SCIENCE AND SOCIETY-
FAN VA JAMIYAT- НАУКА И ОБЩЕСТВО
ILMIY JURNAL



Issue - 11(2026) / ISSN 2992-913X Available at www.uznauka.uz

ПРАВОВЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦИФРОВУЮ ЭПОХУ

Махмудов Алишер Тимур угли

Студент факультета международного права и сравнительного правоведения
Ташкентского государственного юридического университета
Электронная почта: maxmudov.alisher.t@gmail.com

Аннотация. *В статье разбираются пять проблем правового регулирования персональных данных: пределы согласия, граница самого понятия персональных данных, трансграничные передачи, национальные модели с требованием локализации и неравномерность правоприменения. Анализ опирается на акты Европейского союза, практику Суда ЕС за 2015–2025 годы, российское и узбекское законодательство. Автор приходит к выводу, что действующие нормы лучше работают против отдельных нарушений, чем против устойчивых бизнес-моделей, построенных на сборе данных, и что острее всего противоречия проявляются на стыке юрисдикций.*

Ключевые слова: *персональные данные, GDPR, согласие, идентифицируемость, трансграничная передача, локализация данных, ответственность оператора.*

RAQAMLI DAVRDA SHAXSGA DOIR MA’LUMOTLARNI HIMOYA QILISHNING HUQUQIY MUAMMOLARI

SCIENCE AND SOCIETY-
FAN VA JAMIYAT- НАУКА И ОБЩЕСТВО
ILMIY JURNAL



Issue - 11(2026) / ISSN 2992-913X Available at www.uznauka.uz

Maxmudov Alisher Timur o‘g‘li
Toshkent davlat yuridik universiteti Xalqaro huquq va qiyosiy huquqshunoslik fakulteti talabasi
Elektron pochta: maxmudov.alisher.t@gmail.com

Annotatsiya. Maqolada shaxsga doir ma’lumotlarni huquqiy tartibga solishning beshta muammosi tahlil qilinadi: rozilik chegaralari, shaxsga doir ma’lumotlar tushunchasining chegarasi, transchegaraviy uzatish, lokalizatsiya talabini nazarda tutuvchi milliy modellar va huquqni qo‘llashning notekisligi. Tahlil Yevropa Ittifoqi hujjatlari, YeI Sudining 2015–2025-yillardagi amaliyoti, Rossiya va O‘zbekiston qonunchiligiga asoslanadi. Muallif amaldagi normalar ma’lumotlar yig‘ishga qurilgan barqaror biznes modellardan ko‘ra alohida qoidabuzarliklarga qarshi yaxshiroq ishlaydi, ziddiyatlar esa yurisdiksiyalar tutashgan joyda eng keskin namoyon bo‘ladi, degan xulosaga keladi.

Kalit so‘zlar: shaxsga doir ma’lumotlar, GDPR, rozilik, identifikatsiyalanuvchanlik, transchegaraviy uzatish, ma’lumotlarni lokalizatsiya qilish, operator javobgarligi.

LEGAL PROBLEMS OF PERSONAL DATA PROTECTION IN THE DIGITAL AGE

Makhmudov Alisher Timur ugli
Student of the Faculty of International Law and Comparative Jurisprudence, Tashkent State University of Law

SCIENCE AND SOCIETY-
FAN VA JAMIYAT- НАУКА И ОБЩЕСТВО
ILMIY JURNAL



Issue - 11(2026) / ISSN 2992-913X Available at www.uznauka.uz

E-mail: maxmudov.alisher.t@gmail.com

Abstract. The article examines five problems of the legal regulation of personal data: the limits of consent, the boundary of the very concept of personal data, cross-border transfers, national models with data localisation requirements, and uneven enforcement. The analysis draws on European Union acts, the case law of the Court of Justice of the EU for 2015–2025, and Russian and Uzbek legislation. The author concludes that the existing rules work better against individual violations than against sustainable business models built on data collection, and that the contradictions are most acute where jurisdictions meet.

Keywords: personal data, GDPR, consent, identifiability, cross-border transfer, data localisation, operator liability.

ВВЕДЕНИЕ. Право на неприкосновенность частной жизни в современном виде описали в 1890 году Сэмюэл Уоррен и Луис Брандейс [1]. В 1967 году Алан Уэстин сформулировал идею, на которой держится большая часть нынешнего регулирования: человек сам решает, когда, как и в каком объёме сведения о нём становятся доступны другим [2]. Первым обязательным международным договором в этой области стала Конвенция Совета Европы № 108, открытая для подписания 28 января 1981 года и вступившая в силу 1 октября 1985 года [3].

С тех пор объём и характер обработки изменились. Сведения о человеке собирают постоянно, как побочный продукт других услуг, а на их анализе строится поведенческая реклама, которую Шошана Зубофф назвала

SCIENCE AND SOCIETY-
FAN VA JAMIYAT- НАУКА И ОБЩЕСТВО
ILMIY JURNAL



Issue - 11(2026) / ISSN 2992-913X Available at www.uznauka.uz

надзорным капитализмом [4]. Право отвечало новыми актами: Общим регламентом ЕС о защите данных (GDPR) [5], Федеральным законом № 152-ФЗ в России [6], Законом № ЗРУ-547 в Узбекистане [7].

ОСНОВНАЯ ЧАСТЬ (ОБСУЖДЕНИЕ И РЕЗУЛЬТАТЫ). Методология исследования. Анализ опирается на акты Европейского союза, практику Суда ЕС за 2015–2025 годы, российское и узбекское законодательство. Ниже рассмотрено, где эти конструкции дают сбой.

Результаты. 1. Согласие и его пределы. Согласие субъекта остаётся основным инструментом контроля над данными. GDPR требует, чтобы оно было свободным, конкретным, информированным и однозначным (ст. 4(11) и 7) [5]. На практике условие свободы часто не выполняется. Пользователь, которому для доступа к почте, карте или мессенджеру нужно принять политику, не может отказаться без потери услуги. Сам регламент признаёт это в преамбуле: согласие не считается свободным, если между субъектом и оператором существует явное неравенство (п. 43 преамбулы) [5].

Есть и вторая причина, когнитивная. Дэниел Солув показал, что модель «самоуправления приватностью» упирается в пределы человеческого внимания: человек сталкивается с сотнями уведомлений, не может оценить совокупный эффект отдельных согласий, а вред наступает позже и по другой цепочке, чем та, которую он видел при нажатии кнопки [8].

Законодатель отвечает расширением списка других оснований обработки: договор, исполнение обязанности, законный интерес (ст. 6(1) GDPR) [5]. Это снижает нагрузку на согласие, но переносит проблему в

SCIENCE AND SOCIETY-
FAN VA JAMIYAT- НАУКА И ОБЩЕСТВО
ILMIY JURNAL



Issue - 11(2026) / ISSN 2992-913X Available at www.uznauka.uz

другое место. Вопрос о том, перевешивает ли законный интерес оператора права субъекта, оператор решает сам, и проверка, как правило, происходит уже после жалобы.

2. Граница понятия персональных данных. Определение в законодательстве широкое. По 152-ФЗ это любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу (п. 1 ст. 3) [6]. GDPR использует близкую формулу (ст. 4(1)) [5]. Надежда Пуртова указывает на побочный эффект: если под определение подпадает почти любая информация, из которой можно сделать вывод о человеке, закон превращается в «право обо всём», и исполнять его всерьёз невозможно [9].

Суд ЕС в решении от 4 сентября 2025 года по делу EDPS v SRB (C-413/23 P) выбрал контекстный подход. Псевдонимизированные данные не обязаны оставаться персональными для любого получателя: значение имеет то, есть ли у конкретного получателя реальные средства установить личность. Для контролёра, который хранит ключ, такие данные остаются персональными, и обязанность сообщить субъектам о получателях возникает в момент сбора [10]. Практическая сторона проблемы в том, что граница между псевдонимизацией и анонимизацией решает, применяется ли закон вообще, а развитие методов сопоставления массивов данных делает оценку риска повторной идентификации зависимой от меняющейся техники.

3. Трансграничные передачи. В деле Schrems (C-362/14) Суд ЕС 6 октября 2015 года признал недействительным режим Safe Harbor [11]. Решением от 16 июля 2020 года по делу Schrems II (C-311/18) Суд отменил и



Issue - 11(2026) / ISSN 2992-913X Available at www.uznauka.uz

его преемника, Privacy Shield, поскольку американское законодательство о доступе властей к данным не обеспечивало защиты, по существу эквивалентной европейской. Стандартные договорные условия остались в силе, но экспортёр обязан оценить, обеспечивает ли право страны назначения необходимый уровень защиты, и при необходимости добавить меры [12]. Договор между двумя компаниями не связывает государственные органы третьей страны, и это ограничение нельзя снять средствами договорного права.

Новая рамка, EU-U.S. Data Privacy Framework, введена Решением Еврокомиссии 2023/1795 [13]. Общий суд 3 сентября 2025 года отклонил иск Филиппа Латомба об отмене этого решения (T-553/23) [14], но 31 октября 2025 года Латомб подал апелляцию в Суд ЕС (C-703/25 P) [15]. Получается, что правовая основа передач данных через Атлантику за десять лет дважды отменялась и теперь снова оспаривается. Сведений о решении по апелляции на момент подготовки статьи найти не удалось.

Глобального режима нет. Ану Брэдфорд описала «брюссельский эффект»: нормы ЕС распространяются через условия доступа к рынку, без международного договора [16]. Протокол CETS № 223 к Конвенции 108 (Конвенция 108+), открытый для подписания 10 октября 2018 года, вступит в силу после ратификации 38 сторонами [3]. По сообщению Совета Европы, Молдова стала 34-й ратифицировавшей стороной [17], то есть универсальный договор пока не действует.

SCIENCE AND SOCIETY-
FAN VA JAMIYAT- НАУКА И ОБЩЕСТВО
ILMIY JURNAL



Issue - 11(2026) / ISSN 2992-913X Available at www.uznauka.uz

Обсуждение. 4. Национальные модели: локализация и уголовная ответственность. В России 30 ноября 2024 года приняты законы № 420-ФЗ (изменения в КоАП) и № 421-ФЗ (изменения в УК) [18]. Статья 272.1 УК РФ действует с 11 декабря 2024 года. Она устанавливает ответственность за незаконные использование, передачу, сбор и хранение компьютерной информации, содержащей персональные данные, вплоть до десяти лет лишения свободы при тяжких последствиях или совершении преступления организованной группой [18]. Поправки в КоАП, вступившие в силу 30 мая 2025 года, ввели оборотные штрафы за утечки [18]. В «Коммерсанте» отмечалось, что соотношение новой статьи с ч. 2 ст. 273 УК и возможность квалификации по совокупности ещё предстоит выяснить на практике [19].

В Узбекистане Закон № ЗРУ-547 принят 2 июля 2019 года и действует с 1 октября 2019 года [7]. Правило о локализации баз данных вступило в силу 16 апреля 2021 года [20]. По оценке М. Махкамовой, узбекская модель закрепляет основные права субъектов и в целом соответствует международным принципам, но содержит особенности, среди которых требование локализации [21].

Автор полагает, что локализация и уголовные нормы решают разные задачи. Локализация даёт государству юрисдикционный доступ к данным, но сама по себе не защищает от утечки: сервер на своей территории так же уязвим для взлома, как и любой другой. Уголовная ответственность направлена на оборот похищенных баз, но размытые составы создают неопределённость для добросовестных операторов. Для компаний с

SCIENCE AND SOCIETY-
FAN VA JAMIYAT- НАУКА И ОБЩЕСТВО
ILMIY JURNAL

Issue - 11(2026) / ISSN 2992-913X Available at www.uznauka.uz

международной инфраструктурой каждая такая норма добавляет ещё один режим, который нужно совместить с GDPR.

5. Правоприменение. GDPR допускает штрафы до 20 млн евро или 4 процентов годового мирового оборота (ст. 83(5)) и требует уведомлять надзорный орган об утечке в течение 72 часов (ст. 33) [5]. Человек, чьи данные утекли, находится в другом положении: он должен доказать ущерб. В деле Österreichische Post (C-300/21, решение от 4 мая 2023 года) Суд ЕС указал, что установление минимального порога тяжести нематериального вреда недопустимо, но сам вред и причинная связь должны быть доказаны [22]. Если данные украдены, а прямых убытков нет, получить компенсацию трудно. Штрафы работают против операторов, а компенсация для субъектов остаётся слабым звеном.

ЗАКЛЮЧЕНИЕ. Первое: согласие нельзя считать достаточной защитой там, где у субъекта нет реального выбора, поэтому нагрузка смещается на обязанности оператора и на надзор. Второе: граница понятия персональных данных стала контекстной, и вопрос о применимости закона всё чаще решается оценкой технических возможностей конкретного получателя. Третье: трансграничные передачи зависят от решений, которые могут быть отменены, пока нет универсального договора, а Конвенция 108+ не вступила в силу. Четвёртое: национальные меры вроде локализации и уголовных норм повышают давление на операторов, но не заменяют механизмов, которые помогают самим субъектам получить защиту и



Issue - 11(2026) / ISSN 2992-913X Available at www.uznauka.uz

компенсацию. Для дальнейшего изучения остаются практика применения ст. 272.1 УК РФ и первые судебные решения по оборотным штрафам.

СПИСОК ЛИТЕРАТУРЫ

1. Warren, S.D., Brandeis, L.D. The Right to Privacy. Harvard Law Review. 1890; 4(5):193–220.

2. Westin, A.F. Privacy and Freedom. New York: Atheneum, 1967.

3. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Strasbourg, 28.01.1981; Protocol amending the Convention (CETS No. 223), 10.10.2018. Council of Europe. https://rm.coe.int/1680ac8ff3

4. Zuboff, S. The Age of Surveillance Capitalism. New York: PublicAffairs, 2019.

5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union. 2016; L 119:1–88.

6. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

7. Закон Республики Узбекистан от 02.07.2019 № ЗРУ-547 «О персональных данных».

8. Solove, D.J. Introduction: Privacy Self-Management and the Consent Dilemma. Harvard Law Review. 2013; 126(7):1880–1903.



Issue - 11(2026) / ISSN 2992-913X Available at www.uznauka.uz

9. Purtova, N. The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology. 2018; 10(1):40–81.

10. Judgment of the Court of Justice of 4 September 2025, EDPS v Single Resolution Board, C-413/23 P.

11. Judgment of the Court of Justice of 6 October 2015, Schrems, C-362/14.

12. Judgment of the Court of Justice of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, C-311/18; Press release No 91/20. https://www.statewatch.org/media/1316/eu-cjeu-schrems-ii-pr-16-7-20.pdf

13. Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 on the adequate level of protection of personal data under the EU-US Data Privacy Framework.

14. Judgment of the General Court of 3 September 2025, Latombe v Commission, T-553/23, ECLI:EU:T:2025:831.

15. Appeal brought on 31 October 2025 by Philippe Latombe against the judgment of the General Court in Case T-553/23, Case C-703/25 P. Official Journal of the European Union. C/2025/6610. https://eur-lex.europa.eu/eli/C/2025/6610/oj/eng

16. Bradford, A. The Brussels Effect. Northwestern University Law Review. 2012; 107(1):1–68.

17. Republic of Moldova becomes the 34th State to ratify the Convention 108+. Council of Europe. https://www.coe.int/en/web/data-protection/-/republic-of-moldova-becomes-the-34th-state-to-ratify-the-convention-108-



Issue - 11(2026) / ISSN 2992-913X Available at www.uznauka.uz

18. Федеральные законы от 30.11.2024 № 420-ФЗ и № 421-ФЗ о внесении изменений в КоАП РФ и УК РФ (ст. 272.1 УК РФ).

19. Домшенко, В. Данные растут в цене. Коммерсантъ. 24.04.2025. https://kommersant.ru/doc/7675231

20. Uzbekistan: data localisation rule enters into force. DataGuidance. https://www.dataguidance.com/news/uzbekistan-data-localisation-rule-enters-force

21. Махкамова, М. Шахсий маълумотларни бошқаришнинг қиёсий таҳлили: Ўзбекистон ва халқаро стандартлар. Жамият ва инновациялар (Society and Innovations). 2025. https://inscience.uz/index.php/socinov/article/download/7259/7025/22149

22. Judgment of the Court of Justice of 4 May 2023, UI v Österreichische Post AG, C-300/21.