LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2025) / ISSN 3030-3052 Available at www.uznauka.uz

СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ МЕЖДУНАРОДНОГО ОПЫТА ОСУЩЕСТВЛЕНИЯ ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Баходирова Икбола Иброхим кизи
Магистр Ташкентского государственного юридического университета

Аннотация: *в статье проводится сравнительно-правовой анализ подходов к обезличиванию персональных данных в различных юрисдикциях. Рассматриваются правовые режимы Европейского союза, США и Китая, а также дается оценка эффективности применяемых механизмов с точки зрения баланса между защитой конфиденциальности и возможностью использования данных. Обосновывается необходимость международной правовой гармонизации и унификации понятийного аппарата в области анонимизации данных.*

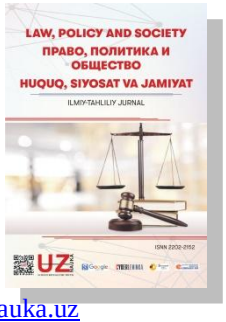
Ключевые слова*: обезличивание, анонимизация, персональные данные, GDPR, HIPAA, PIPL, правовое регулирование, сравнительный анализ.*

COMPARATIVE LEGAL ANALYSIS OF INTERNATIONAL EXPERIENCE IN IMPLEMENTING PERSONAL DATA DEPRESSION

Bakhodirova Ikbola Ibrohim kizi
Master of Tashkent State University of Law

Abstract*: the article provides a comparative legal analysis of approaches to anonymization of personal data in different jurisdictions. The legal regimes of the European Union, the USA and China are considered, and the efficiency of the applied mechanisms is assessed from the point of view of the balance between privacy protection and the possibility of data use. The necessity of international legal harmonization and unification of the conceptual apparatus in the field of data anonymization is substantiated.*

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2025) / ISSN 3030-3052 Available at www.uznauka.uz



Keywords: *depersonalization, anonymization, personal data, GDPR, HIPAA, PIPL, legal regulation, comparative analysis.*

Современное общество характеризуется растущей цифровизацией всех сфер жизни, что неизбежно влечет за собой активную обработку персональных данных. В этом контексте проблема их надлежащей защиты становится не только предметом национальной, но и глобальной правовой повестки. Одним из ключевых механизмов, обеспечивающих защиту конфиденциальности личности при сохранении функциональности данных, выступает их обезличивание.

Однако несмотря на широкое признание важности обезличивания, в международной практике отсутствует единый подход к его правовой природе, методологии и критериям допустимости. Это порождает как практические затруднения в трансграничной передаче данных, так и теоретические споры о границах правового регулирования. Настоящая статья ставит целью проведение сравнительно-правового анализа международного опыта в этой области с акцентом на выявление общих принципов и национальных особенностей.

Общий регламент по защите данных представляет собой всеобъемлющий правовой акт, регулирующий обработку персональных данных на территории Европейского Союза. Одной из центральных тем GDPR является обеспечение конфиденциальности при обработке данных, включая методы снижения рисков через обезличивание (анонимизацию) и псевдонимизацию. GDPR прямо не вводит термин «обезличивание», но в

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2025) / ISSN 3030-3052 Available at www.uznauka.uz

рецитале 26[1] указывается, что: «Принципы защиты данных не применяются к анонимной информации, то есть информации, которая не относится к идентифицированному или идентифицируемому физическому лицу, или к персональным данным, анонимизированным таким образом, что субъект данных не может быть идентифицирован».

Таким образом, обезличенные данные исключаются из сферы действия GDPR, при условии, что идентификация субъекта невозможна ни напрямую, ни косвенно — даже с использованием дополнительных данных, которые могут быть «разумно доступны» третьим лицам.

GDPR признаёт обезличивание как эффективный способ выведения данных из-под действия законодательства, но предъявляет к ней жесткие технические и юридические требования. Псевдонимизация, в свою очередь, рассматривается как важный инструмент повышения безопасности, но не освобождает от соблюдения закона. Надлежащая реализация этих механизмов требует как глубокого технического анализа, так и правовой экспертизы, особенно в условиях использования больших данных и ИИ.

В законодательстве **Соединенных Штатах Америки** принято два уровня правового регулирования любых значимых отношений: на уровне федерации и на уровне штатов, чьи полномочия в области законотворчества по Конституции США очень широки В США регулирование обезличивания персональных данных в здравоохранении осуществляется в первую очередь в рамках Закона HIPAA[2], принятого в 1996 году. Конкретные положения касаются защищённой медицинской информации (PHI – Protected Health

[1] Общий регламент Европейского Союза по защите данных (GDPR) [Электронный ресурс]. – https://gdpr-text.com/ru/.
[2] HIPAA (Закон о переносимости и подотчётности медицинского страхования) [Электронный ресурс]. Режим доступа: https://www.cms.gov/priorities/key-initiatives/burden-reduction/administrative-simplification/hipaa.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2025) / ISSN 3030-3052 Available at www.uznauka.uz

Information) и содержатся в HIPAA Privacy Rule, утвержденном Министерством здравоохранения и социальных служб США (HHS).

PHI охватывает любую информацию, связанную с состоянием здоровья, оказанием медицинских услуг или оплатой, которая может быть связана с конкретным пациентом. Закон разрешает использование PHI только с соблюдением строгих условий, включая согласие пациента, за исключением специальных случаев.

Несмотря на формальную «защиту» обезличенных данных от HIPAA, в США активно обсуждается вопрос повторной идентификации при помощи внешних наборов данных (например, при сопоставлении с соцсетями или данными мобильных операторов). Это особенно актуально в эпоху больших данных и искусственного интеллекта.

Порядок обезличивания персональных данных в рамках HIPAA строится на двух официальных методах, обеспечивающих юридическое освобождение от большинства требований закона. Однако при этом сохраняется обязанность добросовестного применения этих методов и минимизации риска повторной идентификации. Практика в США показывает, что организациям необходимо сочетать формальные правовые критерии с современными техническими средствами защиты данных, чтобы обезличивание было эффективным и устойчивым.

Китайский **Закон о защите персональной информации (PIPL)** регулирует анонимизацию в общем виде, признавая ее способом обработки, не позволяющим идентифицировать личность. Регулирование обработки и защиты персональных данных в Китае получило четкое правовое оформление с принятием закона от 1 ноября 2021 года.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2025) / ISSN 3030-3052 Available at www.uznauka.uz

Согласно ст. 4 PIPL[3], персональная информация определяется как любая информация, связанная с идентифицированным или идентифицируемым физическим лицом, за исключением информации, которая была обезличена. Обезличенная информация определяется в китайском законе как данные, которые не могут быть использованы для идентификации конкретного субъекта персональных данных без использования дополнительной информации. Это понятие аналогично псевдонимизации в европейском GDPR.

Однако китайское законодательство делает важное разграничение: даже обезличенная информация может считаться персональной, если существует возможность повторной идентификации. Следовательно, данные признаются неперсональными только в том случае, если обезличивание носит устойчивый и необратимый характер.

PIPL устанавливает несколько ключевых требований к порядку обезличивания:

- **Технические и организационные меры:** организации обязаны принимать меры, предотвращающие повторную идентификацию данных, включая шифрование, маскирование, агрегирование и минимизацию.

- **Оценка рисков:** до использования обезличенных данных необходимо провести оценку рисков повторной идентификации и зафиксировать ее результаты в отчетах внутреннего контроля.

[3] Закон КНР «О защите персональной информации» https://m.thepaper.cn/baijiahao_15176859.

Issue - 5(2025) / ISSN 3030-3052 Available at www.uznauka.uz

- **Отдельное хранение идентификаторов:** информация, которая позволяет восстановить идентичность субъекта, должна храниться отдельно, с ограниченным доступом.

- **Учет целей обработки:** данные, прошедшие псевдонимизацию, могут использоваться для статистики и научных исследований без получения согласия субъекта, при условии, что личность не будет восстановлена.

Однако китайское законодательство подчёркивает, что технические средства должны сопровождаться правовой и организационной ответственностью. Статья 73 PIPL[4] гласит, что «организация обязана предотвращать несанкционированный доступ, раскрытие или повторную идентификацию обезличенных данных». В случае утечки или нарушений — даже в отношении обезличенной информации — возможна административная или уголовная ответственность.

Таким образом, законодательство Китая признаёт важность обезличивания персональных данных как меры защиты конфиденциальности и как условия законного использования данных без согласия субъекта. Вместе с тем китайский подход требует строгой правовой, технической и организационной дисциплины, чтобы данные действительно утратили идентифицирующий характер. PIPL демонстрирует стремление Китая к гармонизации с международной практикой, включая элементы, сходные с GDPR, при этом сохраняя характерную строгость в отношении контроля государства за оборотом данных.

[4] Закон КНР «О защите персональной информации» https://m.thepaper.cn/baijiahao_15176859.

В условиях роста объемов трансграничных потоков данных разработка международно-признанных руководящих принципов по обезличиванию является приоритетной задачей правового сообщества и должна базироваться на балансе интересов личности, бизнеса и государства.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Общий регламент по защите данных (GDPR) [Электронный ресурс]. Режим доступа: https://gdpr-text.com/ru/.

2. HIPAA (Закон о переносимости и подотчётности медицинского страхования) [Электронный ресурс]. Режим доступа: https://www.cms.gov/priorities/key-initiatives/burden-reduction/administrative-simplification/hipaa.

3. Закон КНР «О защите персональной информации» [Электронный ресурс]. Режим доступа: https://m.thepaper.cn/baijiahao_15176859.

4. Малеина, М.Н. Право на тайну и неприкосновенность персональных данных / М.Н. Малеина // Журнал российского права. - 2010. - № 11. - С. 19 - 24.