ПРАВОВОЙ РЕЖИМ ПЕРСОНАЛЬНЫХ ДАННЫХ В СОЦИАЛЬНЫХ СЕТЯХ: ТЕОРЕТИЧЕСКИЕ И ПРАВОВЫЕ АСПЕКТЫ

Караева Камолахон Рахматилло кизи

Магистрант факультета «Отрасли права, прикладной анализ правовых и политических исследований»

Ташкентский государственный юридический университет

Аннотация. *В настоящей статье исследуются теоретические и правовые основы регулирования персональных данных пользователей социальных сетей. Анализируется понятие персональных данных в контексте цифровой среды, рассматриваются основные угрозы приватности и механизмы правовой защиты. Особое внимание уделяется международному опыту в сфере защиты персональных данных, в частности Общему регламенту о защите данных Европейского союза (GDPR), а также законодательству Республики Узбекистан. Обосновывается необходимость совершенствования национального законодательства в условиях стремительного развития технологий и расширения деятельности платформ социальных сетей. Делаются выводы о необходимости комплексного подхода к обеспечению информационной безопасности и защите права граждан на неприкосновенность частной жизни в цифровом пространстве.*

Ключевые слова: *персональные данные, социальные сети, правовой режим, защита данных, приватность, цифровые права, GDPR, информационная безопасность, законодательство Узбекистана, оператор данных.*

Abstract. This article examines the theoretical and legal foundations for regulating the personal data of social media users. It analyzes the concept of personal data in the context of the digital environment, discusses the main threats to privacy, and examines legal protection mechanisms. Particular attention is paid to international experience in the field of personal data protection, in particular the European Union's General Data Protection Regulation (GDPR), as well as the legislation of the Republic of Uzbekistan. The need to improve national legislation is substantiated in the context of rapid technological development and the expansion of social media platforms. Conclusions are drawn regarding the need for a comprehensive approach to ensuring information security and protecting citizens' right to privacy in the digital space.

Keywords: personal data, social media, legal regime, data protection, privacy, digital rights, GDPR, information security, legislation of Uzbekistan, data operator.

ВВЕДЕНИЕ

Стремительное развитие информационно-коммуникационных технологий и широкое распространение социальных сетей коренным образом трансформировали характер межличностных коммуникаций, бизнес-процессов и общественных отношений. Социальные сети - Facebook, Instagram, Twitter (X), TikTok, ВКонтакте, Одноклассники и другие платформы - стали неотъемлемой частью повседневной жизни миллиардов людей по всему миру. В процессе пользования данными платформами граждане добровольно или неосознанно предоставляют огромные массивы персональных данных: имена, контактные сведения, геолокацию, сведения о личных предпочтениях, политических взглядах и поведенческих паттернах.

Подобная открытость порождает серьёзные правовые и этические вопросы, связанные с обеспечением конфиденциальности, предотвращением

несанкционированного использования личных сведений и защитой цифровых прав граждан. Проблема правового режима персональных данных приобрела особую актуальность в связи с громкими скандалами, связанными с утечками данных (Cambridge Analytica, 2018), кибератаками на крупные платформы и случаями неправомерного использования личной информации в политических и коммерческих целях.

В Республике Узбекистан данная проблематика также приобретает всё большее значение на фоне реализации государственной программы «Цифровой Узбекистан - 2030» и последовательного расширения охвата интернет-пользователей. По данным Агентства по развитию рынка капитала (AKFA Research), по состоянию на 2024 год доля интернет-пользователей в стране превысила 70%, а аудитория социальных сетей неуклонно растёт. В этих условиях надлежащее правовое регулирование обращения с персональными данными является одним из ключевых направлений обеспечения цифрового суверенитета и защиты конституционных прав граждан.

Цель настоящей статьи - комплексное исследование теоретических и правовых аспектов правового режима персональных данных в социальных сетях, выявление пробелов и перспектив совершенствования законодательства Республики Узбекистан в данной сфере.

ПОНЯТИЕ И ПРАВОВАЯ ПРИРОДА ПЕРСОНАЛЬНЫХ ДАННЫХ

Персональные данные как правовая категория представляют собой любую информацию, относящуюся к прямо или косвенно идентифицированному или идентифицируемому физическому лицу (субъекту данных). Данное определение закреплено в статье 4 Регламента (ЕС) 2016/679

(GDPR) и воспринято большинством национальных правовых систем, в том числе законодательством Республики Узбекистан.

Закон Республики Узбекистан «О персональных данных» (принят 2 июля 2019 года, № ЗРУ-547) определяет персональные данные как «сведения, относящиеся к определённому или определяемому на основании таких сведений физическому лицу». В контексте социальных сетей данное понятие охватывает широкий спектр информации: анкетные данные (имя, фамилия, дата рождения), контактные реквизиты (номер телефона, адрес электронной почты), биометрические данные (фотографии лица), сведения о местоположении, данные о поведении пользователя в сети и его коммуникациях.

Особую правовую значимость представляют так называемые «специальные категории» персональных данных, обработка которых сопряжена с повышенным риском дискриминации или нарушения прав: расовая и этническая принадлежность, политические взгляды, религиозные убеждения, состояние здоровья, сексуальная ориентация. Социальные сети, в силу специфики своей архитектуры, аккумулируют именно такие чувствительные сведения, что предопределяет необходимость их усиленной правовой охраны.

Профессор В.А. Копылов справедливо отмечал, что информация как объект права обладает рядом особых свойств: нематериальностью, возможностью неограниченного тиражирования, независимостью от носителя. Применительно к персональным данным эти свойства обусловливают специфику их правового режима: однажды утраченный контроль над личными сведениями практически невозможно восстановить, что делает превентивную защиту данных приоритетом правового регулирования.

ПРАВОВЫЕ УГРОЗЫ И РИСКИ В СОЦИАЛЬНЫХ СЕТЯХ

Социальные сети как среда обращения персональных данных сопряжены с многообразием правовых рисков. В научной литературе принято выделять несколько ключевых угроз:

Во-первых, несанкционированный сбор и коммерческое использование данных. Платформы социальных сетей, как правило, монетизируют свою деятельность через таргетированную рекламу, основанную на детальном профилировании пользователей. При этом пользователи зачастую не осознают истинного масштаба собираемых о них сведений и целей их использования. Пользовательские соглашения (Terms of Service), как правило, содержат объёмный текст на иностранном языке, фактически лишающий гражданина возможности осознанного согласия на обработку данных.

Во-вторых, утечки данных вследствие кибератак и уязвимостей платформ. По данным компании IBM Security, среднемировая стоимость одного инцидента утечки данных в 2023 году составила 4,45 млн долларов США. Для субъектов данных подобные инциденты означают риски мошенничества, шантажа, дискриминации и нарушения репутации.

В-третьих, трансграничная передача данных. Большинство популярных социальных платформ зарегистрированы в юрисдикции США или иных государств и обрабатывают данные на серверах, расположенных за пределами страны проживания пользователя. Это порождает коллизию применимого права и существенно затрудняет реализацию субъектом данных своих прав.

В-четвёртых, профайлинг и алгоритмическая дискриминация. Использование технологий больших данных (Big Data) и искусственного интеллекта для автоматизированного принятия решений на основе анализа персональных данных создаёт риски дискриминации по защищаемым признакам без участия человека в процессе принятия решений.

МЕЖДУНАРОДНО-ПРАВОВЫЕ СТАНДАРТЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

На международном уровне наиболее значимым документом в сфере защиты персональных данных является Общий регламент о защите данных Европейского союза (GDPR), вступивший в силу 25 мая 2018 года. GDPR устанавливает экстерриториальный принцип действия: его нормы применяются к любому оператору, обрабатывающему данные граждан ЕС, вне зависимости от места его нахождения. Регламент закрепляет ряд фундаментальных принципов обработки персональных данных: законность, справедливость, прозрачность; ограничение целей обработки; минимизация данных; точность; ограничение хранения; целостность и конфиденциальность.

Существенным нововведением GDPR является право на забвение (right to erasure), позволяющее субъекту данных требовать удаления своих сведений из систем оператора, а также право на переносимость данных. Санкции за нарушение Регламента достигают 4% годового глобального оборота компании или 20 млн евро - в зависимости от того, какая сумма больше. Данные меры обеспечили реальный сдвиг в практике социальных платформ: Meta (Facebook) только в 2023 году была оштрафована Ирландской комиссией по защите данных на 1,2 млрд евро.

Помимо GDPR, ориентиром для национальных законодателей служат Руководящие принципы ОЭСР по защите конфиденциальности (1980, обновлены в 2013), Конвенция Совета Европы № 108 о защите физических лиц в отношении автоматизированной обработки данных (Конвенция 108+, обновлена в 2018), а также рекомендации ООН в области цифровой конфиденциальности.

ПРАВОВОЙ РЕЖИМ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЗАКОНОДАТЕЛЬСТВЕ РЕСПУБЛИКИ УЗБЕКИСТАН

Правовую основу регулирования персональных данных в Республике Узбекистан составляют: Конституция Республики Узбекистан (статьи 27, 30), гарантирующая неприкосновенность частной жизни и тайну переписки; Закон «О персональных данных» (2019); Закон «Об информатизации» (2003, в редакции 2022 года); Закон «О принципах и гарантиях свободы информации» (2002); Уголовный кодекс (статья 141-1 - нарушение неприкосновенности частной жизни).

Закон «О персональных данных» 2019 года существенно модернизировал национальную правовую базу: введены понятия «оператор баз персональных данных», «база персональных данных», установлены требования к трансграничной передаче данных и локализации. Примечательно, что статья 23 Закона предусматривает требование о хранении персональных данных граждан Узбекистана на серверах, расположенных на территории республики, - аналогичный механизм действует в Российской Федерации (статья 18 Федерального закона № 152-ФЗ).

Вместе с тем действующее законодательство имеет ряд существенных пробелов применительно к деятельности социальных сетей. В частности, отсутствуют специальные нормы, регулирующие: алгоритмическую обработку данных и профайлинг; право на забвение в цифровой среде; ответственность социальных платформ за утечку данных пользователей; минимальные стандарты конфиденциальности пользовательских соглашений. Механизм надзора за операторами социальных сетей, зарегистрированными за рубежом, также нуждается в дальнейшем совершенствовании.

Актуальным направлением является имплементация международных стандартов, прежде всего принципов GDPR, с учётом специфики национальной правовой системы и уровня цифровизации. Ряд государств постсоветского пространства - Казахстан, Армения, Молдова - уже

приступили к реформированию законодательства о персональных данных в русле европейских стандартов, что создаёт благоприятный сравнительно-правовой контекст для соответствующей работы в Узбекистане.

ПРОБЛЕМЫ ПРАВОПРИМЕНЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Эффективное правоприменение в сфере защиты персональных данных в социальных сетях сталкивается с рядом системных проблем. Первая из них - юрисдикционная: социальные платформы, как правило, отрицают наличие постоянного представительства на территории Узбекистана, что затрудняет привлечение их к юридической ответственности по национальному праву. Вторая проблема - технологическая сложность доказывания нарушений: установление факта несанкционированной обработки данных требует специальных технических компетенций, которыми зачастую не располагают ни контролирующие органы, ни суды.

Третья проблема - низкий уровень правовой грамотности пользователей. Социологические исследования свидетельствуют о том, что подавляющее большинство пользователей социальных сетей не читают пользовательские соглашения и не осознают, на что именно они дают согласие при регистрации на платформе. Это делает концепцию «информированного согласия» во многом формальной.

Среди перспективных направлений совершенствования правового регулирования следует выделить: принятие специального закона или поправок, устанавливающих требования к деятельности социальных сетей на территории Узбекистана; введение института уполномоченного по защите персональных данных (Data Protection Officer) в организациях, обрабатывающих значительные объёмы личных сведений; разработку механизма «одного окна» для реализации гражданами своих прав в отношении

персональных данных в цифровой среде; внедрение требований к локализации данных и стандартов Privacy by Design при разработке цифровых сервисов.

Немаловажную роль должно сыграть международное сотрудничество в данной сфере: участие Узбекистана в переговорах о присоединении к Конвенции 108+, заключение двусторонних соглашений о защите данных с ключевыми торговыми партнёрами, а также активное взаимодействие с международными организациями (ООН, ОБСЕ, СНГ) по вопросам цифровых прав.

ЗАКЛЮЧЕНИЕ

Проведённое исследование позволяет сформулировать следующие выводы. Правовой режим персональных данных в социальных сетях представляет собой комплекс правовых норм, принципов и механизмов, регулирующих сбор, хранение, обработку, передачу и уничтожение личной информации пользователей цифровых платформ. В условиях стремительной цифровизации данная сфера правового регулирования приобрела критическое значение для обеспечения конституционных прав граждан на неприкосновенность частной жизни.

Анализ международных стандартов (GDPR, Конвенция 108+, руководящие принципы ОЭСР) и законодательства Республики Узбекистан свидетельствует о том, что отечественная правовая база, при всей её значимости, нуждается в существенном развитии применительно к специфике деятельности социальных сетей. Приоритетными направлениями являются: установление специальных требований к платформам, управомочивающих граждан на реализацию цифровых прав; совершенствование механизмов надзора и ответственности; повышение правовой грамотности пользователей.

Защита персональных данных в социальных сетях - это не только правовая, но и социально-политическая задача, решение которой требует

координации усилий государства, бизнеса и гражданского общества. Только комплексный подход, сочетающий эффективное законодательство, дееспособные институты надзора, технические стандарты и просветительскую работу, способен обеспечить подлинную защиту цифровых прав граждан в современном информационном обществе.

СПИСОК ЛИТЕРАТУРЫ

1. Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 года, № ЗРУ-547.
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation, GDPR). - Official Journal of the European Union. 2016.
3. Конвенция Совета Европы № 108 о защите физических лиц при автоматизированной обработке персональных данных (в редакции Протокола CETS № 223, 2018).
4. Копылов В.А. Информационное право: учебник. 2-е изд., перераб. и доп. М.: Юристъ, 2002. 512 с.
5. Городов О.А. Информационное право: учебник. М.: Проспект, 2011. 243 с.
6. Алешкова И.А., Яковлев В.Ф. Цифровые права человека: понятие, содержание, гарантии // Государство и право. 2021. № 4. С. 7–18.
7. IBM Security. Cost of a Data Breach Report 2023. URL: https://www.ibm.com/reports/data-breach (дата обращения: 01.03.2025).
8. Агентство по развитию рынка капитала Республики Узбекистан (AKFA Research). Отчёт о цифровизации экономики Узбекистана 2024. Ташкент, 2024.
9. Солове Д. Будущее репутации: сплетни, слухи и конфиденциальность в Интернете / пер. с англ. - М.: Альпина Паблишер, 2016. 264 с.
10. Рассолов И.М. Право и интернет: теоретические проблемы. - 2-е изд., доп. - М.: Норма, 2009. 383 с.