

ПРАВОВЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НА МАРКЕТПЛЕЙСАХ

В статье рассматриваются правовые проблемы защиты персональных данных пользователей маркетплейсов. Анализируются три основные проблемы: формальный характер согласия на обработку данных, частые утечки информации и сложность доказывания вины оператора. Приводится практический пример из жизни. Предлагаются пять конкретных мер по совершенствованию законодательства: осознанное согласие, обязательное уведомление об утечках, презумпция вины маркетплейса, штрафы, привязанные к выручке, и право на простое удаление данных. Сделан вывод о необходимости точечной настройки правового регулирования в сфере защиты персональных данных.

The article examines legal issues of personal data protection on marketplaces. Three main problems are analyzed: the formal nature of consent to data processing, frequent data leaks, and the difficulty of proving the operator's fault. A practical example is provided. Five specific measures for improving legislation are proposed: informed consent, mandatory breach notification, presumption of marketplace guilt, revenue-based fines, and the right to easy data deletion. The conclusion highlights the need for targeted adjustments in personal data protection regulation.

Ключевые слова: персональные данные; маркетплейс; интернет-торговля; защита информации; утечка данных; согласие на обработку; цифровые права; законодательство Республики Беларусь.

Key words: personal data; marketplace; e-commerce; data protection; data breach; consent to processing; digital rights; legislation of the Republic of Belarus.

С каждым годом интернет-торговля в Беларуси занимает все более прочное место в жизни людей, и такие маркетплейсы, как Wildberries, Ozon и другие, стали привычной платформой для покупок благодаря своему удобству и доступности. Однако вместе с удобством возникает серьезная проблема, связанная с безопасностью личной информации, потому что при регистрации на подобных сайтах пользователь передает свои персональные данные, включая фамилию, имя, адрес, номер телефона, а нередко и данные банковской карты, при этом далеко не все задумываются о том, как эти данные хранятся, кто имеет к ним доступ и что произойдет в случае их утечки.

В соответствии с Законом Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» под персональными данными понимается любая информация, позволяющая идентифицировать физическое лицо, и это не только паспортные данные, но и адрес проживания, номер мобильного телефона, сведения о банковской карте, а в некоторых случаях даже фотография. На маркетплейсах покупатель вынужден предоставлять весь этот объем сведений, чтобы оформить заказ, и при этом он практически не контролирует дальнейшее использование своих данных.

Одна из главных проблем заключается в том, что согласие на обработку персональных данных, которое пользователь дает при регистрации, зачастую носит формальный характер, поскольку вместо того, чтобы четко и понятно информировать о том, какие данные собираются, с какой целью и кому они будут переданы, маркетплейсы прячут эту информацию в длинных пользовательских соглашениях на десятки страниц. Пользователь, желая быстро оформить заказ, ставит галочку «Я согласен», не читая условия, и в результате автоматически разрешает передачу своих данных службам доставки, партнерским организациям, рекламным сетям и другим третьим лицам, тогда как закон требует, чтобы согласие было информированным, но на практике это требование почти не выполняется.

Еще одной острой проблемой являются утечки персональных данных, и за последние несколько лет в средствах массовой информации неоднократно появлялись сообщения о том, что базы данных крупных маркетплейсов оказывались в открытом доступе, в результате чего в руки мошенников попадали номера телефонов, адреса, история заказов и даже данные банковских карт. После таких утечек злоумышленники начинали обзванивать людей, представляясь сотрудниками службы безопасности, и под различными предлогами выманивали деньги, и хотя

законодательство предусматривает ответственность операторов персональных данных за подобные инциденты, размеры штрафов зачастую несопоставимы масштабам бизнеса крупных маркетплейсов, и это не создает достаточного стимула для вложения средств в защиту информации.

Третья проблема связана с трудностью доказывания вины, потому что если после совершения покупки на маркетплейсе персональные данные покупателя оказываются у мошенников, установить, по чьей вине произошла утечка, крайне сложно: данные могли быть похищены у самого маркетплейса, у продавца, у курьерской службы или у самого покупателя. В соответствии с действующим законодательством бремя доказывания лежит на потерпевшем, т. е. на покупателе, однако обычный человек не обладает ресурсами для проведения технического расследования, и в результате маркетплейс всегда может заявить, что он не причастен к утечке, а виноват продавец, либо сослаться на отсутствие доказательств.

Ситуацию, описанную выше, хорошо иллюстрирует пример из практики, когда минчанка Елена (имя изменено по этическим соображениям) заказала на одном из маркетплейсов наушники в подарок, и через несколько дней ей позвонил мужчина, который представился сотрудником того же маркетплейса. Он назвал ее полное имя, адрес доставки и последние четыре цифры банковской карты, после чего сообщил, что заказ завис и для его подтверждения необходимо продиктовать код из смс-сообщения, и женщина продиктовала код, после чего с ее карты было списано 500 р. В милиции возбудили уголовное дело, однако установить личность мошенников не удалось, а на обращение к маркетплейсу был получен ответ, что площадка не передает данные третьим лицам, кроме продавца и службы доставки, и что проблема, вероятно, возникла по вине продавца, который оказался организацией, прекратившей деятельность сразу после совершения данной продажи.

Представляется, что сложившаяся ситуация требует изменений в подходе к правовому регулированию защиты персональных данных, и в первую очередь необходимо сделать согласие пользователя на обработку данных действительно осознанным, для чего вместо единого документа, содержащего все условия, целесообразно разбить согласие на несколько отдельных пунктов: на передачу данных службе доставки, на получение рекламных рассылок, на передачу данных партнерам, причем каждый из этих пунктов пользователь должен подтверждать отдельно, и отказ от одного из них не должен препятствовать совершению покупки.

Вторым важным направлением является введение обязательного уведомления об утечках данных, и если произошел инцидент, в результате которого персональные данные пользователей оказались скомпрометированы, маркетплейс должен в течение суток сообщить об этом каждому пострадавшему лицу, а также опубликовать информацию на своем сайте, причем уведомление должно содержать не общие фразы, а конкретные сведения: какие именно данные утекли, когда произошла утечка и какие меры приняты для предотвращения подобных ситуаций в будущем.

Третье направление связано с перераспределением бремени доказывания, потому что в настоящее время потерпевший должен доказывать вину оператора персональных данных, и предлагается установить презумпцию вины маркетплейса: если данные покупателя были использованы мошенниками после совершения покупки на данной площадке, именно маркетплейс должен доказать, что он принял все необходимые меры для их защиты и что утечка произошла не по его вине, и такой подход стимулировал бы операторов более ответственно относиться к безопасности.

Четвертое предложение касается размера штрафов за нарушения в сфере защиты персональных данных, поскольку действующие в Беларуси штрафы даже в максимальном размере для крупных маркетплейсов не являются существенными, и более эффективной мерой было бы установление штрафов, привязанных к выручке компании, например в размере от одного до трех процентов годового оборота, что создало бы реальный экономический стимул для вложения средств в информационную безопасность.

Наконец, пятое направление касается реализации права пользователя на удаление своих данных, и хотя действующее законодательство предусматривает такое право, на практике воспользоваться им непросто, потому что на многих маркетплейсах отсутствует кнопка «Удалить аккаунт» в личном кабинете, а для удаления данных требуется писать заявление в службу поддержки, ждать ответа и подтверждать личность, причем в некоторых случаях данные продолжают храниться даже после формального удаления аккаунта, поэтому представляется необходимым законодательно закрепить обязанность маркетплейсов предоставлять пользователю простой и понятный механизм полного удаления всех персональных данных в один клик.

Подводя итог, можно сказать, что маркетплейсы стали неотъемлемой частью современной жизни, предлагая удобство и широкий выбор товаров, однако удобство не должно достигаться ценой потери контроля над личной информацией. Законодательство Республики Беларусь, в частности Закон «О защите персональных данных», заложило необходимую правовую основу, но практика применения выявила пробелы, требующие устранения, и такие меры, как осознанное согласие, обязательное уведомление об утечках, презумпция вины оператора, соразмерные штрафы и реальная возможность удалить свои данные, позволят сделать защиту персональных данных на маркетплейсах более эффективной. Пока же каждый покупатель вынужден полагаться только на свою осторожность, что в условиях растущих цифровых рисков является недостаточным.

Список использованной литературы

1. **О защите** персональных данных : Закон Респ. Беларусь от 7 мая 2021 г. № 99-З // ЭТАЛОН: информ.-поисковая система (дата обращения: 05.04.2026).
2. **Ковалёва, И. В.** Проблемы правового регулирования персональных данных в сети Интернет / И. В. Ковалёва // Журнал правовых исследований. – 2023. – № 2. – С. 45–52.
3. **Утечка** данных пользователей Wildberries: что известно и какие риски // CNews.ru. – 2023. – 12 окт. – URL: <https://www.cnews.ru> (дата обращения: 20.03.2026).
4. **Судебная** практика по спорам о защите персональных данных за 2023 год / Верховный Суд Республики Беларусь // Судовы веснік. – 2024. – № 2. – С. 33–38.