УДК 34.096

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ БИЗНЕСА: К ВОПРОСУ О СООТНОШЕНИИ ЧАСТНОПРАВОВЫХ И ПУБЛИЧНО-ПРАВОВЫХ МЕХАНИЗМОВ

Рогиз И.В.[1]

магистрант,

Белгородский государственный национальный

исследовательский университет,

Белгород, Россия

Аннотация. Статья посвящена соотношению частноправовых и публично-правовых способов защиты персональных данных клиентов в предпринимательской деятельности. В центре анализа находится положение бизнеса как оператора персональных данных, который использует клиентскую информацию в продажах, сервисном обслуживании, маркетинге, цифровых платформах и взаимодействии с подрядчиками. Раскрывается значение публично-правовых требований к обработке и защите данных, включая обязанности оператора, меры информационной безопасности и административную ответственность за нарушения. Отдельное внимание уделяется частноправовым инструментам: договорному регулированию, политике обработки персональных данных, условиям передачи данных подрядчикам, требованиям о прекращении незаконной обработки и распределению ответственности между оператором и привлеченными лицами. Обосновывается вывод о том, что эффективная защита клиентских данных возможна только при сочетании государственного контроля и договорно-правовой дисциплины самого бизнеса.

[1] **Научный руководитель: В.С. Синенко**, доцент кафедры трудового и предпринимательского права юридического института НИУ «БелГУ», Белгородский государственный национальный исследовательский университет, г. Белгород, Россия.

Ключевые слова: персональные данные, клиентские данные, оператор персональных данных, бизнес, частноправовая защита, публично-правовое регулирование, согласие на обработку данных, утечка данных, цифровые платформы, конфиденциальность.

PROTECTION OF PERSONAL DATA OF BUSINESS CUSTOMERS: ON THE QUESTION OF THE CORRELATION BETWEEN PRIVATE AND PUBLIC LAW MECHANISMS

Rogiz I.V.
Master's student,
Belgorod State National Research University,
Belgorod, Russia

Annotation. The article is devoted to the correlation between private and public law methods of protecting personal data of clients in business activities. At the center of the analysis is the position of the business as a personal data operator that uses customer information in sales, service, marketing, digital platforms and interaction with contractors. The importance of public law requirements for the processing and protection of data, including the obligations of the operator, information security measures and administrative liability for violations, is revealed. Special attention is paid to private law instruments: contractual regulation, personal data processing policy, conditions for the transfer of data to contractors, requirements to stop illegal processing and the distribution of responsibility between the operator and the parties involved. The conclusion is substantiated that effective protection of client data is possible only with a combination of state control and contractual and legal discipline of the business itself.

Keywords: personal data, customer data, data controller, business, privacy protection, public law regulation, consent to data processing, data leakage, digital platforms, privacy.

Защита персональных данных клиентов для бизнеса на современном этапе развития общественных отношений уже не может рассматриваться исключительно как вопрос технической безопасности или формального согласия на сайте или ином аналогичном ресурсе. Клиентские данные участвуют в продажах, маркетинге, скоринге, сервисной поддержке, доставке, бонусных программах, работе мобильных приложений и цифровых платформ. Поэтому бизнес одновременно получает экономическую выгоду от обработки данных и принимает на себя повышенный правовой риск. Ошибка здесь редко остается внутри самой компании. Так, утечка клиентской базы, незаконная рассылка, передача данных подрядчику без надлежащего поручения или сбор избыточных сведений могут повлечь административные санкции, гражданско-правовые требования, репутационные потери и снижение доверия потребителей.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» определяет персональные данные как «любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу», а оператором признает юридическое или физическое лицо, которое организует или осуществляет обработку персональных данных, определяет цели, состав данных и действия с ними [2]. Таким образом, интернет-магазин, банк, медицинская клиника, агрегатор услуг, туроператор, образовательная платформа, сервис доставки почти всегда выступают операторами, если собирают телефоны, адреса, паспортные данные, платежные сведения, историю заказов или иные данные клиента. Законодатель намеренно закрепил достаточно широкую формулировку, поэтому попытка вывести клиентскую информацию из режима персональных данных обычно выглядит слабой защитной позицией.

Публично-правовой механизм строится вокруг обязательных требований оператора. Статья 18.1 Федерального закона «О персональных данных» требует от оператора принимать меры, необходимые и достаточные

для выполнения обязанностей, а также опубликовать или иным образом обеспечить доступ к политике обработки персональных данных. Статья 19 того же закона обязывает принимать правовые, организационные и технические меры для защиты данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления и распространения. В этом блоке государство действует императивно, не спрашивая, удобно ли бизнесу вести реестр обработок, публиковать политику, ограничивать доступ сотрудников, настраивать информационные системы и контролировать подрядчиков. Это обязательная инфраструктура законной обработки.

В.Д. Рузанова точно показывает, почему одних публичных запретов недостаточно. В научной статье автора представлен следующий тезис: «Одним из направлений усиления безопасности персональных данных является включение мер частноправового воздействия в применяемый охранительный механизм» [6, 78]. В современных условиях такая позиция принципиальна, так как публичное право дисциплинирует оператора через обязанности, надзор и санкции, но клиенту как частному лицу нужна еще возможность защищать свой интерес в конкретном конфликте, например, требовать прекращения нарушения, удаления данных, возмещения убытков, компенсации морального вреда, доказывать нарушение условий договора или политики конфиденциальности.

Частноправовой механизм проявляется прежде всего в договорной и деликтной плоскости. Клиент передает данные в рамках покупки товара, оказания услуги, регистрации в приложении, договора с банком или медицинской организацией. Значит, обработка данных становится частью доверительного коммерческого взаимодействия. Политика обработки персональных данных, согласие, пользовательское соглашение, договор с клиентом, договор поручения обработки с подрядчиком – все это не заменяет закон, но конкретизирует правовой режим данных в частной связи между

лицами. Если компания обещает использовать данные только для доставки товара, а затем передает их маркетинговым партнерам, нарушение имеет не только административный, но и частноправовой смысл: клиент вправе говорить о нарушении его автономии, ожиданий конфиденциальности и условий взаимодействия.

Именно здесь важно не противопоставлять частное и публичное право. В.Д. Рузанова в ранее упомянутом исследовании пишет, что законодательство о персональных данных «должно устанавливать баланс между частными интересами субъектов персональных данных и интересами общества и государства», а выполнение этой роли обеспечивается «применением публичных и частных методов правового регулирования» [6, 79]. Для бизнеса это означает смешанный режим ответственности. Государство через Роскомнадзор и Кодекс Российской Федерации об административных правонарушениях [1] наказывает за нарушение обязательных требований, но частное лицо остается самостоятельным носителем права, а не только поводом для проверки. Если публичная санкция обеспечивает поступление денежных средств в бюджет, то частноправовая защита направлена уже на восстановление положения конкретного клиента.

Наиболее чувствительный публично-правовой блок сегодня связан с утечками информации. Статья 13.11 КоАП РФ предусматривает специальные составы за нарушение законодательства в области персональных данных, включая невыполнение обязанности уведомить уполномоченный орган о факте неправомерной или случайной передачи данных, а также ответственность за действия оператора, повлекшие неправомерную передачу информации, включающей персональные данные. При повторных крупных нарушениях для юридических лиц предусмотрен оборотный штраф от 1 до 3 процентов выручки, но не менее 20 миллионов рублей и не более 500 миллионов рублей. Такая модель показывает, что утечка клиентских данных

стала рассматриваться не как техническая оплошность, а как серьезный публичный риск и самостоятельный вид правонарушения.

Однако штраф сам по себе не решает проблему клиента. Е.И. Казакевич обоснованно указывает, что «представляется обоснованным распространить действие законодательства о защите прав потребителей на отношения субъекта персональных данных с оператором» [3, 43]. Направление мысли Е.И. Казакевич представляется абсолютно верным. Действительно, клиент цифрового сервиса часто слабее оператора не только информационно, но и организационно. Он не знает, где хранятся данные, кто имеет доступ, каков реальный круг подрядчиков и какие алгоритмы используются. Поэтому частноправовая защита должна учитывать асимметрию между бизнесом и клиентом, а не исходить из равенства, которого фактически нет.

Отдельную группу рисков создают цифровые платформы. А.С. Кошель, Я.И. Кузьминов, Е.В. Кручинская и Б.В. Лесив, рассматривая возможности нахождения «регуляторного оптимума деятельности цифровых платформ» отмечают: «второй этап характеризуется признанием значимости защиты персональных данных в условиях растущего влияния цифровых платформ и принятием соответствующих законодательных актов» [4, 15]. Для бизнеса платформенного типа персональные данные являются почти производственным ресурсом. Здесь публично-правовой контроль должен ограничивать злоупотребление массивами данных, а частноправовые инструменты должны давать пользователю понятные права: узнать цели обработки, отказаться от избыточных рассылок, потребовать удаления данных, оспорить незаконную передачу третьим лицам.

Особой зоной, требующей отдельного внимания, выступают биометрия и иные чувствительные данные. Е.Е. Фролова и А.М. Берман обоснованно пишут о том, что: «Ключевая трудность повсеместного использования биометрических данных связана с необходимостью их защиты. Получение доступа к таким данным – безусловная цель киберпреступников» [7, 77]. В

обычных клиентских данных риск часто можно снизить заменой номера телефона, карты или пароля. Биометрические данные устроены иначе, так как к ним относится лицо, голос, отпечаток пальца, которые невозможно просто «перевыпустить». Поэтому бизнесу, использующему биометрию для идентификации, оплаты или доступа к услугам, недостаточно получить формальное согласие. Нужны повышенные технические меры, минимизация данных и реальная альтернатива для клиента.

М.Н. Малеина применительно к вендинг-бизнесу делает показательный вывод: «обработка вендинговым автоматом персональных данных покупателей без их согласия в любом виде (включая сбор, запись, накопление, хранение, использование и пр.) незаконна» [5, 69-70]. Данный пример важен, так как он иллюстрирует вывод, который выходит далеко за пределы купли-продажи с использованием вендинг-автоматов. Это обусловлено тем, что современный бизнес все чаще собирает данные через кассы самообслуживания, приложения, терминалы, камеры, программы лояльности. Само собой, технологическая незаметность сбора не отменяет правового требования, в соответствии с которым клиент должен понимать, что именно собирается, зачем и на каком основании.

Значим и вопрос подрядчиков. Бизнес редко обрабатывает данные полностью самостоятельно. CRM (управление взаимоотношениями с клиентами), облачные хранилища, сервисы рассылок, колл-центры, платежные агрегаторы и службы доставки получают доступ к клиентской информации. Часть 5 статьи 6 Федерального закона «О персональных данных» прямо устанавливает: если оператор поручает обработку персональных данных другому лицу, «ответственность перед субъектом персональных данных за действия указанного лица несет оператор», а лицо, осуществляющее обработку по поручению, отвечает перед оператором [2]. Поэтому договор с подрядчиком должен содержать не общие юридически бессодержательные формулировки о конфиденциальности, а перечень данных, цели и операции

обработки, требования к защите, обязанность подтверждать принятые меры, порядок уведомления об инциденте и ответственность за нарушение.

Подводя итог, соотношение частноправовых и публично-правовых механизмов защиты персональных данных клиентов бизнеса можно описать следующим образом: публичное право задает обязательный минимум поведения оператора, частное право превращает этот минимум в защищаемый интерес конкретного клиента и в договорную дисциплину контрагентов. Для бизнеса безопасная модель начинается не с внешне «красивой» политики конфиденциальности, располагающейся на сайте компании, а с карты данных, в которой указывается: какие сведения собираются, для какой цели, на каком основании, где хранятся, кому передаются, когда и при каких условиях уничтожаются. Публичный механизм отвечает на вопрос, выполнил ли оператор требования закона. Частноправовой – восстановлены ли интересы клиента и правильно ли распределены риски между бизнесом, подрядчиком и субъектом данных.

Именно сочетание этих механизмов дает реальную защиту. Если оставить только публичный контроль, клиент превращается в объект административной проверки. Если оставить только частноправовые иски, защита станет слишком дорогостоящей и медленной для большинства граждан. Поэтому эффективная модель должна быть смешанной: надзор, штрафы и обязательные технические меры со стороны государства; договорная прозрачность, компенсационные требования, конфиденциальность и ответственность подрядчиков со стороны частного права. Для бизнеса такой подход к регулированию является ключевым условием доверия со стороны клиентов. Клиентские данные сегодня являются активом, но это актив с чужой личной сферой внутри, и обращаться с ним как с обычным коммерческим ресурсом юридически уже невозможно, особенно в условиях продолжающихся процессов цифровизации различных сфер предпринимательской деятельности и угрозы роста киберпреступлений.

Библиографический список:

1. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (ред. от 02.05.2026) // Собрание законодательства РФ. – 2002. – № 1. – Ст. 1.

2. О персональных данных : Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. – 2006. – № 31. – Ст. 3451.

3. Казакевич, Е.И. Защита прав и свобод человека при обработке персональных данных в период цифровой трансформации / Е.И. Казакевич // Уральский журнал правовых исследований. 2022. № 4. С. 36-46.

4. Кошель, А.С., Кузьминов, Я.И., Кручинская, Е.В. Поиск регуляторного оптимума деятельности цифровых платформ (сравнительный анализ) / А.С. Кошель, Я.И. Кузьминов, Е.В. Кручинская [и др.] // Право. Журнал Высшей школы экономики. – 2025. – Т. 18. – № 2. С. 4-58.

5. Малеина, М.Н. Договор продажи с использованием автоматов в структуре вендинг-бизнеса / М.Н. Малеина // Право. Журнал Высшей школы экономики. – 2024. – Т. 17. – № 2. – С. 51-73.

6. Рузанова, В.Д. Персональные данные как гражданско-правовая категория / В.Д. Рузанова // Правовое государство: теория и практика. – 2022. – № 3. – С. 77-83.

7. Фролова, Е.Е., Берман, А.М. Способы волеизъявления сторон в условиях цифровой трансформации: актуальные тренды правоприменения / Е.Е. Фролова, А.М. Берман // Право. Журнал Высшей школы экономики. – 2024. – Т. 17. – № 3. – С. 57-83.