



Data processing on digital platforms: topical issues of improving legislation and practice

S. V. Simonova¹

¹P. G. Demidov Yaroslavl State University, 14 Sovetskaya str., Yaroslavl 150003, Russian Federation

DOI: 10.18255/1996-5648-2022-4-642-649

Research article
Full text in Russian

The article is devoted to the analysis of current legal problems arising in the process of collecting, using and distributing users' personal data of modern digital platforms. The paper emphasizes that the issue of protecting user data has a significant legal component and allows to take a fresh look at the usual concept of privacy and the content of the right to privacy. On the example of the property of the network effect of digital platforms, the interest of users in building up large arrays of user data by platforms is substantiated and a conclusion is made about the key role of the authority to control the volume and fate of the information collected about a person in the content of the right to privacy.

Based on the experience of the European Union, the author substantiates the need to regulate in domestic legislation the system of requirements for the basic and subsequent settings for the confidentiality of digital services, the acts for designing the protection of personal data by operators who process such information. In addition to this, the author highlights advantages of legal regulation of the procedures for transferring data between digital platforms and exercising the right to be forgotten. As conclusions, recommendations are formulated aimed at developing transparency in the procedures for collecting personal data by platforms, countering parsing and leakage of personal data, as well as deformalizing the dissemination of personal information based on the concept of open data..

Keywords: digital platforms; personal data; privacy; users; leaks; data processing; services; network effect; confidentiality

INFORMATION ABOUT AUTHORS

Simonova, Snezhana V. | E-mail: snezh-simonova@yandex.ru
Cand. Sc. (Jurisprudence), Associate Professor

Funding: Yaroslavl State University (project VIP-014).



Обработка данных пользователей цифровых платформ: актуальные вопросы совершенствования законодательства и практик

С. В. Симонова¹

¹Ярославский государственный университет им. П. Г. Демидова, ул. Советская, 14,
Ярославль, 150003, Российская Федерация

DOI: 10.18255/1996-5648-2022-4-642-649
УДК 342.721

Научная статья
Полный текст на русском языке

Статья посвящена анализу актуальных правовых проблем, возникающих в процессе сбора, использования и распространения персональных данных пользователей современных цифровых платформ. В работе подчеркивается, что вопрос защиты пользовательских данных имеет значимую правовую составляющую и позволяет по-новому взглянуть на привычную концепцию приватности и содержание права на неприкосновенность частной жизни. На примере свойства сетевого эффекта цифровых платформ обосновывается заинтересованность пользователей в наращивании платформами больших массивов пользовательских данных и делается вывод о ключевой роли правомочия контроля объема и судьбы собираемой информации о человеке в содержании права на неприкосновенность частной жизни.

Опираясь на опыт Европейского союза, обосновывается необходимость регламентации в отечественном законодательстве системы требований к базовым и последующим настройкам конфиденциальности цифровых сервисов, процессам проектирования защиты личных данных операторами, которые ведут обработку подобной информации. В дополнение к этому автор освещает ряд преимуществ правовой регламентации процедур переноса данных между цифровыми платформами и реализации права на забвение. В качестве выводов формулируются рекомендации, направленные на развитие прозрачности процедур сбора платформами личных данных, противодействие парсингу и утечкам персональных данных, а также деформализации распространения личной информации на основе концепции открытых данных.

Ключевые слова: цифровые платформы; персональные данные; приватность; пользователи; утечки; обработка данных; сервисы; сетевой эффект; конфиденциальность

ИНФОРМАЦИЯ ОБ АВТОРАХ

Симонова, Снежана Владимировна | E-mail: snezh-simonova@yandex.ru
Кандидат юридических наук, доцент

Финансирование: ЯрГУ (проект VIP–14).

© Симонова С. В., 2022

Статья открытого доступа под лицензией CC BY (<https://creativecommons.org/licenses/by/4.0/>)

Общеизвестно, что феномен цифровой платформы¹ неразрывно связан с процессами обработки данных, основывается на этих процессах и без них немислим. Причем как в законодательстве, так и в юридической литературе обозначенная связь активно подчеркивается. Например, в отечественных правовых актах понятие платформы дается через призму информационной системы². Ученые справедливо отмечают, что сбор пользовательских данных образует сердцевину бизнес-модели современных цифровых платформ [1, с. 86–94]. Как видится, в «ковидные времена», когда объемы обрабатываемых в цифровой среде данных достигли беспрецедентных объемов, и особенно в 2022 году, актуальность этого тезиса повысилась в разы.

Что важно, в этом аспекте ценность имеют не только данные, предоставляемые пользователями платформам явно и напрямую (например, фамилия, имя, отчество, адрес электронной почты, номер телефона, вводимые при регистрации), но и «динамичная» информация, «генерируемая» поведением пользователей на самой платформе. Это, прежде всего, данные о просматриваемых страницах, лайках, поисковые запросы, покупки и пр. формы пользовательской активности. Как первая, так и вторая группа сведений уже давно однозначно определяется в контексте персональных данных – особого типа информации ограниченного доступа, а значит, и проблемы, связанные с процедурой обработки таких данных в границах цифровых платформ имеют не только технический, но и правовой контур, отражающий систему прав пользователей на свои данные и их защиту.

И здесь сложно не заметить такой нюанс: активное развитие платформенной экономики устойчиво влияет и на институт персональных данных, способствуя пересмотру традиционного и сложившегося десятилетиями содержания права на неприкосновенность частной жизни и режима конфиденциальности. Так, в доктринальных источниках не перестают повторять, что в настоящее время данные (в том числе и личные) – это своего рода новая цифровая «валюта», которая с легкостью обменивается на услуги бесплатных сервисов и имеет в значительном роде коммерческое значение [2, с. 119–120]. Что это, как не коммерциализация изначально конституционных благ и ценностей?

¹ Платформы могут предоставлять доступ к услугам, информации, товарам, капиталу, быть транзакционными и нетранзакционными, функционировать в B2B (business-to-business) или B2C (business-to-consumer) сегментах и пр. Яркими примерами платформ выступают видеохостинги, социальные сети, агрегаторы такси, вакансий, сервисы объявлений, маркетплейсы и пр.

² См.: Федеральный закон от 20.07.2020 № 211-ФЗ (ред. от 14.07.2022) «О совершении финансовых сделок с использованием финансовой платформы» // СЗ РФ. 2020. № 30, ст. 4737.

Вопрос о позитивной или негативной окраске отмеченной тенденции, а также о том, кому подобная коммерциализация выгодна, – отдельный и заслуживающий самостоятельного рассмотрения. И ответить на него невозможно лишь в контексте сугубо платформенных интересов, ведь интерес самих пользователей в наращивании платформами объемов агрегируемых данных – налицо. Эта заинтересованность напрямую определяется таким свойством современных платформ, как «сетевой эффект» [3, с. 43–50]: чем больше пользователей объединяет платформа, тем более ценной она становится с точки зрения удовлетворения потребностей и запросов пользователей. Например, сервис поиска такси, которым пользуется большое число водителей и пассажиров, более привлекателен по сравнению со своими скромными аналогами. Мы скорее будем использовать ту социальную сеть, в которой зарегистрировано большое число наших друзей и коллег, чем непопулярные в нашем окружении площадки. А функционал платформы (с точки зрения поиска, систематизации отображения результатов запросов и т. п.) будет более отлаженным лишь в случае, если алгоритмы платформы знают наши предпочтения и «натренировались» на данных похожих на нас профилей пользователей.

С учетом отмеченных наблюдений нельзя не обратить внимание на то, что развитие цифровых платформ идет бок о бок с содержательными изменениями категории приватности³. Вне всякого сомнения, частная жизнь уже давно не воспринимается как сфера жизнедеятельности, полностью защищенная от фактического и юридического доступа третьих лиц. Доступность (на законной основе) информации о человеке является важным условием многих правовых отношений, в которых вступают физические лица. Однако в современном понимании обеспечение неприкосновенности частной жизни уже немислимо без возможности сохранения анонимности человека при использовании отдельных цифровых сервисов и его контроля за информацией о себе [4, с. 213–214].

К слову, последний тезис в условиях активного использования ресурсов цифровых платформ предполагает интерес индивида в самостоятельном и осознанном решении вопроса о том, какими личными данными и в каком объеме делиться с сервисами, в каких целях предоставлять им доступ к личной информации и до какого момента. Все сказанное в целом составляет правомочие контроля за судьбой информации, которую мы сами передаем платформе или которую платформа собирает о нас. Более того, со временем появляется все больше правовых инструментов для подобного контроля: например, ряд наиболее значимых были с 2018 года предусмотрены

³ Термин «privacy» широко используется в международной практике, но не является типичным для российского права.

в Общем регламенте защиты персональных данных (GDPR) Европейского союза. Причем многие из них системно не выражены в российском правовом порядке.

Речь прежде всего идет о правиле спроектированной защиты персональных данных (privacy by design), предполагающем внедрение защиты данных в процессы разработки цифровых сервисов и в проектирование бизнес-процессов, а также о правиле конфиденциальности по умолчанию (privacy by default)⁴. Последнее означает требование к оператору (например, к цифровому сервису) о сохранении по умолчанию таких настроек конфиденциальности его продукта, которые являются минимально необходимыми для достижения конкретной цели обработки и не требуют от пользователя принятия каких-либо мер по защите своей конфиденциальности. Если пользователь и согласен на предоставление оператору новой информации о себе, то он может это сделать через процедуру согласия⁵.

Развитию механизма контроля пользователей за процессами обработки их данных цифровыми платформами способствует также провозглашение на уровне Европейского союза права на переносимость данных, обязывающее компании предоставлять пользователям их данные в машиночитаемом формате (например, данные, собранные одной цифровой платформой) в целях их использования у другого оператора (в рамках другой цифровой платформы) и объявлять возможность субъектов осуществлять дальнейшую передачу этих данных. Немаловажное значение в цифровой среде имеет и право пользователей цифровых платформ «быть забытыми», то есть возможность требовать от платформ полного удаления накопленной о себе информации.

Однако несмотря на отмеченное регулирование, ряд иных значимых международных ориентиров⁶, а также достигнутые успехи некоторых цифровых гигантов, реальная ситуация в части защиты данных пользователей цифровых платформ, увы, все еще далека от своего идеала. В этом есть вполне понятный экономический расчет, ведь объем собираемых данных напрямую может влиять на прибыль компаний, поэтому цифровым игрокам не всегда интересно снижать объемы сбора

⁴ См. ст. 25 Общего регламента защиты персональных данных (GDPR) Европейского Союза // GDPR TEXT. URL: <https://gdpr-text.com/ru/> (дата обращения: 30.09.2022).

⁵ Более подробно также см.: Руководство по 25 статье GDPR (Защита персональных данных: проектируемая и по умолчанию) в соответствии с Регламентом 2016/679 // GDPR TEXT. URL: <https://gdpr-text.com/ru/guidelines/pbd/> (дата обращения: 30.09.2022).

⁶ Речь идет, прежде всего, об актах Международного союза электросвязи (МСЭ), Организации экономического союза и развития (ОЭСР).

и уж тем более безвозвратно удалять уже «накопленное»⁷. Кроме того, нередко становится известно, что новые настройки приватности имеют «оборотную сторону» и, наоборот, упрощают слежку за пользователями, например включающими режим приватности.

Основываясь на материалах российской юридической практики, в целом можно выделить следующие проблемы в сфере защиты прав пользователей цифровых платформ на личные данные.

Во-первых, достаточно существенной видится проблема прозрачного сбора пользовательских данных. Российское законодательство в 2022 году было усилено целесообразными нормами, ограничивающими избыточный сбор персональных данных всеми операторами, в том числе и владеющими платформами. Речь идет прежде всего о новых требованиях к согласиям на обработку персональных данных (в части их предметности и однозначности), а также о недопустимости отказа в заключении и исполнении договора с потребителями, которые не считают нужным предоставлять несущественные для целей договора персональные данные⁸. Однако применение многих норм, регламентирующих сбор персональных данных, все еще оставляет желать лучшего. К сожалению, правила о политике конфиденциальности многих цифровых операторов на деле составляются формально и на шаблонной основе, без претворения в жизнь декларированных в них процедур. Кроме того, как видится, на законодательном уровне требует однозначного запрета т. н. парсинг (извлечение) пользовательских данных из открытых частей баз цифровых платформ (например, социальных сетей)⁹.

Во-вторых, обращает на себя внимание большое количество формализованных процедур, которыми на текущий момент сопровождается процесс распространения персональных данных в России при менее пристальном внимании к процедурам уничтожения персональных данных, востребованных в связи с формированием больших массивов данных в период пандемии [5, с. 46–50]. Общим основанием распространения пер-

⁷ Интересная тенденция была замечена осенью 2021 года: было зафиксировано, что ввод новых настроек конфиденциальности на технических устройствах способствовал снижению привлекательности акций некоторых сервисов. См., например: Новые настройки приватности Apple заставили доходы Snap упасть на 22 % // Хабр. URL: <https://habr.com/ru/news/t/585004/> (дата обращения: 30.09.2022).

⁸ См.: Федеральный закон от 01.05.2022 № 135-ФЗ «О внесении изменения в статью 16 Закона Российской Федерации «О защите прав потребителей» // СЗ РФ. 2022. № 18, ст. 3021.

⁹ В известном деле ООО «В Контакте» против ООО «Дабл» подобные действия были признаны нарушением исключительных прав владельца базы данных, при этом комплексная оценка «парсинга» с позиции Закона о персональных данных не приводилась. См.: Постановление Девятого арбитражного апелляционного суда от 08.07.2021 по делу № А40-18827/17 // Электронное правосудие. URL: <https://kad.arbitr.ru> (дата обращения: 30.09.2022).

сональных данных с 2021 года может выступать только письменное согласие субъекта на такое распространение, что требует получения такого согласия на каждый случай публикации личной информации (абсурд, но даже – для публикации программы мероприятий). Дифференциации для данных нет, хотя многие ученые предлагают ее вводить через режим открытых данных [6, с. 130–137]. В целом подобная строгость де-факто не способствует усилению защищенности пользовательских данных, которые по-прежнему распространяются в больших объемах свободно, а случаи утечек данных пользователей кратно растут. При этом институт ответственности за утечки не развит: в условиях отсутствия оборотных штрафов за утечки, слабых традиций гражданско-правовой защиты прав пользователей, пострадавших от утечек, практики отказа в возбуждении уголовных дел по фактам утечек ответственность компаний, как правило, ограничивается очень скромными штрафами¹⁰. Новый институт уведомления Роскомнадзора об инцидентах с персональными данными по состоянию на конец 2022 года пока не апробирован на практике.

Таким образом, как видим, правомочие контроля объема и судьбы обрабатываемых личных данных является ключевой составляющей современной концепции права на неприкосновенность частной жизни и приватности. Создание инструментов, возможностей и институтов, упрощающих и развивающих такой контроль, – ключевая задача как государства в целом, так и операторов цифровых платформ, которым важно действовать в этой части на основе единых принципов и стандартов. Последними могли бы стать требования к проектированию защиты персональных данных на этапе разработки платформ, гарантированные процедуры обеспечения конфиденциальности по умолчанию и перенесения данных. При этом текущее правовое регулирование персональных данных нуждается в пересмотре в части менее строгих требований к распространению данных и более строгих – к фактам утечек, понятие и санкции в отношении которых должны быть предусмотрены законодательно.

Ссылки

1. Алтухов А. В., Кашкин С. Ю. Правовая природа цифровых платформ в российской и зарубежной доктрине // Актуальные проблемы российского права. 2021. Т. 16. № 7. С. 86–94. DOI 10.17803/1994-1471.2021.128.7.086-094.

¹⁰ См.: Постановление мирового судьи судебного участка № 281 района Вешняки города Москвы от 08.07.2022 № 5-564/2022 // Портал единого информационного пространства мировых судей города Москвы. URL: <https://mos-sud.ru> (дата обращения: 30.09.2022).

2. Щербович А. А. Конфликты прав в регулировании онлайн-платформ в России // Сравнительное конституционное обозрение. 2021. № 6. С. 106-122. DOI 10.21128/1812-7126-2021-6-106-122.

3. Петров А. В. Сетевые эффекты и недобросовестная конкуренция на рынках цифровых платформ: дело Avito против Auto.ru // Предпринимательское право. 2020. № 4. С. 43–50.

4. Шадрин С. А. Содержание права на неприкосновенность частной жизни по российскому и европейскому законодательству // Актуальные проблемы российского права. 2018. № 9. С. 208-217. DOI 10.17803/1994-1471.2018.94.9.208-217.

5. Салихов Д. Р. Пандемия и персональные данные: как распространение новой коронавирусной инфекции бросает новые вызовы персональным данным // Конституционное и муниципальное право. 2021. № 3. С. 46-50. DOI 10.18572/1812-3767-2021-3-46-50.

6. Гонтарь Л. О. Защита персональных данных в условиях развития интернет-компаний: международно-правовое регулирование vs саморегулирование // Труды по интеллектуальной собственности. 2021. № 1–2. С. 116–140.