“ADOLAT”
MILLIY HUQUQIY AXBOROT MARKAZI
Guvohnoma № 636478
Litsenziya C-5669732

“HUQUQ va BURCH+” —
«ПРАВО и ДОЛГ+» —
"RIGHT and DUTY+"
Journal home page:
https://adolatmarkazi.uz/magazine/electron?id=351

2026-yil
2-son
fevral
ISSN 3093-8546

# Совершенствование правоприменительной практики в области гражданско-правовой защиты персональных данных

*Мавжуда Атажанова,*
*Докторант Академии правосудия*
*Республики Узбекистан*
*e-mail: brakhimjanova@gmail.com*

***Аннотация.*** Mazkur maqolada O‘zbekiston Respublikasida shaxsiy ma’lumotlarni fuqarolik-huquqiy himoya qilish sohasidagi huquqni qo‘llash amaliyoti muammolari va uni takomillashtirish yo‘nalishlari ko‘rib chiqiladi. «Shaxsgadoirma’lumotlar to‘g‘risida»gi Qonun (№ O‘RQ-547), Fuqarolik kodeksi hamda mualliflik huquqi to‘g‘risidagi qonunchilik normalari tahlili asosida shaxsiy ma’lumotlarning fuqarolik qonunchiligi vositalari bilan muhofaza qilinadigan nomoddiy ne’mat sifatidagi fuqarolik-huquqiy tabiati ochib berilgan.Alohida e’tibor qonunning $27^1$-moddasida nazarda tutilgan ma’lumotlarni lokalizatsiya qilishga oid qoidalarni amalga oshirish muammolariga, shuningdek shaxsiy ma’lumotlar subyektlari huquqlari buzilishiga oid ishlar bo‘yicha yagona sud amaliyotining mavjud emasligiga qaratilgan. O‘zbekiston, Yevropa ittifoqi, AQSh va Xitoy qonunchiligining qiyosiy-huquqiy tahlili o‘tkazilib, ma’lumotlarni himoya qilish bo‘yicha xalqaro standartlar va tendensiyalar, jumladan GDPR modeli asosidagi yondashuvlar aniqlangan.Muallif tomonidan huquqni qo‘llash amaliyotini takomillashtirish bo‘yicha quyidagi chora-tadbirlar taklif etilgan: fuqarolik-huquqiy javobgarlik choralarini kodifikatsiya qilish, ma’lumotlarga ishlov berishning subyektlar huquqlariga ta’sirini baholash institutini joriy etish, sud amaliyotini rivojlantirish va xalqaro hamkorlikni kuchaytirish. Xulosa sifatida, shaxsiy ma’lumotlarni himoya qilish huquqini raqamli innovatsiyalar va shaxsiy hayot daxlsizligi o‘rtasidagi muvozanatni ta’minlovchi mustaqil fuqarolik huquqi sifatida e’tirof etish zarurligi asoslab berilgan.

***Калит сўзлар.*** shaxsiy ma’lumotlar, fuqarolik-huquqiy himoya, ma’lumotlarni lokalizatsiya qilish, GDPR, raqamlashtirish, maxfiylik, operator javobgarligi

***Аннотация.*** В статье рассматриваются проблемы и направления совершенствования правоприменительной практики в области гражданско-правовой защиты персональных данных в Республике Узбекистан. На основе анализа норм Закона «О персональных данных» (№ ЗРУ-547), Гражданского кодекса и законодательства об авторском праве раскрывается гражданско-правовая природа персональных данных как нематериального блага, подлежащего охране средствами гражданского законодательства.Особое внимание уделено проблемам реализации

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

положений статьи 27[1] Закона, касающейся локализации данных, а также отсутствию единообразной судебной практики по делам о нарушении прав субъектов персональных данных. Проведён сравнительно-правовой анализ законодательства Узбекистана, Европейского союза, США и Китая, выявлены тенденции и международные стандарты защиты данных, в том числе по моделиGDPR.Автором предлагаются меры по совершенствованию правоприменения: кодификация мер гражданско-правовой ответственности, введение института оценки воздействия обработки данных на права субъектов, развитие судебной практики и международного сотрудничества. Сделан вывод о необходимости признания права на защиту персональных данных в качестве самостоятельного гражданского права, обеспечивающего баланс между цифровыми инновациями и охраной частной жизни.

***Ключевые слова.*** персональные данные, гражданско-правовая защита, локализация данных, GDPR, цифровизация, конфиденциальность, ответственность оператора

***Annotation.*** The article examines the challenges and prospects for improving the law enforcement practice in the field of civil-law protection of personal data in the Republic of Uzbekistan. Based on the analysis of the Law “On Personal Data” (No. ZRU-547), the Civil Code, and the Law on Copyright and Related Rights, the author reveals the civil-law nature of personal data as an intangible good protected by the mechanisms of private law.Special attention is paid to the implementation issues of Article 27[1] of the Law concerning data localization, as well as to the absence of consistent judicial practice in cases involving violations of personal data rights. A comparative legal analysis of the legislation of Uzbekistan, the European Union, the United States, and China highlights international trends and standards for data protection, including the GDPR model.The author proposes specific measures for improving law enforcement practice: codification of civil liability mechanisms, introduction of the impact assessment procedure, development of case law, and strengthening international cooperation. It is concluded that the right to personal data protection should be recognized as an independent civil right ensuring a balance between digital innovation and privacy protection.

***Keywords.*** personal data, civil-law protection, data localization, GDPR, digitalization, confidentiality, operator’s liability

В эпоху цифровизации общества персональные данные становятся одним из важнейших объектов гражданско-правового регулирования. Развитие цифровых технологий, искусственного интеллекта и платформенной экономики делает сбор, обработку и передачу информации о личности неотъемлемой частью экономических и социальных отношений. В то же время расширение сфер применения персональных данных приводит к росту рисков вмешательства в частную жизнь граждан, что требует совершенствования

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

правовых и институциональных механизмов их защиты.

В Республике Узбекистан ключевым нормативным актом в этой сфере является Закон «О персональных данных» № ЗРУ-547 от 2 июля 2019 г. (с изменениями 2021 и 2023 гг.)[1]. В нём впервые закреплены принципы обработки, гарантии защиты, права субъектов и обязанности операторов. Однако практика его применения выявила ряд проблем – от технической неготовности операторов к обеспечению локализации баз данных (ст. $27^1$) до отсутствия единообразного толкования категорий «конфиденциальность», «согласие субъекта» и «анонимизация».

Проблема гражданско-правовой защиты персональных данных имеет не только внутреннее, но и международное измерение. Взаимодействие с глобальными цифровыми платформами – Google, Meta, NVIDIA, Apple Pay, Google Pay – требует гармонизации национального законодательства с мировыми стандартами, включая Общий регламент ЕС по защите данных (GDPR) и аналогичные акты США и Китая. Как отмечается в исследовании Ларса Хорнуфа, Соньи Мангольд и Яйюнь Ян, современные подходы к защите данных в разных странах демонстрируют не только общие тенденции, но и особенности, определяющие правоприменительную практику[2].

**Гражданско-правовая природа защиты персональных данных.** Персональные данные представляют собой сведения, относящиеся к определённому или определяемому физическому лицу и позволяющие установить его личность. В соответствии со ст. 27 Закона РУз государство гарантирует их защиту, а собственники и (или) операторы обязаны принимать правовые, организационные и технические меры, обеспечивающие целостность, сохранность и конфиденциальность информации. Тем самым законодатель формирует гражданско-правовую основу для реализации конституционного права личности на неприкосновенность частной жизни.

С гражданско-правовой точки зрения персональные данные обладают признаками нематериального блага, защищаемого наравне с честью, достоинством и деловой репутацией (ст. 9 и 10 Гражданского кодекса РУз). Согласно этим нормам, граждане и юридические лица свободны в осуществлении принадлежащих им прав, включая право на защиту. Отказ от такого права не прекращает его существования. Тем самым личные данные входят в систему субъективных гражданских прав, а их защита подчиняется общим способам, предусмотренным ст. 11 ГК РУз – признанием права, восстановлением положения, возмещением убытков и компенсацией морального вреда[3:56].

Таким образом, защита персональных данных выступает частным случаем охраны личных неимущественных прав,

обеспечиваемых средствами гражданского законодательства. Их нарушение порождает обязательство правонарушителя возместить причинённый вред, включая как имущественные, так и моральные потери субъекта данных.

Особое значение в контексте цифровой экономики приобретает вопрос вины и причинной связи при незаконной обработке данных. В отличие от традиционных гражданских дел о нарушении прав личности, здесь вред может быть причинён не физическим действием, а результатом автоматизированной обработки информации, что требует адаптации классических конструкций гражданско-правовой ответственности.

Персональные данные, находящиеся в распоряжении оператора, не могут рассматриваться как его собственность – они принадлежат субъекту, который лишь предоставляет согласие на их использование. Такая модель корреспондирует принципам самоопределения личности и добровольного распоряжения личной информацией, закреплённым как в национальном праве, так и в международных стандартах (GDPR, 2021[4], PIPL КНР)[5].

В Узбекистане ст. 28–31 Закона «О персональных данных» детализируют права и обязанности субъектов, собственников и операторов. Субъект имеет право знать, какие данные о нём хранятся, получать информацию об их обработке, требовать приостановления либо уничтожения незаконно полученных сведений. Оператор обязан обеспечить конфиденциальность и представить доказательство получения согласия субъекта. Эти нормы реализуют общий принцип – законность и пропорциональность обработки персональных данных, соответствующий международной практике.

**Проблемы правоприменения в условиях цифровизации.** Несмотря на наличие современного законодательного регулирования, практика применения норм о защите персональных данных в Узбекистане сталкивается с рядом системных проблем. Наиболее актуальной является неопределённость содержания и объёма обязанностей оператора, особенно в части реализации ст. $27^1$ Закона «О персональных данных», предусматривающей хранение и обработку данных граждан на серверах, расположенных на территории Республики Узбекистан.

Требование о «локализации» баз данных, по сути, направлено на обеспечение суверенитета над цифровыми ресурсами, однако на практике оно создаёт затруднения для международных компаний. Именно это обстоятельство стало препятствием для выхода на рынок таких глобальных платёжных систем, как Apple Pay и Google Pay. Как отмечал Президент Ш.М. Мирзиёев в ходе визита в Вашингтон (ноябрь 2024 г.), пересмотр законодательства о персональных данных должен «создать возможности для внедрения глобальных

платёжных систем и развития сети цифровых академий»; в противном случае национальное регулирование рискует стать барьером для цифровой интеграции страны[6].

Дополнительную сложность представляет отсутствие единообразной судебной практики. На данный момент дела, связанные с незаконной обработкой персональных данных, рассматриваются судами общей юрисдикции и экономическими судами на основе общих положений Гражданского кодекса (ст. 9–11), что приводит к разночтениям при определении состава правонарушения и объёма ответственности.

В отличие от авторского права, где Закон № ЗРУ-42 (ст. 65) чётко определяет способы защиты (восстановление положения, возмещение убытков, компенсация морального вреда и конфискация контрафактных экземпляров), в сфере персональных данных отсутствует аналогичный механизм. Судебная защита зачастую ограничивается предписаниями об устранении нарушений, без последствий в виде компенсации ущерба субъекту данных.

Кроме того, правоприменители недостаточно используют потенциал досудебных средств защиты, предусмотренных ст. 30 Закона – обращения в уполномоченный орган или к оператору с требованием о приостановлении обработки. Это связано как с недостаточной цифровой грамотностью населения, так и с отсутствием единой электронной платформы для подачи жалоб.

**Сравнительно-правовой анализ и международные подходы.** Исследование Л. Хорнуфа, С. Мангольд и Я. Ян показывает, что правовые режимы Германии, США и Китая развиваются в сходном направлении, но существенно различаются по уровню детализации и enforceability (применимости) норм[7].

В Германии защита персональных данных базируется на Общем регламенте ЕС по защите данных (GDPR), который предусматривает принципы законности, справедливости и прозрачности обработки. Особое значение имеет институт Data Protection Impact Assessment – оценки влияния обработки на права субъекта. GDPR устанавливает высокие стандарты ответственности – штрафы до 4 % годового оборота компании, а также прямое право лица на судебную защиту и компенсацию морального вреда[8].

В США действует фрагментированная система: регулирование распределено между федеральным законом о защите потребителей (FTC Act) и многочисленными актами штатов (например, California Consumer Privacy Act 2020). Американский подход опирается на модель «ответственного использования данных» и в меньшей степени на понятие «согласия», что обусловлено приоритетом коммерческой свободы. По данным исследования, в США развита внутренне-корпоративная система контроля, но отсутствует

единый надзорный орган, что приводит к «регуляторным провалам» в онлайн-среде[9].

В Китае действует Закон о защите личной информации (PIPL, 2021), который во многом воспроизводит GDPR, но дополняется жёстким государственным контролем и приоритетом общественной безопасности. Закон обязывает операторов проходить оценку рисков и регистрировать базы данных в госреестре, аналогичном узбекской модели. Особенностью является институт «внешнего надзора» – обязанность операторов представлять отчёт в государственный орган о каждом случае утечки или несанкционированного доступа [10].

Сравнение показывает, что узбекская модель находится в процессе формирования и занимает промежуточное положение: она заимствует принципы GDPR, но сохраняет административно-централизованный подход, типичный для азиатских систем права. При этом в Узбекистане пока отсутствует институт оценки воздействия обработки данных, а ответственность за нарушения носит декларативный характер.

**Взаимосвязь гражданско-правовой и информационно-технологической защиты.** Современная правоприменительная практика показывает, что гражданско-правовые средства защиты данных должны сочетаться с техническими и организационными мерами. Положения ст. 27 Закона «О персональных данных» требуют обеспечения целостности и сохранности информации, однако в реальности большинство операторов ограничиваются минимальной защитой – шифрованием или паролями, без проведения регулярного аудита.

Опыт ЕС и Германии показывает, что эффективная гражданско-правовая защита возможна лишь при наличии института внутреннего контроля (Data Protection Officer) и публичной отчётности перед надзорным органом. В узбекском законодательстве аналогичные функции возложены на ответственного работника по обработке данных (ст. 31 Закона), но правовой статус этого лица не определён, что уменьшает эффективность механизма.

Таким образом, для совершенствования практики необходимо развивать систему технических стандартов и нормативов, а также установить обязанность операторов ежегодно публиковать отчёты о состоянии информационной безопасности и о выявленных инцидентах. Это будет способствовать повышению прозрачности и доверия со стороны пользователей.

**Пути совершенствования правоприменительной практики.** Следует ввести в Закон «О персональных данных» отдельную главу о видах и мерах ответственности, аналогичную ст. 65–66 Закона «Об авторском праве и смежных правах», включая право субъекта на компенсацию морального вреда и

возмещение упущенной выгоды [11:543].

Создание единого реестра судебных решений по делам о нарушении прав на персональные данные для формирования прецедентной практики и правовой определённости.

Внедрение института оценки воздействия на права субъекта (аналог GDPR Art. 35), обязывающего операторов проводить самоаудит перед внедрением новых информационных систем.

Развитие международного сотрудничества в сфере трансграничной передачи данных и присоединение к международным соглашениям о взаимном признании стандартов защиты (в том числе по линиям ОЭСР и Совета Европы).

Разъяснительная работа и повышение цифровой грамотности населения – формирование навыков самозащиты прав в информационной среде и пользования инструментами удалённого контроля (право на «забвение», право на ограничение обработки и т. д.).

Усиление роли судов в обеспечении эффективной защиты – расширение практики компенсации нематериального вреда и применение аналогии с авторско-правовыми спорами в части оценки ущерба.

**Заключение**

Современные тенденции цифровизации требуют перехода от формального регулирования к функциональной системе защиты персональных данных, сочетающей гражданско-правовые, административные и технические меры. Законодательство Республики Узбекистан заложило правовую основу для такой системы, однако для её эффективного применения необходима глубокая адаптация механизмов ответственности и судебного контроля.

Сравнение с европейской, американской и китайской моделями показывает, что универсальным направлением развития является усиление прозрачности и подотчётности операторов, а также признание права на защиту персональных данных в качестве самостоятельного гражданского права. Именно в этом направлении должно развиваться узбекское законодательство и правоприменительная практика, чтобы обеспечить баланс между инновациями и охраной личной сферы.

Персональные данные по своей правовой природе относятся к числу нематериальных благ, находящихся под охраной гражданского законодательства (ст. 9 ГК Республики Узбекистан). Их правовой режим формируется на основе принципов автономии воли, добросовестности и соразмерности, что требует признания права на защиту персональных данных как самостоятельного субъективного гражданского права.

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

Действующий Закон «О персональных данных» (№ ЗРУ-547) сочетает публично-правовые и организационные механизмы, но недостаточно закрепляет «частноправовые последствия» нарушений. В отличие от авторско-правовой защиты (ст. 65 Закона РУз «Об авторском праве и смежных правах»), институт защиты персональных данных пока не содержит чёткой конструкции гражданско-правовой ответственности и критериев возмещения вреда.

Формулировка статьи 27 носит декларативный характер: отсутствуют понятия «надлежащая защита», «уровень безопасности» и «мера ответственности оператора». Это затрудняет судебную квалификацию нарушений и снижает эффективность правоприменения.

Установленное требование хранения данных граждан Узбекистана на территории Республики имеет легитимную цель — обеспечение национального цифрового суверенитета, однако в его нынешней форме оно ограничивает свободу договора и трансграничное движение данных. Вследствие этого возникают барьеры для привлечения зарубежных ИТ-компаний и внедрения международных цифровых платформ (Apple Pay, Google Pay и др.).

В большинстве государств наблюдается отход от модели «жёсткой локализации» в пользу механизма взаимного признания эквивалентной защиты:

ЕС (GDPR) — принцип adequate level of protection;

РФ (ФЗ № 152-ФЗ, ст. 18.1) — допускается трансграничная передача при соблюдении международных договоров;

КНР (PIPL, 2021) — предусмотрена обязательная оценка рисков и уведомление государственного органа.

Следовательно, приоритетной тенденцией является не территориальная изоляция, а «функциональная обеспеченность защиты персональных данных», независимо от местонахождения серверов.

Президент Ш.М. Мирзиёев справедливо указал, что обновление законодательства о персональных данных является ключевым условием цифровой интеграции Узбекистана в мировое экономическое пространство. Баланс между безопасностью и инновациями должен достигаться не запретительными, а правовыми и технологическими средствами.

Дополнить ст. 27 Закона новой частью следующего содержания:

«Собственник и (или) оператор несут гражданско-правовую ответственность за причинённый субъекту персональных данных вред, включая имущественные убытки и моральный вред, в соответствии с гражданским законодательством. При определении размера компенсации суд учитывает характер нарушения, степень вины оператора и последствия утраты конфиденциальности данных.»

Уточнить ст. 27[1] Закона, установив возможность хранения персональных данных за пределами Республики Узбекистан «при наличии договора о взаимном признании эквивалентной защиты» или официального решения уполномоченного органа о надлежащем уровне безопасности иностранного оператора.

Ввести обязанность оператора проводить ежегодную оценку воздействия обработки персональных данных на права субъектов (аналог Data Protection Impact Assessment, предусмотренного ст. 35 GDPR).

Закрепить в законе прямое право субъекта данных на подачу гражданского иска о возмещении ущерба и компенсации морального вреда вследствие незаконной обработки или утечки данных.

Создать единую судебно-информационную базу решений по делам о персональных данных, обеспечивающую единообразие практики и возможность научного анализа правоприменения.

Разработать модель частно-публичного контроля: наряду с государственным надзором (Агентство по информации и массовым коммуникациям) ввести институт уполномоченного представителя по защите персональных данных (Data Protection Officer) с чётко определённым правовым статусом.

Разработать международные соглашения о взаимном признании стандартов защиты персональных данных с основными торговыми и технологическими партнёрами (ЕС, РФ, КНР, Южная Корея), что позволит сохранить национальный контроль при расширении трансграничного цифрового сотрудничества.

**Библиография**

1. Закон Республики Узбекистан “О персональных данных”. //Национальная база данных законодательства, 03.07.2019 г., № 03/19/547/3363; 15.01.2021 г., № 03/21/666/0032; 29.11.2023 г., № 03/23/880/0905

2. Lars Hornuf, Sonja Mangold, Yayun Yang. Data Privacy and Crowdsourcing A Comparison of Selected Problems in China, Germany and the United States. Springer. 2023. 149-p. https://doi.org/10.1007/978-3-031-32064-4

3. Гражданский кодекс Республики Узбекистан // Ведомости Олий Мажлиса Республики Узбекистан, 1996 г., приложение к № 2; 1997 г., № 2, ст. 56/

4. European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.

5. National People’s Congress of the People’s Republic of China. (2021). Personal Information Protection Law of the People’s Republic of China (PIPL). Beijing: NPC. (PIPL, 2021).

6. https://www.gazeta.uz/ru/2025/11/07/personal-data/
7. Lars Hornuf, Sonja Mangold, Yayun Yang. Data Privacy and Crowdsourcing A Comparison of Selected Problems in China, Germany and the United States. Springer. 2023. 149-p. https://doi.org/10.1007/978-3-031-32064-4
8. https://gdpr.eu/data-protection-impact-assessment-template/?utm_source=chatgpt.com
9. https://www.dlapiperdataprotection.com/?c=US&utm_source=chatgpt.com
10. Ultimate Guide to PIPL Compliance: Navigating China’s Personal Information Protection Law» — China Briefing. URL: https://www.china-briefing.com/doing-business-guide/china/company-establishment/pipl-personal-information-protection-law
11. Закон Республики Узбекистан «Об авторском праве и смежных правах». //Собрание законодательства Республики Узбекистан, 2006 г., № 28-29, ст. 260; 2013 г., № 1, ст. 1, № 41, ст. 543.