

DIRECTIONS FOR DEVELOPMENT OF LEGAL REGULATION OF CROSS-BORDER TRANSFER OF PERSONAL DATA: REVIEW OF KEY COURT DECISIONS AND THEIR IMPACT ON THE PRACTICE OF CROSS-BORDER TRANSFER OF DATA

ИСАКОВА МАЛИКА МАХСУДОВНА

malikaisakova1907@gmail.com

Ташкентский государственный юридический университет

Направление "Право СМИ"

<https://doi.org/10.5281/zenodo.11276876>

Abstract

This article explores the developments in legal regulation concerning the cross-border transfer of personal data. The author conducts a review of key judicial decisions related to this issue and analyzes their impact on the practice of cross-border data transfers. The paper examines pertinent issues in personal data protection, such as conflicts of interest between countries, security standards, and compliance with regulatory requirements. The research aims to provide a comprehensive overview of judicial decisions influencing the formation of legal norms in the field of cross-border personal data transfers.

Key words: Cross-border data transfers, personal data protection, legal regulation, judicial decisions, data privacy, transnational data flow, regulatory compliance, security standards, international conflicts, legal norms.

НАПРАВЛЕНИЯ РАЗВИТИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ТРАНСГРАНИЧНОЙ ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ: ОБЗОР КЛЮЧЕВЫХ СУДЕБНЫХ РЕШЕНИЙ И ИХ ВЛИЯНИЕ НА ПРАКТИКУ ТРАНСГРАНИЧНОЙ ПЕРЕДАЧИ ДАННЫХ

Аннотация

Данная статья посвящена изучению направлений развития правового регулирования трансграничной передачи персональных данных. Автор проводит обзор ключевых судебных решений, касающихся данной проблематики, и анализирует их воздействие на практику трансграничной передачи данных. В работе рассматриваются актуальные вопросы в области защиты личных данных, такие как конфликт интересов между странами, стандарты безопасности и соблюдение нормативных требований. Исследование призвано предоставить полный обзор судебных решений, которые оказывают влияние на формирование правовых норм в области трансграничной передачи персональных данных.

Ключевые слова: трансграничные передачи данных, защита персональных данных, правовое регулирование, судебные решения, конфиденциальность данных, трансграничный поток данных, соблюдение нормативов, стандарты безопасности, международные конфликты, правовые нормы.

В эпоху информационных технологий, когда цифровые потоки персональных данных пересекают границы национальных юрисдикций, вопросы, связанные с трансграничной передачей данных, становятся предметом внимания и обсуждения на мировой арене.

Нарастающая сложность этой темы требует не только постоянного совершенствования правового регулирования, но и внимательного анализа ключевых судебных решений, которые формируют основные принципы и стандарты в этой области.

В данном контексте, рассмотрим направления развития правового регулирования трансграничной передачи персональных данных с особым акцентом на примеры законодательства Узбекистана. В стремлении адаптировать национальное законодательство к вызовам цифровой эры, Узбекистан принимает меры для обеспечения адекватной защиты личных данных своих граждан в контексте глобального обмена информацией.

Проанализируем, например, последние изменения в законодательстве Узбекистана, направленные на усиление контроля и безопасности при трансграничной передаче персональных данных. Это может включать в себя меры, предусматривающие обязательное соблюдение стандартов шифрования, ужесточение требований к процедурам аутентификации при обработке данных, а также установление ответственности за нарушения, связанные с трансграничной передачей данных.

Такой фундаментальный анализ законодательных инициатив Узбекистана в контексте трансграничной передачи данных предоставит более глубокое понимание того, как страна адаптируется к вызовам цифровой эры, обеспечивая баланс между своими национальными интересами и международными стандартами защиты данных.

Теоретическую базу начнем с работы Cross-Border data transfers: A global perspective on privacy regulation (2019) [1], который представляет собой важное исследование, в рамках которого авторы подробно анализируют сложности и тенденции в области трансграничной передачи данных, фокусируясь на правовых нормах, регулирующих этот процесс в различных странах мира. Stephen Adi Odey внимательно изучает ключевые аспекты законодательства, касающегося передачи данных через границы, выделяя различия и общие черты между национальными нормами. В частности, особое внимание уделяется вопросам конфиденциальности и безопасности данных, так как эти аспекты играют решающую роль в формировании стратегий компаний и организаций, занимающихся международными данными. Исследование подробно рассматривает текущие тренды в разработке и изменениях законодательства, предостерегая читателя от изменений в применимых нормах и политиках конфиденциальности. Особое внимание уделяется влиянию таких правовых норм, как Общий регламент по защите данных (GDPR) в Европейском союзе, на стандарты конфиденциальности и безопасности данных в мировом масштабе.

В исследовании A Mattoo представляет глубокий анализ в International data flows and privacy: The conflict and integration of global and local norms (2018) именно динамики и конфликтов между глобальными и локальными нормами в контексте передачи данных через границы. Автор занимается разбором вызовов, возникающих из-за различий в законодательстве разных стран, и предлагает стратегии для разрешения этих конфликтов в контексте защиты данных.[2] Основной фокус исследования направлен на обнаружение и понимание противоречий между мировыми стандартами и национальными законами в области защиты данных. Автор приступает к анализу того, как эти противоречия влияют на международные потоки данных и создают

юридические, технологические и организационные вызовы для корпораций и государств.

Книга Peter Philip Carey Data protection: A practical guide to UK and EU Law (2021) представляет собой важный ресурс, который не только предоставляет обширный обзор теоретических аспектов правового регулирования защиты данных в Великобритании и Евросоюзе, но и фокусируется на практических аспектах, ориентированных на трансграничную передачу персональных данных.[3] Автор подробно анализирует требования законодательства, касающегося защиты данных, предоставляя читателям подробное понимание основных принципов и стандартов, которым должны соответствовать организации, осуществляющие передачу данных между Великобританией и Евросоюзом. Важным компонентом книги является оценка последних изменений в законодательстве и судебных решений, которые могут иметь существенное воздействие на практику трансграничной передачи персональных данных. Дополнительно, книга предоставляет реальные примеры и кейсы, демонстрируя, как конкретные судебные решения или изменения в законодательстве могут повлиять на бизнес-процессы и стратегии компаний. Автор рассматривает сценарии конфликтов и их разрешения, что делает книгу не только актуальным источником информации, но и ценным практическим руководством для организаций, занимающихся трансграничной передачей данных в контексте Великобритании и Евросоюза.

Узбекистан внедрил уголовное преследование киберпреступности в свой Уголовный кодекс. Несмотря на это, международные соглашения пока не решают вопросы, связанные с международным расследованием и уголовным преследованием киберпреступлений. В самом Уголовном кодексе страны уделено внимание киберпреступности, имеется специальная глава, регулирующая эти аспекты.

Узбекистан выражает поддержку необходимости борьбы против терроризма в интернете, при этом уделяя внимание соблюдению прав человека и своим международным обязательствам.

Основой для обеспечения безопасности при использовании информационно-коммуникационных технологий (ИКТ) в Узбекистане служат Законы РУ "О принципах и гарантиях свободы информации", "Об электронной цифровой подписи", "Об информатизации" и "О защите персональных данных".[4]

В целях единой государственной политики в сфере информационной безопасности принято Постановление Президента Республики Узбекистан от 21 ноября 2018 года № ПП-4024. Это постановление устанавливает задачи, такие как сбор и анализ данных об угрозах информационной безопасности, взаимодействие с операторами и провайдерами сетей телекоммуникаций, проведение аттестации и экспертизы аппаратных средств и программного обеспечения, а также содействие в разработке политики информационной безопасности. Среди ключевых задач также оказание содействия в разработке и реализации политики информационной безопасности государственных информационных систем и ресурсов, а также выработка предложений по совершенствованию нормативно-правовой базы в этой области.[5]

В заключении исследования можно сделать ряд общих выводов. Во-первых, актуальность проблемы трансграничной передачи персональных данных в

современном мире подчеркивается не только национальными законодательствами, но и международными нормами. Принятие специальных глав в уголовных кодексах, криминализирующих киберпреступность, свидетельствует о стремлении государств обеспечить эффективную защиту данных в цифровой эре.

Во-вторых, несмотря на наличие национальных законов, вопросы международного расследования и уголовного преследования киберпреступности остаются нерешенными. Это создает проблемы в судебной практике и требует дополнительных усилий в направлении международного сотрудничества.

Третий вывод связан с важностью соблюдения прав человека в контексте борьбы с киберпреступностью. Узбекистан, подчеркивая важность борьбы против терроризма в Интернете, выражает готовность бороться с этим явлением, соблюдая основные нормы прав человека.

В целом, страны, подобно Узбекистану, с учетом современных вызовов, должны продолжать укреплять свою правовую основу в области трансграничной передачи данных, учитывая международные стандарты и стремясь к усовершенствованию судебных практик для более эффективной борьбы с киберпреступностью при соблюдении прав и свобод человека.

References:

1. Stephen Adi Odey. Cross-Border data transfers: A global perspective on privacy regulation - 2019.
2. A Mattoo. International data flows and privacy: The conflict and integration of global and local norms - 2018.
3. Peter Philip Carey. Data protection: A practical guide to UK and EU Law - 2021.
4. Законы РУ:
5. - "О принципах и гарантиях свободы информации".
6. - "Об электронной цифровой подписи".
7. - "Об информатизации".
8. - "О защите персональных данных".
9. Постановление Президента Республики Узбекистан от 21 ноября 2018 года № ПП-4024: "О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты".