“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=341

2025-yil
5-son
dekabr
ISSN 3093-8546



Персональные данные как объект гражданско-правовой защиты

Mavjuda Atajanova,
Академии правосудия Республики Узбекистан
Докторант
e-mail: brakhimjanova@gmail.com

Аннотация. Mazkur maqolada jamiyatning raqamlashtirilishi sharoitida shaxsiy ma’lumotlarning fuqarolik-huquqiy mohiyati va ularni himoya qilish masalalari ko‘rib chiqiladi. Muallif O‘zbekiston Respublikasi, Rossiya Federatsiyasi, Yevropa Ittifoqi (GDPR) hamda Amerika Qo‘shma Shtatlarining (Privacy Act, CCPA) qonunchiligini tahlil qilib, huquqiy tartibga solishdagi umumiy prinsiplar va farqli jihatlarni aniqlaydi. Qayd etilishicha, O‘zbekiston qonunchiligi deklarativ xususiyatga ega bo‘lib, shaxsiy ma’lumotlarni fuqarolik-huquqiy himoya qilishning samarali mexanizmlarini belgilash, subyekt roziligi institutini mustahkamlash hamda operatorlarning javobgarligini aniqlash nuqtayi nazaridan yanada takomillashtirishni talab qiladi. Maqolada O‘zbekiston Respublikasi Fuqarolik kodeksida shaxsiy ma’lumotlarni nomoddiy ne’mat sifatida e’tirof etish, shuningdek Yevropa modeli asosida ma’lumotlarni ko‘chirish huquqi va “unutib qo‘yilish huquqi”ni joriy etish zarurati asoslab berilgan. Axborotni himoya qilish bo‘yicha milliy huquqiy tizimni xalqaro standartlarga moslashtirish zarurligi to‘g‘risida xulosalar qilingan.

Калит сўзлар. shaxsiy ma’lumotlar, fuqarolik-huquqiy himoya, maxfiylik, GDPR, CCPA, unutib qo‘yilish huquqi, operator, shaxsiy ma’lumotlar subyekti, nomoddiy ne’matlar, O‘zbekiston qonunchiligi

Аннотация. В статье рассматривается гражданско-правовая природа персональных данных и их защита в условиях цифровизации общества. Автор анализирует законодательство Республики Узбекистан, Российской Федерации, Европейского союза (GDPR) и Соединённых Штатов Америки (Privacy Act, CCPA), выявляя общие принципы и различия в регулировании. Отмечается, что узбекское законодательство носит декларативный характер и требует дальнейшего совершенствования с точки зрения установления эффективных гражданско-правовых механизмов защиты, института согласия субъекта и ответственности операторов. В работе обоснована необходимость признания персональных данных нематериальным благом в Гражданском кодексе Республики Узбекистан, а также внедрения права на переносимость данных и «права быть забытым» по примеру европейской модели. Сделаны выводы о необходимости адаптации национальной правовой системы к международным стандартам защиты информации.

Ключевые слова. персональные данные, гражданско-правовая защита, конфиденциальность, GDPR, CCPA, право на забвение, оператор, субъект персональных данных, нематериальные блага, законодательство Узбекистана

Annotation. The article examines the civil-law nature of personal data and its protection in the context of digital transformation. The author analyzes the legislation of the Republic of Uzbekistan, the Russian Federation, the European Union (GDPR), and the United States (Privacy Act, CCPA), identifying similarities and differences in the legal regulation. It is emphasized that Uzbekistan's legislation remains largely declarative and requires improvement in terms of establishing effective civil-law mechanisms of protection, strengthening the institution of consent, and ensuring the liability of data operators. The study argues for the recognition of personal data as an intangible good within the Civil Code of the Republic of Uzbekistan and for the introduction of the rights to data portability and the "right to be forgotten," following the European approach. The conclusions highlight the need to harmonize Uzbekistan's legal system with international data protection standards.

Keywords. personal data, civil-law protection, confidentiality, GDPR, CCPA, right to be forgotten, data operator, data subject, intangible goods, legislation of Uzbekistan

В условиях цифровизации общества обращение с персональными данными становится одной из ключевых сфер правового регулирования. Персональные данные представляют собой сведения, позволяющие идентифицировать личность, и потому требуют особой правовой защиты. В Узбекистане данный вопрос регулируется Законом «О персональных данных» № ЗРУ-547 от 2 июля 2019 года[1].

Однако стремительное развитие технологий и международные стандарты, заложенные в таких актах, как GDPR (ЕС)[2], Федеральный закон РФ №152-ФЗ[3], а также Privacy Act (США)[4], демонстрируют необходимость совершенствования национального законодательства.

Персональные данные – это зафиксированная на электронном или ином носителе информация, относящаяся к определенному физическому лицу. Они включают сведения о личности, здоровье, биометрические и иные данные. С гражданско-правовой точки зрения такие данные можно рассматривать как нематериальное благо, охраняемое законом. Гражданский кодекс Республики Узбекистан в статьях о нематериальных правах не содержит прямого упоминания персональных данных, что создает пробел в определении их статуса.

Персональные данные следует рассматривать как объект гражданских прав, так как они связаны с личностью человека и

его правом на частную жизнь. Нарушение права на защиту персональных данных может повлечь моральный вред, репутационные потери и иные последствия, требующие гражданско-правовой защиты. В рамках гражданско-правового механизма защиты должны быть предусмотрены: требование об удалении данных, возмещении вреда, а также возможность обращения в суд с требованием о прекращении неправомерной обработки данных. Действующий Закон закрепляет общие гарантии, но не содержит прямого механизма компенсации ущерба.

В Российской Федерации законодательство о персональных данных характеризуется высокой степенью нормативной детализации. Федеральный закон №152-ФЗ «О персональных данных» от 27 июля 2006 года закрепляет базовые принципы обработки информации, включая законность, добросовестность, целесообразность и минимизацию данных. Он вводит четкое разграничение ролей между оператором и субъектом персональных данных, устанавливая обязанность оператора получать согласие на обработку, обеспечивать безопасность хранения и предотвращать несанкционированный доступ. Особое внимание уделено техническим и организационным мерам защиты, включая сертификацию информационных систем и ответственность за утечку данных в административной и уголовной формах.

В ст.152.2 ГК РФ закреплено, что получение, обработка, хранение и распространение сведений, относящихся к личной сфере – таких как происхождение, место жительства, семейные обстоятельства и иные аспекты частной жизни – допускаются исключительно с согласия самого лица. Норма направлена на обеспечение баланса между правом на неприкосновенность частной жизни и свободой информации. Без согласия гражданина любые действия, связанные с обращением информации о его личной жизни (в том числе сбор, хранение, передача или использование), считаются неправомерными. Исключения возможны только в случаях, прямо установленных законом.

Отдельное значение имеет требование конфиденциальности: участники гражданско-правовых отношений не вправе разглашать сведения личного характера, ставшие им известными при исполнении договорных обязательств, если иное не вытекает из содержания договора или закона. Использование информации о частной жизни в произведениях науки, литературы или искусства также должно осуществляться с соблюдением прав и интересов гражданина; нарушение этих требований рассматривается как вмешательство в личную жизнь.

Гражданин, чьи права нарушены, имеет право обратиться в суд с требованиями об удалении незаконно полученных сведений, прекращении их распространения и запрете

дальнейшего использования. Суд также может обязать нарушителя уничтожить материальные носители, содержащие такую информацию. Закон предусматривает после смерти лица право требовать охраны его частной жизни принадлежит ближайшим родственникам: детям, родителям и пережившему супругу. Это обеспечивает продолжение правовой защиты личных интересов даже после смерти гражданина[5].

В США регулирование носит децентрализованный характер: Privacy Act 1974 распространяется на госорганы, а CCPA[6] 2018 – на частные компании, обеспечивая право потребителя на доступ и удаление данных. В сравнении с ними узбекское законодательство более декларативно, недостаточно развит институт согласия субъекта и отсутствует эффективный механизм надзора и ответственности.

В Соединенных Штатах Америки подход к защите персональных данных имеет децентрализованный характер. Основополагающий акт – Privacy Act 1974 – регулирует деятельность федеральных органов власти, устанавливая требования к сбору, использованию и хранению информации о гражданах. Однако в частном секторе регулирование осуществляется на уровне отдельных штатов. Наиболее значимым актом является California Consumer Privacy Act (CCPA) 2018 года, который предоставляет потребителям право знать, какие данные собираются, требовать их удаления и запрещать продажу информации третьим лицам. Таким образом, американская модель основана на принципе «информационного самоуправления», предоставляя гражданам возможность контролировать использование собственных данных.

Вместе с тем американская система имеет и определённые недостатки: отсутствие единого федерального закона о защите данных создает разрозненность правоприменения, а также усложняет трансграничное регулирование. Различия между штатами, например, между Калифорнией и Техасом, приводят к правовой неопределённости и увеличению административных издержек для бизнеса. Однако гибкость американского подхода позволяет быстро адаптироваться к технологическим инновациям, что делает его привлекательным для коммерческого сектора.

В отличие от указанных юрисдикций, узбекское законодательство о персональных данных, закрепленное в Законе № ЗРУ-547 от 2 июля 2019 года, носит более декларативный характер. В нём отсутствует детально проработанный механизм гражданско-правовой защиты, а также не сформирован институт согласия субъекта в его современных формах (например, электронное согласие с возможностью отзыва). Кроме того, в законе не определены критерии «адекватной защиты» при трансграничной передаче данных, что затрудняет международное взаимодействие и

участие узбекских компаний в глобальных цифровых сервисах.

Глава 5 закона Республики Узбекистан «О персональных данных» закрепляет комплекс публично-правовых и частноправовых гарантий, направленных на обеспечение безопасности, конфиденциальности и целостности персональных данных граждан. В отличие от предыдущих редакций, современная структура норм этой главы отражает интеграцию национальной модели регулирования с международными стандартами защиты данных, включая положения GDPR (ЕС), а также положения Конвенции Совета Европы №108.

Статья 27 формулирует общий принцип ответственности государства за создание эффективного правового механизма защиты информации о личности. Системный анализ показывает, что законодатель выделяет три уровня гарантий:

Правовой уровень – закрепление прав и обязанностей субъектов и операторов персональных данных, включая санкции за нарушение установленного режима;

Организационный уровень – внедрение процедур внутреннего контроля, инструкций, регламентов и аудита обработки данных;

Технический уровень – применение сертифицированных средств защиты информации, шифрования и безопасного хранения.

Таким образом, ответственность за соблюдение прав граждан распределяется между государством как гарантом и операторами данных как непосредственными исполнителями. Центральным элементом является право субъекта на защиту от вмешательства в частную жизнь, что соотносится с положениями статьи 27 Конституции Республики Узбекистан и статьи 17 Международного пакта о гражданских и политических правах.

Статья 27^1 представляет собой проявление цифрового суверенитета государства, направленного на обеспечение территориального контроля над обработкой данных. Обязанность размещать серверы и базы персональных данных граждан исключительно на территории Узбекистана служит инструментом минимизации трансграничных рисков и утечки конфиденциальной информации. Введение регистра баз данных обеспечивает прозрачность и подотчётность операторов, а также позволяет государству осуществлять надзор за деятельностью субъектов цифровой экономики. При этом такая территориальная привязка не исключает необходимости международного обмена данными, но требует соблюдения режима адекватной защиты, аналогичного принципу, закреплённому в статье 45 GDPR.

Закон устанавливает основополагающий принцип персональной автономии – запрет на распространение и раскрытие персональных данных без согласия субъекта. В

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

отличие от информационной открытости, конфиденциальность персональных данных носит императивный характер, то есть не может быть ограничена договором, кроме случаев, прямо предусмотренных законом (например, по запросу суда или следственных органов).

Следует отметить, что законодатель закрепил не только обязанность не разглашать данные, но и ответственность за их незаконное использование, включая случаи, когда информация используется в научных, литературных или коммерческих целях без согласия субъекта. Такой подход соответствует принципу «data minimization» — минимизации объёма обрабатываемых данных и целей их использования.

Статья 29 вводит важное разграничение между закрытой и открытой информацией. Общедоступными признаются данные, раскрытые самим субъектом по его волеизъявлению. Это положение закрепляет принцип информированного согласия и предусматривает возможность отзыва согласия, что обеспечивает динамичность правового режима персональных данных. Создание открытых источников (телефонных справочников, интернет-ресурсов, биографических баз) возможно лишь при соблюдении письменной формы согласия и возможности последующего удаления сведений. Эта конструкция призвана предотвратить навязывание открытого доступа и обеспечить гражданину контроль над своим цифровым образом.

Значимым аспектом является право субъекта требовать исключения информации из открытых источников не только по личному обращению, но и по решению суда или уполномоченного органа, что усиливает судебную защиту и делает её превентивным инструментом.

В целом, нормы главы 5 формируют комплексную модель защиты персональных данных, основанную на принципах законности, добросовестности, пропорциональности и прозрачности. Их системное толкование показывает, что законодатель стремится соединить гарантии неприкосновенности частной жизни с требованиями цифровой безопасности, создавая условия для формирования доверия к институтам электронной экономики и государственных онлайн-сервисов.

В дальнейшем развитие этой сферы требует принятия подзаконных актов, детализирующих порядок кибербезопасности, сертификации операторов и трансграничной передачи данных, а также усиления институциональной роли Уполномоченного органа по защите персональных данных как независимого регулятора.

Следует отметить и недостаточную институциональную обеспеченность контроля: уполномоченный государственный орган – Государственный центр персонализации – выполняет преимущественно регистрационные и координационные

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

функции, тогда как полномочия по расследованию нарушений, наложению санкций и защите прав субъектов персональных данных явно ограничены. Отсутствие действенного механизма ответственности, включая административные и гражданско-правовые меры, снижает уровень доверия граждан к цифровым платформам и затрудняет реализацию их права на защиту личной информации. В связи с этим назрела необходимость комплексной модернизации законодательства Республики Узбекистан с учётом принципов GDPR и практики РФ и США, что позволит создать эффективную систему гражданско-правовой охраны персональных данных.

Целесообразно включить в Гражданский кодекс Республики Узбекистан норму, прямо признающую персональные данные нематериальным благом. Также необходимо уточнить порядок возмещения морального вреда при нарушении права на персональные данные, расширить полномочия уполномоченного органа, предусмотрев механизм административных расследований. Необходимо внедрить право субъекта на переносимость данных и «право быть забытым» по примеру GDPR. Установить четкие критерии ответственности операторов баз персональных данных, в том числе в сфере трансграничной передачи.

Персональные данные представляют собой важный элемент правового статуса личности. Они тесно связаны с правом на неприкосновенность частной жизни и требуют комплексного гражданско-правового регулирования. Совершенствование законодательства Республики Узбекистан с учетом международных стандартов позволит повысить уровень доверия к цифровым услугам, обеспечить баланс интересов личности, общества и государства.

Список использованной литературы

1. Закон Республики Узбекистан «О персональных данных» № ЗРУ-547 от 2 июля 2019 г.

2. General Data Protection Regulation (EU) 2016/679 (GDPR).

3. Федеральный закон Российской Федерации «О персональных данных» №152-ФЗ от 27 июля 2006 г.

4. Privacy Act of 1974 (United States).

5. Гражданский кодекс Российской Федерации (часть первая). https://www.consultant.ru/document/cons_doc_LAW_5142/9c307a0f2164645c15ca4e3146ff5f6e56060b23/

6. California Consumer Privacy Act (CCPA), 2018.