

Вероника Сергеевна Кубрак
Аспирант Департамента
правового регулирования
экономической деятельности
Финансового университета
при Правительстве РФ
E-mail: penskaya2015@mail.ru

Проблемы правового регулирования данных в контексте построения безопасной информационно-телекоммуникационной инфраструктуры

Аннотация. В последнее время актуализировалась проблема создания эффективной системы обеспечения информационной безопасности на уровне программного обеспечения, обработки и передачи данных. На основе анализа правовой доктрины и судебной практики через призму правовой культуры автор выявляет основные проблемы правового регулирования данных: 1) неопределенность правового режима данных; 2) проблемы конфиденциальности данных пользователей. В заключении автор работы приходит к выводу, что в целях поддержания баланса интересов между коммерциализацией данных и построением безопасной информационно-телекоммуникационной инфраструктуры необходимо совершенствование правового регулирования. Автором сделаны предложения по совершенствованию законодательства в двух направлениях – коммерциализации данных и построении безопасной информационно-телекоммуникационной инфраструктуры. В целях коммерциализации автор считает нужным признать данные в качестве самостоятельного объекта гражданских прав. Для повышения безопасности сервисов/программного обеспечения и защиты персональных данных пользователей необходимо: 1) установить повышенные требования к защите конфиденциальности при использовании данных, в частности определить, что в состав больших данных могут входить только неперсональные данные; в качестве способа получения неперсональных установить анонимизацию (безвозвратное удаление идентифицирующих данных).

Ключевые слова: регулирование информационно-телекоммуникационной инфраструктуры, данные, большие данные, технологии, конфиденциальность, правовой режим, правовая культура.

Veronika Sergeevna Kubrak
Postgraduate Student of the
Department of Legal Regulation of
Economic Activities Of Financial
University under the Government
of the Russian Federation

Issues Related to Legal Regulation of Data in the Context of Building Saved Informational Communicative Infrastructure

Annotation. *The relevance of the present paper is due to the fact that there is the problem of making effective system aimed to provide informational security at the software level as well as at the level of data processing and transmission; and this problem was actualized recently. The author analyzes legal doctrine and judicial practice in the context of legal culture to indicate the following issues of legal regulation of data: 1) uncertainty of data legal status; 2) the problem of users' data confidentiality. In the end the author concludes that there is the need to improve legal regulation in this sphere; the author believes that it can help to maintain the balance of interests between data commercialization and formation of saved informational telecommunication infrastructure. Thus the author suggests some concepts to improve legislation in two sectors, which are the commercialization of data and forming saved informational telecommunication infrastructure. To commercialize data the author claims that there is the need to recognize data as an independent object of civil rights. To strengthen safety of services or software and personal data the author suggests: 1) to established increased requirements to protecting the privacy when using the data, in particular, the author means to determine that big data can include unpersonalized information only; 2) to anonymize the way of getting unpersonalized data (irretrievable removal of identifying data).*

Keywords: *regulation of informational telecommunication infrastructure, data, big data, technologies, privacy, legal regime, legal culture.*

В настоящее время актуализируется проблема создания эффективной системы обеспечения информационной безопасности на уровне программного обеспечения и сервисов, предоставляемых с использованием Интернета, безопасности процессов обработки и передачи данных.

Дальнейшее развитие информационных технологий зависит от создания нормативной базы, построенной с позиций информационной безопасности, и формирования соответствующей правовой культуры в обществе. Вместе с внедрением информационных технологий в повседневную жизнь возрастает количество информационных угроз и их негативное влияние на жизнь общества и государства.

Вопросы правового регулирования данных тесно связаны с правовым регулированием информационных технологий.

Технологии — многогранное понятие, которое в широком смысле (для целей права) можно определить как совокупность способов, процессов, направленных на преобразование среды обитания или как совокупность методов, позволяющих решить конкретную задачу [1].

В связи с этим особую важность приобретают правовые исследования по вопросам регулирования сквозных цифровых технологий. «Сквозной» характер цифровых технологий выражается во взаимопроникновении технологий и их взаимном усилении друг друга. К сквозным технологиям относятся: большие данные, искусственный интеллект, робототехника, технология распределенных реестров, Интернет вещей, технологии виртуальной реальности и др.

Интенсификация использования технологии обработки больших объемов данных (технология больших данных), без которой невозможно развитие ряда других технологий, актуализирует проблему определения надежности данной технологии в контексте обеспечения конфиденциальности данных и проблему правового режима «больших данных».

В нормативно-правовой базе России такая дефиниция, как «большие данные», отсутствует, однако ее можно встретить в международных официальных документах, например, в Политике Европейской комиссии по большим данным [2]. «Большие данные» часто определяются как массивы структурированных или неструктурированных данных, обладающих большим объемом, разнообразием, высокой скоростью изменения или обработки.

Отмечая коммерческую ценность больших данных, ряд ученых приходит к выводу о необходимости установления правового режима для больших объемов данных, имеющих коммерческую ценность.

В научной литературе термин «большие данные» употребляется в нескольких аспектах: с одной стороны, как наборы структурированной и или неструктурированной информации; с другой стороны, как сама технология, т. е. способы и методы обработки больших объемов информации.

В контексте определения больших данных как массивов информации/данных в доктрине можно выделить два основных подхода к узакониванию больших данных: 1) как новый объект гражданских прав; 2) как база данных.

Ценными представляются выводы, касающиеся определения правового статуса больших данных через цифровой актив. Так, Ю. С. Харитонов, Л. В. Санникова предлагают легализовать «большие данные» путем введения нового объекта гражданских прав для блоков информации, а именно, цифрового актива; закрепить двойственность (дуализм) для данной категории данных [3].

А. И. Савельев предлагает определять «большие данные» через понятие «массив данных», отличительными особенностями которого являются большой объем и способность к обработке автоматизированными средствами для дальнейшего коммерческого использования [4].

Несмотря на всю привлекательность подхода к определению «больших данных» через цифровой актив или массив, существуют некоторые проблемы. Так, М. А. Рожкова обращает внимание, что в России рассмотрение больших данных в качестве самостоятельного оборотоспособного объекта встречает следующие ограничения:

1) информация имеет нематериальную природу, что не позволяет отнести ее к объектам вещных прав;

2) информация изъята из оборота как объект, оборотными выступают лишь права на нее (по аналогии с интеллектуальной собственностью) [5].

Данный подход уже известен на примере института интеллектуальной собственности: объектами гражданско-правовых сделок выступают не результаты интеллектуальной деятельности/средства индивидуализации как таковые, а исключительные права на них.

В науке существует позиция, согласно которой большие данные могут охраняться с помощью юридической конструкции — базы данных. Несмотря на логичность данного заключения, подобный подход имеет свои ограничения: 1) авторско-правовая охрана баз данных осуществляется в случае применения человеком «творческого труда», «новаторского подхода» при размещении данных внутри базы; 2) правовая охрана в качестве объекта смежных прав предоставляется при накоплении значительных объемов информации (в целях защиты инвестиций). При этом защиту получает именно целостность базы данных, а не данные сами по себе.

Вторая проблема, а именно проблема нарушения конфиденциальности обычно возникает при использовании больших пользовательских данных (или также социальных данных), которые могут пересекаться с особым режимом персональных данных.

Правовые аспекты использования больших данных в контексте конфиденциальности рассматривались рядом российских ученых. Ключевым риском при использовании больших пользовательских данных считается нарушение прав человека на неприкосновенность частной жизни.

Появление права на неприкосновенность частной жизни (privacy) обычно связывается со статьей С. Уоррена и Л. Брэндайса, изданной в 1890 г. в *Harvard Law Review*. Размышляя о конфиденциальности, авторы пришли к выводу, что «защита, предоставляемая мыслям, чувствам и эмоциям, выраженным посредством письма или искусства, в той мере, в какой она заключается в предотвращении публикации, является всего лишь примером обеспечения более общего права личности на то, чтобы ее оставили в покое» (the right to be left alone) [6].

Основные нарушения, которые могут возникать при использовании данной технологии: утечка данных; обработка неполных/неточных данных; дискриминация.

А. И. Савельев считает, что в целях защиты прав граждан на неприкосновенность частной жизни необходимо:

- 1) совершенствовать подходы к получению согласия субъекта на обработку;
- 2) обеспечение прозрачности процесса сбора данных;
- 3) внедрение саморегулирования для операторов персональных данных;
- 4) предоставление гражданам новых механизмов защиты прав [4].

Правовое регулирование данных представляет собой важный вопрос как с теоретической, так и практической точки зрения, способный вызвать научные дискуссии. Этот тезис можно подтвердить актуальной судебной практикой в сфере использования технологии больших данных.

В данном случае наиболее показательным является судебный спор между ООО «Дабл» и ООО «ВКонтакте», рассматривавшийся в 2017–2022 гг. ООО «Дабл» (ответчик) предоставляло услуги в сфере финансового скоринга (анализ кредитоспособности физических лиц) посредством автоматизированной обработки пользовательских данных социальной сети «ВКонтакте».

ООО «ВКонтакте» (истец) в свою очередь заявило о неправомерности сбора данных пользователей по причине того, что действия ответчика по сбору данных нарушают исключительные права истца на базу данных.

В первой инстанции суд отказал в удовлетворении требований заявителя на основе нескольких обстоятельств:

- 1) суд пришел к выводу о недоказанности факта создания базы данных.

Базой данных является совокупность (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны ЭВМ;

- 2) суд пришел к выводу о недоказанности факта возникновения исключительных прав на базу данных.

Изготовителем признается лицо, организовавшее создание базы и работу по сбору материалов.

Исключительные права предоставляются изготовителю в связи с существенными затратами (финансовыми, временными и др.) по созданию и наполнению базы данных.

Это аргументировалось также путем отсылки к правилам «ВКонтакте», которые подтверждали, что именно пользователь самостоятельно формирует содержание своей персональной страницы;

3) суд пришел к выводу о недоказанности факта извлечения данных из базы данных ответчиком.

ООО «Дабл» обращалось к общедоступным данным пользователей в соответствии с режимом конфиденциальности страницы, настроенной физическим лицом [7].

В дальнейшем суды отменили данное решение. Судебная практика выработала следующую позицию:

1. Исключительные права на базу данных, включающую пользовательские данные, признаются.

Суды признали, что данные, содержащиеся в социальной сети «ВКонтакте» постоянно добавляются и изменяются – на создание и поддержание за весь период формирования были понесены значительные затраты.

Аргумент о том, что информация вносится пользователями самостоятельно, был отклонен, поскольку не учитываются иные затраты, связанные с созданием и поддержанием базы данных; не имеет правового значения способ внесения данных в базу.

2. Извлечение пользовательских данных признается неправомерным.

Суд отклонил довод о том, что обрабатывались общедоступные данные пользователей. В соответствии с правилами социальной сети пользователям гарантируется защита информации от третьих лиц.

Благодаря анализу судебной практики мы можем выявить несколько существенных проблем.

Во-первых, неопределенность правового регулирования в связи с коммерциализацией данных. Интерес различных структур к введению данных в коммерческий оборот высок, однако представляется затруднительным применить к ним разработанный правовой инструментарий. При распространении режима базы данных на «большие данные» как оценить капиталовложения/усилия по сбору открытых данных/данных из разных источников? Особенно в случае, если они собраны в автоматическом режиме.

Во-вторых, применительно к «большим пользовательским данным» актуален вопрос: могут ли личные данные пользователей входить в состав базы данных (и охраняться авторско-правовым режимом), если на них должен распространяться особый правовой режим – режим персональных данных?

Распространение режима базы данных на данные пользователей без правовых оснований может быть рассмотрено как нарушение правил обработки персональных данных.

Существует два подхода к данному вопросу: 1) персональные данные входят в состав больших данных; 2) в состав больших данных могут входить только «неперсональные» данные.

Под неперсональными данными понимаются личные данные, прошедшие процессы обезличивания либо анонимизации. Обезличивание (псевдонимизация) данных представляет собой метод, результатом которого является

невозможность идентификации индивида без дополнительной информации. Анонимизация – метод, позволяющий полностью удалить идентифицирующую информацию из состава данных. М. А. Рожкова отмечает, что наиболее перспективным методом является именно анонимизация, т. к. представляет собой необратимый процесс, без возможности становления неперсональных обратно персональными [8].

Таким образом, в целях развития правовой культуры мы приходим к выводам о необходимости совершенствования законодательства по двум направлениям: с одной стороны, нужны изменения в законодательство в части коммерциализации данных, с другой стороны, требуется установление дополнительных мер защиты в целях построения безопасной информационно-телекоммуникационной инфраструктуры.

В целях коммерциализации данных считаем нужным признать данные в качестве самостоятельного объекта гражданских прав. Для повышения безопасности сервисов/программного обеспечения и защиты персональных данных пользователей необходимо: 1) установить повышенные требования к защите конфиденциальности при использовании данных, в частности определить, что в состав больших данных могут входить только неперсональные данные; в качестве способа получения неперсональных данных установить анонимизацию (безвозвратное удаление идентифицирующих данных).

Пристатейный библиографический список

1. История техники // Encyclopedia Britannica. Encyclopedia Britannica Online. Encyclopedia Britannica Inc. 2016. С. 14–15.
2. Большие данные [Электронный ресурс]. URL: <https://digital-strategy.ec.europa.eu/en/policies/big-data> (дата обращения : 01.08.2022).
3. Санникова Л. В., Харитонов Ю. С. Цифровые активы: правовой анализ. М. : 4 Принт, 2020.
4. Савельев А. И. Направления регулирования Больших данных и защита неприкосновенности частной жизни в новых экономических реалиях // Закон. 2018. № 5. С. 122–144.
5. LegalTech, FinTech, RegTech etc: правовые аспекты использования цифровых технологий в коммерческой деятельности / [М. А. Рожкова, А. А. Алексейчук, О. В. Белая и др.]. М. : Статут : IP Club, 2021. С. 135–136.
6. Уоррен С., Брандейс Л. Право на неприкосновенность частной жизни // Harvard Law Review. 1980. № 4. Р. 206.
7. Решение Арбитражного суда г. Москвы по делу № А40-18827/17-110-180 [Электронный ресурс]: А40-18827-2017__20171012.pdf (arbitr.ru) (дата обращения: 28.08.2022).
8. Рожкова М. А., Глонина В. Н. Персональные и неперсональные данные в составе больших данных // Право цифровой экономики – 2020. Ежегодник-антология / рук. и науч. ред. М. А. Рожкова. М. : Статут, 2020.

References

1. Istoriya tekhniki [History of technology] // Encyclopedia Britannica. Encyclopedia Britannica Online. Encyclopedia Britannica Inc. 2016. Pp. 14–15.

2. Bol'shie dannye [Big Data] [Elektronnyj resurs]. URL: <https://digital-strategy.ec.europa.eu/en/policies/big-data> (access date: 01.08.2022).
3. Sannikova L. V., Haritonova YU. S. Cifrovye aktivy: pravovoj analiz. [Digital assets: legal analysis] M. : 4 Print Publishing house, 2020.
4. Savel'ev A. I. Napravleniya regulirovaniya Bol'shih dannyh i zashchita neprikosновенности chastnoj zhizni v novyh ekonomicheskikh realiyah // Zakon. [Directions of Big Data regulation and protection of privacy in new economic realities // Law] 2018. No. 5. Pp. 122–144.
5. LegalTech, FinTech, Regtech ect : pravovye aspekty ispol'zovaniya cifrovyyh tekhnologij v kommercheskoj deyatelnosti [LegalTech, FinTech, Regtech : legal aspects of the use of digital technologies in commercial activities: collective monograph] / [M. A. Rozhkova, A. A. Aleksejchuk, O. V. Belaya and others]. M. : Statut : IP Club [Publishing house], 2021. Pp. 135–136.
6. Uorren S., Brandeys L. Pravo na neprikosновенnost' chastnoj zhizni [The right to privacy] // Harvard Law Review. 1980. No. 4. P. 206.
7. Reshenie Arbitrazhnogo suda g. Moskvy po delu № A40-18827/17-110-180. [Decision of the Moscow Arbitration Court in case No. A40-18827/17-110-180] / [Elektronnyj resurs]: A40-18827-2017__20171012.pdf (arbitr.ru) (access date: 28.08.2022).
8. Rozhkova M. A., Glonina V. N. Personal'nye i nepersonal'nye dannye v sostave bol'shih dannyh // Pravo cifrovoj ekonomiki – 2020. Ezhegodnik-antologiya [Personal and non-personal data as part of big data // Law of the Digital Economy - 2020. Anthology Yearbook] / advisor and academic editor is M. A. Rozhkova. M. : Statut [Publishing house]. 2020.

Александра Георгиевна Марценюк
Аспирант Иркутского
института (филиала)
ВГУЮ (РПА Минюста России)
E-mail: ezhik94@mail.ru

Исполнительский иммунитет единственного жилья: в поисках баланса интересов кредиторов и должника

Аннотация. Актуальность статьи состоит в анализе появившейся в последнее время обширной судебной практики, складывающейся относительно применения пределов исполнительского иммунитета в отношении единственного жилья в делах о банкротстве. Предметом исследования являются положения российского законодательства о несостоятельности (банкротстве), а также правоприменительная практика в сфере защиты жилищных прав граждан при разрешении вопросов относительно применения пределов исполнительского иммунитета. Цель работы заключается в необходимости обозначить ключевые моменты, требующие законодательного урегулирования вопросов, касающихся применения пределов исполнительского иммунитета с учетом соблюдения баланса интересов между кредиторами и должником. Основные методы проведенного исследования: логический и метод анализа. Новизна работы сводится к попытке сформулировать блок вопросов, требующих разрешения на законодательном уровне, в частности,