



ПРАВОВОЕ РЕГУЛИРОВАНИЕ БОЛЬШИХ ДАННЫХ В ЭЛЕКТРОННОЙ КОММЕРЦИИ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Хакимов Асадбек Ботир угли

*Магистрант Ташкентского государственного
юридического университета*

e-mail: asadbekkhakimov421@gmail.com

Актуальность В современную эпоху цифровой экономики сбор и анализ больших данных (Big Data) стали неотъемлемой частью электронной коммерции. Электронные торговые площадки и онлайн-сервисы ежедневно генерируют и обрабатывают огромные массивы информации о пользователях – от истории покупок до поведенческих факторов. В Узбекистане наблюдается бурный рост рынка e-commerce: по данным исследования KPMG, объём электронной торговли в 2020 году достиг 150 млн долл. США, а в 2022 году – 311 млн долл. США, что в 2,5 раза превышает показатель 2018 года [3]. Соответственно экспоненциально растёт объём собираемых и обрабатываемых персональных данных граждан при оказании электронных услуг [3]. Если использование больших данных не будет надлежащим образом регулируемо, возникают риски утечки конфиденциальной информации, нарушения права на частную жизнь и мошенничества с персональными данными [3].

Защита персональных данных стала приоритетной задачей во всем мире: по состоянию на 2021 год 128 из 194 стран мира (66%) уже приняли национальные законы о персональных данных [4]. Международный тренд показывает, что доверие пользователей и успешное развитие цифровой экономики невозможны без эффективного правового механизма охраны личных данных. Для Узбекистана, активно интегрирующегося в мировую цифровую торговлю, вопрос правового регулирования Big Data в электронной коммерции с акцентом на защиту персональных данных является чрезвычайно актуальным и востребованным.

Цель

Целью настоящего тезиса является анализ действующего законодательства Республики Узбекистан в сфере регулирования больших данных в электронной коммерции сквозь призму защиты персональных данных, а также выработка выводов и предложений по совершенствованию правовой базы. В работе рассмотрены основополагающие нормативные акты – Закон «Об электронной коммерции» (ЗРУ-792 от 29.09.2022 г.) [2] и Закон «О персональных данных» (ЗРУ-547 от 02.07.2019 г.) [1] – с целью выявления их достоинств и пробелов применительно к Big Data. На основе анализа планируется сформулировать





MODERN PROBLEMS IN EDUCATION AND THEIR SCIENTIFIC SOLUTIONS

рекомендации по улучшению законодательства Узбекистана с учётом международных тенденций в сфере защиты данных и развития цифровой экономики.

Краткий анализ проблем

Понятие Big Data и сфера электронной коммерции. Под «большими данными» обычно понимаются значительные объёмы разнородной информации, собираемой из множества источников и обрабатываемой специализированными методами для выявления скрытых закономерностей и поддержки принятия решений. В контексте электронной коммерции Big Data используются для персонализации сервисов, таргетированного маркетинга, прогнозирования спроса и иных коммерческих целей. Однако такие данные нередко включают персональные данные пользователей, что требует соблюдения правовых норм о конфиденциальности и защите частной жизни.

Действующее законодательство Узбекистана. В Республике Узбекистан вопросы электронной коммерции и обращения данных регулируются рядом актов. Базовым является Закон «Об электронной коммерции» № ЗРУ-792 от 29 сентября 2022 года [2], который определяет правовые основы отношений в области e-commerce. Данный Закон закрепляет права и обязанности основных субъектов (продавцов, покупателей, операторов электронной коммерции и электронных торговых площадок) и содержит нормы, направленные на защиту информации. В частности, операторы электронной коммерции обязаны обеспечивать защиту электронных сообщений и персональных данных от несанкционированного доступа или использования, а также не передавать их третьим лицам без законных оснований [2]. Эти требования обязывают участников рынка внедрять меры информационной безопасности и соблюдать конфиденциальность сведений о клиентах. Кроме того, условия договоров в электронной коммерции могут специально оговаривать порядок использования персональных данных и иной информации ограниченного распространения, что позволяет сторонам заранее определить правила обработки таких данных [2].

Параллельно специальным законом выступает Закон Республики Узбекистан «О персональных данных» № ЗРУ-547 от 2 июля 2019 года [1], прямо регулирующий отношения по сбору, обработке и защите персональных данных. Он устанавливает ключевые принципы работы с персональными данными: законность и справедливость обработки, соответствие объёма и характера данных заявленным целям, достоверность и актуальность данных, ограничение сроков хранения и др. Так, цели обработки персональных данных должны соответствовать тем целям, которые были заявлены при их сборе; изменение первоначальной цели требует получения отдельного согласия субъекта данных [1]. Закон требует минимизации данных – объём и характер обрабатываемых персональных данных должны соответствовать целям их обработки [1]. Прямо





MODERN PROBLEMS IN EDUCATION AND THEIR SCIENTIFIC SOLUTIONS

предусмотрено, что по истечении срока действия согласия субъекта дальнейшая обработка данных недопустима [1]. Более того, персональные данные могут обрабатываться либо в идентифицируемой форме, либо в обезличенном (анонимизированном) виде [1]. Таким образом, закон стимулирует использование методов обезличивания (анонимизации) при работе с большими массивами данных, чтобы снизить риски для частной жизни граждан.

Закон «О персональных данных» подробно регламентирует права субъектов персональных данных. Граждане имеют право получать информацию о целях и способах обработки их данных, требовать уточнения или уничтожения данных в случае необходимости, а также **не подпадать под решения, основанные исключительно на автоматизированной обработке** (например, алгоритмические решения без участия человека), если такие решения затрагивают их права и законные интересы [1]. Последнее положение особенно важно в эпоху Big Data, поскольку предусматривает защиту от неблагоприятных последствий автоматизированного профилирования и иных форм **алгоритмического принятия решений** в электронной коммерции. Данная норма соответствует международной практике (например, ст.22 GDPR в Европейском Союзе) и свидетельствует о стремлении узбекского законодателя учитывать цифровые риски.

Отдельное внимание уделяется трансграничному обмену данными. Узбекистан, как и многие страны, устанавливает ограничения на вывоз персональных данных за рубеж. Трансграничная передача персональных данных допускается только в государства, обеспечивающие адекватную правовую защиту прав субъектов данных [1]. Если же иностранное государство не предоставляет достаточных гарантий, передача возможна лишь при наличии явного согласия субъекта либо в отдельных случаях, предусмотренных законом или международными договорами [1]. Более того, законодательством предусмотрено право правительства вводить запрет или ограничения на передачу данных за рубеж в целях защиты национальных интересов, общественной нравственности, здоровья населения, обороны и безопасности страны [1]. Эти положения аналогичны механизмам, используемым в мировой практике (например, концепции «адекватности» из GDPR) и направлены на предотвращение неконтролируемого вывоза больших массивов персональных сведений из страны.

За последние годы национальное законодательство было усилено с учётом международных тенденций. Так, в январе 2021 года в Закон «О персональных данных» введена статья 27¹, устанавливающая **требование локализации персональных данных граждан Узбекистана**. Согласно этой норме, владельцы и операторы, обрабатывающие персональные данные граждан РУз через информационные сети (в том числе интернет), обязаны обеспечивать хранение и систематизацию таких данных на технических средствах, физически





MODERN PROBLEMS IN EDUCATION AND THEIR SCIENTIFIC SOLUTIONS

расположенных на территории Узбекистана [4]. Иными словами, глобальные сервисы (социальные сети, крупные интернет-компании) должны размещать серверы с данными узбекских пользователей внутри страны. Данная мера, аналогичная требованиям, действующим в России и ряде других государств, призвана защитить данные граждан от иностранной юрисдикции и облегчить государственный контроль. В то же время, она вызывает дискуссии: представители индустрии указывают, что жесткая локализация может создавать барьеры для международных IT-бизнесов и потенциально сдерживать развитие цифровых услуг [4]. Следовательно, законодателю предстоит искать баланс между суверенитетом данных и открытостью цифровой экономики.

Практические вызовы и пробелы. Несмотря на наличие упомянутых законов, на практике остаются проблемы в сфере Big Data и персональных данных. Во-первых, **понятие больших данных прямо не определено** в узбекском законодательстве, что затрудняет правоприменение в специфических ситуациях массового анализа данных. Нет отдельных нормативных актов или подробных подзаконных документов, регламентирующих именно большие данные (в отличие, например, от инициатив в некоторых других странах по принятию специальных «законов о больших данных»). Во-вторых, **соблюдение законодательства частными компаниями** вызывает вопросы. Многие участники рынка ограничиваются формальным размещением на сайтах пользовательских соглашений и политик конфиденциальности, часто объемных и трудных для понимания рядовым пользователем [3]. Пользователи практически не читают длинные «Правила использования» и «Соглашения о конфиденциальности», что ставит под сомнение осознанность их согласия на обработку данных. Нет уверенности, что собранные персональные данные действительно используются строго в заявленных целях и надлежащим образом защищены. В Узбекистане пока не проводилось широкомасштабных исследований соответствия практик ведущих e-commerce компаний требованиям законов о персональных данных [3]. Вместе с тем, периодически фиксируются инциденты утечки персональных данных или незаконной продажи баз данных граждан, что указывает на недостаточный уровень безопасности и контроля [3].

Кроме того, **наказуемость и контроль** в области Big Data остаются областями для развития. Закон «Об электронной коммерции» устанавливает, что нарушение законодательства в этой сфере влечёт ответственность, однако конкретные санкции предусмотрены административным и уголовным законодательством. Необходимо эффективное применение этих санкций. Только в 2022 году введена административная ответственность за непредоставление данных для реестра персональных данных и нарушение требований локализации, что свидетельствует о стремлении государства усилить контроль. Однако регуляторные органы, ответственные за надзор (например, уполномоченный государственный орган по





MODERN PROBLEMS IN EDUCATION AND THEIR SCIENTIFIC SOLUTIONS

персональным данным), ещё формируют практику мониторинга и притворения норм в жизнь.

Международный опыт и стандарты. В глобальном масштабе прослеживаются две взаимосвязанные тенденции: усиление требований к защите персональных данных и стимулирование развития цифровой экономики на основе данных. Европейский союз в 2018 году ввёл Общий регламент по защите данных (GDPR), который стал **золотым стандартом**: он вводит строгие правила обработки персональных данных, требует прозрачности, согласия пользователя, отчётности компаний и устанавливает серьёзные штрафы за утечки и нарушения. Многие страны мира, включая соседние с Узбекистаном государства, модернизируют свои национальные законы по образцу GDPR. Одновременно обсуждаются новые аспекты: например, в ЕС разрабатывается **Актив о цифровых услугах и Актив об искусственном интеллекте**, направленные в том числе на регуляцию алгоритмов и больших данных, использующихся онлайн-платформами. В Российской Федерации в последние годы также проявляется интерес к регулированию больших данных на законодательном уровне – предпринимались попытки закрепить в законе определения «больших пользовательских данных» и ввести реестры операторов Big Data [5], что свидетельствует о появлении специализированного подхода к этой сфере. В ведущих державах Азии (Китай, Южная Корея, Сингапур) вводятся строгие требования к крупным интернет-компаниям по защите информации о пользователях, одновременно поддерживается инновационное использование данных для экономического роста. Таким образом, международный опыт подсказывает, что для успешного развития электронной коммерции необходим **комплексный подход**: сильные механизмы защиты персональных данных должны сочетаться с созданием условий для законного и безопасного использования больших данных в интересах экономики.

Выводы и предложения

Выводы. Анализ показывает, что Узбекистан заложил правовую основу для защиты персональных данных в условиях цифровой экономики: приняты специальные законы, частично учитывающие международные стандарты и современные риски. Закон «О персональных данных» обеспечивает базовые гарантии приватности граждан, устанавливает принципы обработки данных и обязанность получения согласия, предусматривает права субъектов (включая защиту от полностью автоматизированных решений) и механизмы трансграничного контроля. Закон «Об электронной коммерции» дополняет эту базу, обязывая участников рынка соблюдать конфиденциальность и безопасность данных в онлайн-сделках. Однако действующее регулирование **не в полной мере охватывает особенности Big Data** – сбор массивов данных из различных источников, профилирование потребителей, автоматическое принятие решений на





MODERN PROBLEMS IN EDUCATION AND THEIR SCIENTIFIC SOLUTIONS

основе аналитики. Имеются пробелы в конкретных нормах и, главное, в **реализации**: требуется более эффективный контроль за соблюдением законодательства в повседневной практике электронной коммерции. В целях гармоничного развития цифровой экономики необходимо актуализировать и усиливать правовые механизмы с учётом лучших мировых образцов.

Предложения по совершенствованию законодательства Республики Узбекистан:

- **Уточнение законодательства и введение понятий.** Рекомендуется определить на законодательном уровне понятие «**большие данные**» и связанные с ними термины (например, «**профилирование**», «**оператор больших данных**»). Это может быть реализовано через внесение изменений в Закон об электронной коммерции или в Закон об информации. Чёткие дефиниции и границы применения Big Data помогут устранить неопределённость и однозначно распространять требования о защите данных на соответствующие процессы.

- **Развитие институционального надзора.** Ввести или усилить независимый институт **надзора за персональными данными** (аналогично европейским регуляторам по защите данных). Уполномоченный орган должен обладать достаточными ресурсами и полномочиями для проведения аудитов в компаниях электронной коммерции, проверки соблюдения требований (регистрации баз данных, локализации, безопасности) и применения санкций за нарушения. Повышение эффективности надзорной практики стимулирует бизнес надлежащим образом относиться к большим данным.

- **Совершенствование механизмов согласия и прозрачности.** Предусмотреть на нормативном уровне требования к форме и содержанию пользовательских соглашений и политик конфиденциальности в интернете. Они должны быть **краткими, понятными** для среднестатистического пользователя и легко доступными на сайте или в приложении. Желательно обязать e-commerce компании предоставлять **сводную информацию** о том, какие данные собираются и для каких целей, в простой форме (например, раздел FAQ или инфографика) [3]. Такое требование повысит осознанность согласия пользователей на обработку их персональных данных и будет соответствовать принципу прозрачности (прозрачной обработки), закреплённому в международных нормах.

- **Защита прав субъектов при Big Data-обработке.** Расширить гарантии для граждан в условиях автоматизированной обработки больших данных. В частности, имплементировать **право на удаление данных** («**право быть забытым**») – чтобы пользователь мог потребовать удалить свои персональные данные, если они более не нужны для заявленных целей. Ввести **право на переносимость данных**, позволяющее получать свои данные в машиночитаемом формате и передавать другим сервисам (это особенно актуально при смене платформ в электронной коммерции). Также следует обеспечить реализацию на





MODERN PROBLEMS IN EDUCATION AND THEIR SCIENTIFIC SOLUTIONS

практике уже предусмотренного права не подвергаться решениям, основанным только на автоматизированной обработке [1], разработав процедуру пересмотра таких решений с участием человека по запросу пользователя.

- **Баланс между инновациями и безопасностью.** Законодательно стимулировать ответственное использование больших данных. Например, разработать руководящие разъяснения или стандарты для анонимизации данных, чтобы компании могли извлекать из больших данных пользу (аналитику, тренды) без нарушения частной жизни граждан. Возможно создание «песочниц» (**regulatory sandboxes**) для пилотных проектов в сфере Big Data, где под надзором регулятора тестируются новые решения (например, системы рекомендательных алгоритмов или динамического ценообразования) с оценкой их влияния на права потребителей. Это позволит обновлять регулирование гибко и вовремя, не дожидаясь появления проблем.

- **Учёт международных тенденций.** Узбекистану целесообразно продолжить гармонизацию своего законодательства с глобальными стандартами. В частности, рассмотрение возможности присоединения к **Конвенции 108+ Совета Европы** о защите физических лиц при автоматизированной обработке персональных данных либо налаживание сотрудничества с международными организациями по выработке лучших практик. Следует отслеживать развитие законодательства в ЕС, США, странах Азии, чтобы заимствовать эффективные решения (например, в сфере **кибербезопасности данных**, требований к информированию о взломах и утечках, кодексов этики для больших данных и искусственного интеллекта). Это поможет обеспечить совместимость требований при трансграничной электронной торговле и привлечь иностранные инвестиции в цифровой сектор, поскольку зарубежные партнёры увидят, что в Узбекистане действуют понятные и надёжные правила обращения с данными.

Заключение. Регулирование больших данных в электронной коммерции – сложная, но насущная задача для законодательства Узбекистана. От успешного решения этой задачи зависит, сумеет ли страна максимально использовать потенциал цифровой экономики, не поступаясь правами и свободами граждан. Проведённый анализ показывает, что законодательная база находится в стадии активного развития: приняты важные акты (Закон «О персональных данных» 2019 г. [1], Закон «Об электронной коммерции» 2022 г.) [2], происходит учёт международных требований (введены нормы о локализации данных, автоматизированных решениях и др.). Тем не менее, для обеспечения полноценной **защиты персональных данных** в условиях Big Data требуется дальнейшее совершенствование норм и их практической реализации. Реализация предложенных мер позволит укрепить доверие пользователей к электронной коммерции, обеспечить законность и прозрачность обработки больших данных, а





также создать благоприятные условия для инновационного роста цифровой экономики Узбекистана в русле мировых тенденций.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ:

1. Закон Республики Узбекистан «О персональных данных» (ЗРУ-547 от 02.07.2019 г.) <https://lex.uz/docs/4396428>
2. Закон Республики Узбекистан «Об электронной коммерции» (ЗРУ-792 от 29.09.2022 г.) <https://lex.uz/ru/docs/6213428>
3. Legal Clinic Uzbekistan – Соблюдение законодательства о персональных данных частными компаниями <https://legalclinic.uz/tpost/mm2pgom8s1-soblyudenie-zakonodatelstva-o-personalni>
4. Uzbekistan Law Blog – Data protection in Uzbekistan: challenges and opportunities <https://uzbekistanlawblog.com/data-protection-in-uzbekistan-challenges-and-opportunities/>
5. Gorodissky & Partners – New legal initiatives to regulate Big Data Articles and Publications <https://www.gorodissky.com/publications/articles/new-legal-initiatives-to-regulate-big-data/>

