТОРЫЕ ПРОБЛЕМЫ РЕАЛИЗАЦИИ МЕХАНИЗМА ПРАВОВОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СОЦИАЛЬНОЙ СЕТИ «ВКОНТАКТЕ»

**Аннотация:** в статье производится обзор выявленных проблем в реализации механизма защиты персональных данных в работе социальной сети «ВКонтакте», обеспеченных нормами российского законодательства. Среди имеющих место проблем выделяется отсутствие должного перечня требований со стороны регулятора к операторам, осуществляющим обработку персональных данных. Также архитектура социальной сети предлагает свободную циркуляцию большого массива добровольно указанных персональных данных, сбор которых субъектом таких данных может быть не санкционирован, что несёт определённые риски для самого субъекта (например, в контексте киберпреступлений, возможностей официального трудоустройства и т.п.).

**Ключевые слова:** социальные сети, ВКонтакте, персональные данные, защита персональных данных, Интернет, доступ и сбор персональных данных, киберпреступления.



## PROTECTION OF PERSONAL DATA IN THE SOCIAL NETWORK

### «VKONTAKTE» AND SOME PROBLEMS OF ITS IMPLEMENTATION

**Annotation:** the article provides an overview of the some problems in the implementation of the mechanism for protecting personal data in the social network «VKontakte». There is no list of requirements on the part of the state regulator for operators processing personal data now. It is one of the significant problems in this context. Moreover, the architecture of the social network offers free circulation of a large array of personal information voluntarily specified by the subject of personal data, the collection of which may not be authorized by him. This carries certain risks for the subject of personal data (for example, in the context of cybercrime, employment opportunities, etc.).

**Key words:** VKontakte, social networks, personal data, protection of personal data, Internet, access and collection of personal data, cybercrime.

Социальные сети являются наиболее ярким примером циркуляции персональных данных в рамках Всемирной паутины. Более того, сами сети снискали большую популярность у пользователей во всём мире, став самым массовым сегментом информационно-телекоммуникационной сети «Интернет», а потому аккумулирующим множество оставляемых ими персональных данных. Социальную сеть при этом отличает именно сетевая организация, узлами которой являются граждане и апатриды (пользователи социальных сетей), а также предприятия, фирмы, представляющие либо дублирующие важную информацию посредством данных электронных платформ. При этом узлы сети взаимодействуют посредством передачи информации [6, с. 33], включая и конфиденциальную информацию.

Само определение социальной сети было дано Дж. Барнсом в 1954 году, акцентируя внимание на специфике связей малых общественных групп [11, р.



42]. Более того, по мнению Д.В. Руденок, эти гражданские процессы заложили базовую основу для понимания сетей как системы с функциями консолидации людей в группы и стратификации по признакам интереса, статуса и т.п. [10] Только с переносом социальных коммуникаций на Интернет-площадки значение данного термина было пересмотрено и приобрело современную коннотацию, когда такая сеть рассматривается как Интернет-ресурс, обеспечивающий социальные коммуникации, взаимоотношения его участников. На данный момент самыми массовыми и значимыми социальными сетями выступают такие, как «ВКонтакте» (ежемесячная аудитория 39 млн. чел.), «Одноклассники» (почти 24,5 млн. чел.), «Facebook» (18,9 млн. чел.) и др [8].

Архитектура социальной сети многогранна и отличается большим числом единиц различного размера (группы, публичные страницы, сообщества, паблики, странички пользователей и др.) и разным уровнем внутреннего регулирования. В силу того, что объединение пользователей в рамках потребления контента того или иного паблика обусловлено личными интересами и хобби, то набор размещаемых персональных данных от одной группы или сообщества к другой различен и вариативен. При этом основные данные указываются на странице профиля пользователя, однако, специфика этих данных строится на идее свободной воли размещения личной информации субъектом персональных данных, а потому верификация этих данных, их правдивость зачастую может подвергаться намеренным искажениям. Тем не менее, в рамках идентификации физического лица при регистрации странички в социальной сети запрашиваются такие персональные данные, как адрес электронной почты, а также номер мобильного телефона регистрируемого лица.

Свободная циркуляция предоставленных публично данных отличает социальные сети, а потому возможен свободный сбор такой информации (о



хобби, увлечениях, месте работы и учёбы, которые, как правило, заносятся в специализированную структурированную форму по желанию пользователя) всеми заинтересованными сторонами, включая структуры по поиску должников. Тем не менее, законодатель в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных» [3] определил условия, которые обязательны для операторов данных, осуществляющих сбор в Интернете. В частности, это касается обязанности публикации оператором данных специализированного документа, размещаемого на своём Интернет-ресурсе, в котором отражены основные положения, касающиеся вопросов обработки и защиты персональных данных, с которыми при регистрации пользователь обязан ознакомиться. Например, для сети «ВКонтакте» таким документом являются Правила защиты информации о пользователях сайта, представляющий собой официальный документ организации ООО «ВКонтакте», где рассмотрены основные положения работы оператора с персональными данными зарегистрированных пользователей. Разработчики документа отмечают, что вся информация размещается и хранится на электронных носителях, а также, что используются автоматизированные системы за исключением случаев, требующих неавтоматизированной обработки, предусмотренных национальным законодательством [9].

Можно считать специфической форму согласия на обработку персональных данных в рассматриваемой социальной сети, которая не подразумевает отдельного соглашения, а только принятие положений Правил защиты информации. Сама обработка данных осуществляется без уведомления уполномоченного специализированного органа, отвечающего за защиту прав субъектов персональных данных (Роскомнадзор). Такой формат имеет высокое распространение в сети «Интернет», что обусловлено складывающимися в его рамках информационными правоотношениями.



В частности, поскольку многие Интернет-ресурсы являются функционально ориентированными на поддержание коммуникации своих пользователей, то поиск и, следовательно, определенная идентификация человека относится к ключевым задачам таких ресурсов, вследствие чего любому заинтересованному лицу, как минимум, зарегистрированному в социальной сети, доступна информация, занесенная в профиль пользователя. Для сети «ВКонтакте» этот перечень включает в себя ФИО и дату рождения пользователя, его фотографию, поставленную в качестве аватара, информацию о законченных учебных заведениях, список друзей, а также сведения о не скрытых режимами приватности сообществах и подписчиках зарегистрированного пользователя [9].

В силу указанной ранее специфики размещаемых пользователем на личной страничке персональных данных, которые могут быть им намеренно искажены, организациям, владеющим социальными сетями и выступающим операторами персональных данных, сложно определить, какие именно из указанных данных относятся к персональным. Поэтому в документах, регулирующих процессы сбора, обработки и защиты данных как правило отделены понятия персональных данных и прочей предоставляемой информации. В свою очередь, ограничением функции поиска помимо ложной предоставляемой информации в арсенале пользователя является «режим приватности», который ограничивает круг третьих лиц, имеющих доступ к предоставляемой в социальной сети пользователем информации личного характера, однако, такой режим может распространяться не на все сведения, как это указано в Правилах «ВКонтакте» [9]. Однако имеются и сведения с обратным эффектом, когда после реформы интерфейса и услуг рассматриваемой социальной сети в 2018 году на фоне роста возбуждаемых административных и уголовных дел за репосты стало невозможно увидеть тех, кто репостнул ту или иную запись на стене пользователя или сообщества, что



было обосновывалось соображениями обеспечения защиты пользователей сети.

Сбор информации в социальной сети производится различными способами, включая и незаконные или неэтичные, например, посредством вредоносных фишинговых программ либо просто с использованием сервиса настроек социальной сети или библиотек с закодированными данными пользователей (например, в рамках API VK и библиотек requests). Также стоит уделить внимание тому, что в рамках роста информационной грамотности и обеспечения дополнительных гарантий защиты прав граждан в отношении их персональных данных необходима дополнительная работа по разъяснению пользователям требований в сфере работы с персональными данными со стороны оператора Интернет-ресурса. Релевантным видится переход на повсеместную практику свободного отказа от обработки части персональных данных, которые могут регулироваться посредством настроек в браузере.

Безусловно, в рамках работы с общей информационной грамотностью населения, необходимо указывать и на риски запроса предоставляемых сведений со стороны уполномоченных на то структур. В частности, в ст. 6 Федерального закона «О персональных данных» предусмотрена передача указанных сведений государственным органам по запросу и при наличии соответствующих на то полномочий [3]. Здесь стоит отметить, что на данный момент социальные сети являются активно используемой органами государственной власти площадкой для поиска граждан, определения их местонахождения. Что касается должников, их имущества, то ФССП России были разработаны соответствующие Методические рекомендации [5]. Так, например, на начальном этапе поиска граждан или организаций, выступающих объектом для судебных приставов, предлагается написание простых поисковых запросов в общедоступных системах (Яндекс, Google, Bing и др.). Более того, рекомендуется также привлекать к поиску такие ресурсы, как Интернет-



каталоги, профили в социальных сетях, личные блоги (странички на «Живом журнале» и т.п.), доступные в сети «Интернет» адресно-телефонные базы (аналоги справочников), новостные ленты и новостные агрегаторы, а также, собственно, ресурсы, позволяющие на электронно-коммерческой основе приобретать или реализовывать собственное имущество (сайты Юла, Avito и др.). Наконец, в рекомендации входит изучение такого же массива данных близких родственников, друзей должников и возможных коллег по работе.

Со вступлением в силу Регламента ЕС 2016/679 (General Data Protection Regulation) [1] в 2018 году были изменены принципы работы социальных сетей. «ВКонтакте» переформатировала свою коммуникацию с пользователями и в рамках соблюдения данного Регламента сначала для граждан Европейского Союза, а затем и для российских граждан ввела возможность запроса информации со стороны пользователя того, какие персональные данные собираются и обрабатываются оператором, а также в каких целях. Можно получить достаточно обширный перечень данных, включая автоматически собираемую информацию (время входа и выхода пользователя из социальной сети, модель ноутбука или телефона, использованного для входа в свой профиль), истории блокировок и оставленные закладки и т.п. В целом нет конкретизированных законов, направленных на обеспечение защиты персональных данных в информационно-коммуникационной сети «Интернет», обязанность по их защите по общему правилу возложена на операторов персональных данных без конкретизации пределов и возможностей их полномочий в указанной сфере.

Существенным вопросом, требующим своего рассмотрения, выступает анализ преступлений, совершаемых через электронные платформы. Наиболее распространенным среди них выступает мошенничество, проявленное к собственности зарегистрированных пользователей. Это может осуществляться, в частности, посредством взлома, неправомерного доступа к личной страничке



пользователя. Как правило, после получения такого несанкционированного доступа производится рассылка сообщений друзьям человека, чей профиль был взломан, с просьбой перевести средства, поскольку сам пользователь находится в сложной жизненной ситуации. Также возможна переписка с потенциальной жертвой без взлома её личной странички, где посредством методов социальной инженерии мошенник узнает необходимые сведения для перевода средств (номер карты, смс-оповещения и т.п.) на свою карту, после чего коммуникация прекращается. Расчет делается на то, что самостоятельно проследить пользователю транзакции довольно сложно, а небольшой объём списанной суммы позволит свести потенциальное обращение жертвы финансового преступления в правоохранительные органы к минимуму [7, с. 135-136].

Российское законодательство отличает почти полное отсутствие актов в отношении сертификации средств защиты информации, за исключением Постановления Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации» [4], регулирующего только способы защиты тех сведений, которые отнесены к государственной тайне. При этом в целом меры, которые необходимы для выполнения требований для защиты персональных данных, выдвигаемых к операторам, определяют последние, что вносит большие неясности в механизм регулирования, обозначенный законодателем в Федеральном законе «О персональных данных» [3]. Единственной регламентированной мерой выступает обязанность оператора персональных данных по выполнению запроса в виде предоставления необходимых документов, направленный Роскомнадзором.

Ещё одной проблемой является защита пользователя в условиях трудового законодательства. Так, например, довольно распространенным является отказ работодателя при приёме на работу нового сотрудника на основании несогласия с содержанием данных, указанных последним на публичных Интернет-ресурсах, это, в частности, касается фотографий,





репостов, собственных постов и т.п. Стоит отметить, что таким образом нарушаются принципы трудовых отношений, установленные в ст. 2 Трудового кодекса (право распоряжения своими способностями к труду, выбор профессии, равенство работников). Более того, такая формулировка является необоснованной при отказе в приёме на работу. В целом, необходимо помнить, что вообще запрещено ограничение прав по обстоятельствам, прямо не вытекающим из содержания деловых качеств потенциального работника (за исключением случаев, когда установление каких-либо преимуществ является закрепленным в федеральном законодательстве), что урегулировано ст. 64 ТК РФ [2].

Можно заключить, что проблемы регулирования механизма защиты персональных данных в сети «Интернет» носят многогранный характер. В целом, специфика информационных правоотношений в сети строится на функциональном принципе свободного поиска и ознакомления с данными других пользователей, администрации Интернет-ресурсов частично данную проблему решают с помощью механизмов «приватности» с оговорками, основанными на национальном законодательстве. Примечательно, что нет разработанных механизмов защиты персональных данных пользователей в виде установления обязанности со стороны оператора персональных данных ограничивать доступ к указанным пользователем сведениям, расположенным в информационно-телекоммуникационной сети «Интернет».

Многообразие проблем также связано с тем, что регулирование многих электронных платформ, в частности, социальных сетей, происходит по модели минимального государственного вмешательства, что приводит к разного рода вопросам, требующим своего разрешения, зачастую осуществимого на основе существующей правоприменительной практики и полученного при коммуникации опыта в сети по регулированию указанных вопросов другими узлами сети.



### Список литературы:

1. 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: [http://ec.europa.eu/justice/dataprotection/reform/files/regulation\\_oj\\_en.pdf](http://ec.europa.eu/justice/dataprotection/reform/files/regulation_oj_en.pdf).
2. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ // «Собрание законодательства РФ», 07.01.2002, № 1 (ч. 1), ст. 3.
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // «Собрание законодательства РФ», 31.07.2006, № 31 (1 ч.), ст. 3451.
4. Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации» // «Собрание законодательства РФ», 03.07.1995, № 27, ст. 257.
5. Методические рекомендации по использованию сети Интернет в целях поиска информации о должниках и их имуществе (утв. ФССП РФ 30.11.2010 № 02-7) // Службы судебных приставов, № 1, 2011.
6. Бобровский С. Эволюция и искусственная жизнь // PC WEEK/RE. 2005. № 4. С. 32-33.
7. Кудашкин Я. В. Правовое обеспечение безопасности обработки персональных данных в сети Интернет: дис.... канд. юрид. наук. – М., 2019. 199 с.
8. Отчет TNS Web Index Report «Аудитория интернет-проектов» // URL: <http://mediascope.net/services/media/media-audience/internet/information/>.
9. Правила защиты информации о пользователях сайта VK.com // URL: <https://vk.com/privacy>.
10. Руденок Д. В. Социальные сети как источник информации // Вестник электронных и печатных МИ. 2016. № 1(24). С. 86-99.



11. Barnes J. A. Class and Committees in a Norwegian Island Parish // Human Relations. 1954. Vol. 7. P. 39-58.