УДК 341:342(4/9)
ГРНТИ: 10.87.17

О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЕВРОПЕЙСКОМ СОЮЗЕ И КАЗАХСТАНЕ В СРАВНИТЕЛЬНОЙ ПЕРСПЕКТИВЕ

Аубакирова Индира Ураловна[1]
Доктор юридических наук, директор Института законодательства и правовой информации МЮ РК; г. Астана, Республика Казахстан; e-mail: aubakirova.i@zqai.kz; IstinaResearcherID (IRID): 22529478; eLIBRARY ID: 819608

Толеубек Айжан Аманбайкызы
Магистрант Maqsut Narikbayev University; г. Астана, Республика Казахстан; e-mail: aizhantoleubekk@gmail.com

Аннотация. *Право на конфиденциальность частной жизни относится к базовым правам человека и гражданина. Оно закреплено в международных правовых документах, конституциях государств, в том числе Конституции Республики Казахстан. В современных реалиях развития цифровых технологий аспекты, связанные с регулированием и реализацией указанного права, приобрели особую актуальность. В данной статье рассматриваются нормативные акты, закрепляющие нормы по защите персональных данных в Европейском союзе, проводится сравнительный их анализ с нормами казахстанского законодательства, а также рассматривается соответствующая правоприменительная практика. Особое внимание уделяется требованиям Общего Регламента о защите персональных данных (GDPR), который является основным нормативным документом, регулирующим обработку персональных данных физических лиц в рамках Европейского союза. Авторы исследуют особенности осуществления процедур сбора, обработки и сроков хранения персональных данных в Казахстане сквозь призму требований GDPR. Проводится сравнительный анализ текущей ситуации по защите персональных данных в законодательствах ЕС и РК, на основе которого предлагаются рекомендации по совершенствованию норм законодательных актов. В результате исследования выявлено наличие пробелов в правовом регулировании защиты персональных данных в ЕС и РК. Авторами было определено, что и в требованиях GDPR, и нормах законодательства Казахстана по защите персональных данных, отсутствует установление сроков хранения информации. Однако в случае GDPR существует прецедентная практика, компенсирующая неопределенность законодательства, тогда как для казахстанского законодательства подобный пробел чреват негативными последствиями. Анализ проблемы защиты персональных данных проводится на основе реальных судебных дел. Авторы акцентируют внимание на том, что ориентация казахстанского законодателя на европейские нормотворческие практики могло бы усилить защищенность казахстанских граждан в вопросах, касающихся их права на конфиденциальность частной жизни.*

Ключевые слова: *персональные данные, сроки хранения персональных данных, сбор и обработка персональных данных, регламент GDPR, закон РК «О персональных данных и их защите», право на частную жизнь, права человека, право на защиту персональных данных.*

ЖАЛПЫ ДЕРЕКТЕРДІ ҚОРҒАУ РЕГЛАМЕНТІ (GDPR) ТАЛАПТАРЫН ҚАЗАҚСТАН ЗАҢНАМАСЫНА ИМПЛЕМЕНТАЦИЯЛАУ ПЕРСПЕКТИВАЛАРЫ

Индира Ураловна Аубакирова
Заң ғылымдарының докторы, ҚР ӘМ Заңнама және құқықтық ақпарат институты директоры; Астана қ., Қазақстан Республикасы; e-mail: aubakirova.i@zqai.kz; IstinaResearcherID (IRID): 22529478; eLIBRARY ID: 819608

[1] *Автор для корреспонденции*

Айжан Аманбайқызы Төлеубек
Maqsut Narikbayev University магистранты; Астана қ., Қазақстан Республикасы; e-mail: aizhantoleubekk@gmail.com

Аннотация. *Жеке өмірдің құпиялылығына құқық – адам мен азаматтың негізгі құқықтарының бірі. Бұл құқық халықаралық құқықтық құжаттарда және Қазақстан Республикасының Конституциясында бекітілген. Сандық технологиялардың дамуы жағдайында аталған құқықты реттеу және жүзеге асыру аспектілері ерекше өзектілікке ие болуда. Бұл мақалада Еуропалық Одақта дербес деректерді қорғау жөніндегі нормаларды бекітетін нормативтік актілер қаралады, оларды қазақстандық заңнама нормаларымен салыстырмалы талдау жүргізіледі, сондай-ақ тиісті құқық қолдану практикасы қаралады. Еуропалық Одақ шеңберінде жеке тұлғалардың дербес деректерін өңдеуді реттейтін негізгі нормативтік құжат болып табылатын дербес деректерді қорғау туралы жалпы Регламенттің (GDPR) талаптарына ерекше назар аударылады. Авторлар Қазақстандағы дербес деректерді жинау, өңдеу және сақтау мерзімдерін жүзеге асыру ерекшеліктерін GDPR талаптары тұрғысынан зерттейді. Еуропалық Одақ пен Қазақстан Республикасының дербес деректерді қорғау саласындағы заңнамалық жағдайының салыстырмалы талдауы жүргізіледі. Осы талдаудың негізінде заңнамалық актілер нормаларын жетілдіруге қатысты ұсыныстар жасалған. Зерттеу нәтижесінде ЕО мен ҚР-дағы дербес деректерді құқықтық реттеуде олқылықтардың бар екендігі анықталды. Авторлар GDPR талаптарында да, Қазақстан Республикасының дербес деректерді қорғау туралы заңнамасында да ақпаратты сақтау мерзімінің нақты белгіленбегенін атап көрсетеді. Алайда, GDPR жағдайында заңнамалық белгісіздікті өтейтін прецеденттік практика бар, ал Қазақстан заңнамасында мұндай олқылық жағымсыз салдарға әкелуі мүмкін. Дербес деректерді қорғау мәселесі нақты сот істерінің негізінде талданады. Авторлар Қазақстан заңнамасының еуропалық заң шығару тәжірибелеріне бағдарлануы ел азаматтарының жеке өмірдің құпиялылығы құқығы саласындағы қорғалу деңгейін арттыра алатынын атап өтеді.*

Түйінді сөздер: *дербес деректер, дербес деректерді сақтау мерзімдері, дербес деректерді жинау және өңдеу, GDPR регламенті, ҚР «Дербес деректер және оларды қорғау туралы» заңы, жеке өмірге құқық, адам құқықтары, дербес деректерді қорғау құқығы.*

PROSPECTS FOR THE IMPLEMENTATION OF THE GENERAL DATA PROTECTION REGULATION (GDPR) REQUIREMENTS INTO THE LEGISLATION OF KAZAKHSTAN

Aubakirova Indira Uralovna
Doctor of Law, Director of the Institute of Legislation and Legal Information of the Ministry of Justice of the RK; Astana c., Republic of Kazakhstan; e-mail: aubakirova.i@zqai.kz; IstinaResearcherID (IRID): 22529478; eLIBRARY ID: 819608

Toleubek Aizhan Amanbaykyzy
Master's Student at Maqsut Narikbayev University; Astana c., Republic of Kazakhstan; e-mail: aizhantoleubekk@gmail.com

Abstract. *The right to privacy is one of the fundamental human and civil rights. It is enshrined in international legal instruments and the Constitution of the Republic of Kazakhstan. In the modern era of digital technology development, issues related to the regulation and implementation of this right have gained particular relevance. This article examines the regulations that establish the norms for the protection of personal data in the European Union, conducts a comparative analysis of them with the norms of Kazakh legislation, and also examines the relevant law enforcement practice. Particular attention is paid to the requirements of the General Data Protection Regulation (GDPR), which is the main regulatory document governing the processing of personal data of individuals within the European Union. The authors analyze the peculiarities of personal data collection, processing, and retention periods in Kazakhstan through the lens of GDPR requirements. A comparative analysis of the current situation regarding personal data protection in the legislation*

of the EU and Kazakhstan is conducted, based on which recommendations for improving legislative norms are proposed. The study identifies gaps in the legal regulation of personal data protection in both the EU and Kazakhstan. The authors determine that both GDPR requirements and the norms of Kazakhstan's legislation on personal data protection lack explicit provisions regarding data retention periods. However, in the case of GDPR, there is established case law that compensates for legislative uncertainty, whereas for Kazakhstan's legal system, such a gap may lead to negative consequences. The analysis of personal data protection issues is based on real court cases. The authors emphasize that aligning Kazakhstan's legislative framework with European regulatory practices could enhance the protection of Kazakhstani citizens in matters related to their right to privacy.

Keywords: *personal data, data retention periods, personal data collection and processing, GDPR regulation, Law of the Republic of Kazakhstan "On Personal Data and Their Protection", right to privacy, human rights, right to personal data protection.*

DOI: 10.52026/2788-5291_2025_80_1_174

Введение

В современном мире эволюция международного права, включая сферу прав человека, объективно актуализирует проблематику соотношения его с национальным законодательством. Цифровые технологии приобретают особую значимость, влияя на темпы модернизации экономики, развитие сфер образования, здравоохранения, культуры. Позитивной стороной этого феномена является улучшение бизнес-процессов, расширение спектра коммуникационных возможностей и доступа к информации, распространение онлайн-образования, развитие телемедицины и других технологий в сфере здравоохранения. Цифровые технологии, безусловно, подняли на более высокий уровень качество оказания государственных и банковских услуг, вовлекая широкие слои населения в использование потенциала электронного правительства.

Вместе с тем, в стремительно меняющихся условиях цифровой эпохи проблематизируется вопрос защиты персональных данных. С каждым годом объем личной информации, собираемой, обрабатываемой и хранимой организациями, в том числе государственными, увеличивается в геометрической прогрессии. Данный процесс становится предметом рассмотрения как отечественных, так и зарубежных ученых и практиков с точки зрения роста потребности в релевантных механизмах обеспечения защиты граждан от использования их личных данных в преступных или недобросовестных целях. По существу, сегодня концепция защиты частной жизни приобрела ключевой аспект в проблематике прав человека и гражданина. Защита персональных данных, являясь неотъемлемой частью конституционного права личности на конфиденциальность своей частной жизни, безусловно, имеет глубокий международно-правововой контекст. В казахстанском юридическом дискурсе справедливо подмечается, что международный опыт демонстрирует различные подходы к регулированию области защиты права на неприкосновенность частной жизни. Так, к частной жизни публичной фигуры допускается более повышенный общественный интерес, чем к обычному гражданину [1]. При этом отечественные ученые-конституционалисты дают следующее определение: «Под правом человека и гражданина на личную неприкосновенность понимается закрепленное в Конституции и законодательстве Республики субъективное право каждого человека на всемерную защиту со стороны государства не только физической, психической и духовной жизни индивида, но и тех условий, которые создают ему возможность беспрепятственно пользоваться своими благами для реализации личных потребностей, если это не противоречит интересам индивида, общества и государства» [2].

Важнейшим инструментом защиты права на приватность в период масштабного использования информационных технологий, включая технологии искусственного интеллекта (ИИ), является разработка государствами соответствующих стандартов по обработке и хранению персональных данных. При этом внедрение подобных систем вызывает среди юридической общественности особое внимание, учитывая, что эта сфера тесно сопряжена с принципом конституционной неприкосновенности частной жизни. Как отмечается в научной литературе, сегодня актуализировалась потребность в четких международных стандартах разработки и использования технологий искусственного интеллекта, которые бы устанавливали запреты и ограничения в тех направлениях деятельности, которые входят в противоречие

с идеей конституционализма. Например, на использование ИИ для массового распознавания лиц и других форм биометрической идентификации публичными и частными субъектами [3].

В настоящее время правовые механизмы контроля и защиты, направленные на обеспечение безопасности личных данных граждан, активно внедряются на европейском пространстве. Заметим, что институт защиты персональных данных и зародился в Европе еще в XIX веке, когда юристы, прежде всего, адвокаты, ратовали за регулирование вопросов, связанных с личной информацией (соблюдение privacy). На это большое влияние оказала христианская традиция тайны исповеди. Сегодня к личной информации относится намного более широкий перечень данных, включая системы биометрических и иных данных, хранящихся в удостоверяющих личность документах, используемых в современных государственных и иных организациях.

В Казахстане государственной структурой, в компетенцию которой входит обеспечение защиты персональных данных, основываясь на принципах законности и конфиденциальности, является Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности. Нормативно-правовое сопровождение сферы обеспечения кибербезопасности и разработка соответствующих рекомендаций по защите персональных данных входит в число основных функций Комитета. Однако сфера защиты персональных данных с неизбежностью входит в той или иной степени в круг полномочий фактически всех государственных органов. Глава государства К.-Ж.К Токаев в этом ракурсе на расширенном заседании Правительства 28 января 2025 года отмечал необходимость объединения усилий Правительства, Комитета национальной безопасности, Генеральной прокуратуры и других ведомств, чтобы помочь МВД РК в раскрытии разного рода преступлений для обеспечения максимальной защиты персональных данных граждан. Учитывая, что рассматриваемая проблематика носит развивающийся и одновременно злободневный для страны характер, и при этом практика зачастую опережает процессы по совершенствованию правового регулирования рассматриваемой сферы, то, полагаем, для казахстанских государственных органов было бы весьма плодотворным познать особенности опыта европейских стран.

Материалы и методы

Материалами для данной статьи стали нормативные требования стран-участниц Европейского Союза, установленные в Общем Регламенте о защите персональных данных (GDPR), материалы по правовому регулированию сферы защиты персональных данных в Республике Казахстан, а также судебные дела. Изучены нормы законодательства европейских стран в правовом регулировании отношений, связанных с правом граждан на конфиденциальность частной жизни. В ходе исследования использовались сравнительно-правовой, диалектический, аналитический, логический и структурно-функциональный методы научного познания.

Результаты и обсуждение

Обратимся к сравнительному анализу казахстанского законодательства с подходами к правовому регулированию рассматриваемых проблем в европейском законодательстве. Вопрос защиты персональных данных и права на частную жизнь является одной из ключевых тем в современных правовых системах, особенно в условиях стремительного развития цифровых технологий и глобализации информационных потоков. Казахстанское законодательство в данной сфере основывается на ряде международных и национальных правовых актов, которые в совокупности формируют систему защиты персональных данных. В этом разделе представлен детальный анализ основных источников права, регулирующих рассматриваемую область, с акцентом на различия между казахстанским и европейским подходами.

Основные источники права, касающиеся предмета рассматриваемой проблематики.

Защита персональных данных и право на неприкосновенность частной жизни регламентируются как международными, так и национальными правовыми актами. Основные источники права в данной области включают следующие нормативные документы:

1. Международный пакт о гражданских и политических правах (ратифицирован Казахстаном 28 ноября 2005 года).

Международный пакт о гражданских и политических правах (МПГПП) является одним из ключевых международных документов, закрепляющих базовые права и свободы человека, включая право на частную жизнь.

— Статья 17.1. пакта закрепляет право каждого человека на защиту от произволь-

ного или незаконного вмешательства в его частную жизнь, семью, жилище или переписку, а также от посягательств на его честь и репутацию.

— В контексте персональных данных данное положение интерпретируется как гарантия защиты информации, относящейся к частной жизни человека. Это подчеркивает необходимость строгого регулирования сбора, хранения и обработки персональных данных, исключая их неправомерное использование.

— Пакт накладывает на государства-участники обязательства по созданию законодательной базы, обеспечивающей реализацию данного права. Казахстан, ратифицировав данный пакт, принял на себя международные обязательства по защите персональных данных и внедрению соответствующих законодательных норм.

— Комитет по правам человека ООН, уполномоченный толковать положения Пакта, неоднократно подчеркивал важность защиты персональных данных как неотъемлемой части права на частную жизнь.

Таким образом, нормы МПГПП служат основой для национального законодательства Казахстана в области защиты персональных данных, определяя общие принципы, которые должны быть учтены при разработке законов и правоприменительной практики.

2. Регламент Европейского Парламента и Совета Европейского Союза 2016/679 (принят 27 апреля 2016 года и вступил в силу 25 мая 2018 года).

Общий регламент о защите персональных данных (General Data Protection Regulation, GDPR) — это фундаментальный нормативный акт ЕС, регулирующий обработку персональных данных физических лиц. Этот документ, принятый 27 апреля 2016 года и вступивший в силу 25 мая 2018 года, считается одним из самых строгих и современных стандартов защиты персональных данных в мире.

— GDPR устанавливает строгие требования к обработке персональных данных, обеспечивая их законность, добросовестность и прозрачность, а также ограничивая их использование только заранее определенными и законными целями. Регламент вводит принцип минимизации данных, требуя сбора только необходимого объема информации, а также устанавливает ограничение сроков хранения, согласно которому персональные данные не могут храниться дольше, чем необходимо.

— Данный документ вводит строгие требования к операторам персональных данных, включая необходимость получения согласия на обработку, обязательства по защите данных и права граждан на доступ к своим данным, их исправление или удаление.

Таким образом, GDPR представляет собой один из наиболее детализированных нормативных актов в сфере защиты персональных данных, устанавливая высокие стандарты обработки, хранения и безопасности информации. Казахстан не является участником GDPR. Однако его требования оказывают значительное влияние на национальные стандарты регулирования персональных данных во многих странах, что позволяет рассматривать их в качестве ориентира и для совершенствования казахстанского законодательства, гармонизации его с лучшими практиками в сфере защиты права на частную жизнь.

3. Конституция Республики Казахстан (принята 30 августа 1995 года на всенародном референдуме).

— В соответствии со статьей 1 Конституции РК, высшей ценностью государства признается человек, его жизнь, права и свободы.

— Статья 18 Конституции закрепляет основные принципы защиты личных данных, утверждая право каждого на неприкосновенность частной жизни, личную и семейную тайну. Диспозиция указанной статьи гарантирует защиту чести и достоинства граждан.

Конституция Казахстана служит фундаментом формирования национального законодательства в области защиты персональных данных, устанавливают правовую основу для разработки специализированных законов и механизмов защиты данных, обеспечивая основные гарантии конфиденциальности и недопустимости незаконного сбора и распространения личной информации,

4. Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года.

— Регулирует вопросы сбора, обработки, хранения и защиты персональных данных на территории Казахстана.

— Устанавливает правила взаимодействия между субъектами персональных данных, операторами и уполномоченными органами.

— С учетом необходимости обеспечения прав и свобод граждан в процессе обработки персональных данных предусматривает ответственность за нарушение установленных норм.

Указанному закону принадлежит важнейшая роль в обеспечении правовой защиты персональных данных, установлении инструментария по их обработке и хранению. Он нацелен на обеспечение права на конфиденциальность и безопасность личной информации, регулирование взаимоотношений между субъектами персональных данных, операторами и государственными органами.

Закон имеет особую значимость в формировании и развитии национальной системы правового регулирования рассматриваемой сферы, и его положения необходимо соотносить с международными стандартами, заимствовать лучшие зарубежные подходы в правовом регулировании.

Сравнительный анализ правовых положений в области персональных данных согласно GDPR и РК.

1. Общее и особенное в основных положениях GDPR и законодательстве Республики Казахстан по защите персональных данных.

Общий регламент по защите данных (GDPR) дает следующее определение понятия персональных данных – это «любая информация, относящаяся к субъекту данных, то есть идентифицированному или поддающемуся идентификации физическому лицу. Под «поддающимся идентификации физическим лицом» понимается лицо, которое можно прямо или косвенно идентифицировать, в частности, посредством ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении, онлайновый идентификатор, либо на один или несколько факторов, специфичных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица.

Если обратиться к Закону Республики Казахстан «О персональных данных и их защите», то в нем под персональными данными понимаются сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе.

Исходя из проведенной аналогии, следует отметить, что ряд признаков, зафиксированных в GDPR, казахстанский законодатель не счел необходимым включить в определение понятия персональных данных.

Сходство в двух рассматриваемых правовых актах наблюдается по следующим позициям:

- Относительно сбора минимально необходимых данных:

GDPR (5 статья) устанавливает принцип минимизации данных, по которому собираемые данные должны быть ограничены лишь необходимой для конкретных целей обработки.

Закон РК (7 статья, п.8) закрепляет аналогичный принцип, подразумевающий сбор и обработку только тех персональных данных, которые необходимы для достижения заявленных целей.

- Относительно прозрачности процесса сбора:

GDPR (5 статья) требует, чтобы обработка персональных данных осуществлялась на основе открытости и прозрачности, необходимости предоставления соответствующим субъектам сведений о целях, правовом основании и других аспектах обработки затрагивающей их информации.

Закон РК (7 статья) фиксирует, что субъекты данных должны быть информированы об обработке их персональных данных, а цели обработки должны быть определены заранее и легко доступны.

- Относительно согласия субъекта данных:

GDPR (5 статья) требует получение четкого согласия от субъекта данных на обработку его личной информации, если нет иного законного основания для этой обработки.

Закон РК (8 статья) закрепляет необходимость согласия субъекта на обработку его персональных данных, за исключением случаев, предусмотренных законом.

- Относительно определения сроков хранения:

GDPR (5 статья) закладывает принцип ограничения сроков хранения данных, указывая, что данные должны храниться лишь столько, сколько необходимо для достижения целей обработки.

Закон РК (7 статья, п.8; статья 24, п.1) аналогично предусматривает определение сроков хранения персональных данных в зависимости от целей их обработки.

2. Пробельность, связанная с защитой персональных данных в ЕС и РК.

Рассматривая и анализируя два указанных выше основных акта, можно определить следующее:

2.1. Особенности отсутствия норм, регулирующих сроки хранения

Как в GDPR, так и в казахстанском законе утверждаются лишь общие принципы, требующие хранения персональных данных в

течение определенного периода, необходимого для целей обработки данных. Полагаем, что подобная пробельность влечет негативные последствия.

Проиллюстрируем проблемы, связанные со сроками хранения данных на материалах дела "Google против Испании". В 2014 году гражданин Испании Марио Костеха Гонсалес обратился с запросом к компании Google об удалении информации о его финансовых трудностях. Конфликт, возникший вокруг этого случая, связан с несовершенством правовых механизмов обеспечения безопасности обработки персональных данных в Интернете. В судебном решении по данному делу было подчеркнуто, что граждане ЕС имеют право требовать удаления своих персональных данных из поисковых систем, если эти данные устарели или перестали быть актуальными. Важно отметить, что указанное дело "Google против Испании" (Google spain sl, Google inc. v. agencia espanola de proteccion de datos, Mario Costeja Gonzalez) отразило необходимость особого внимания к соблюдению сроков хранения, предусмотренных в GDPR. Вынесенное решение было в пользу Марио Костеха Гонсалеса и благодаря ему признано право граждан требовать удаления устаревших или неактуальных персональных данных из поисковых систем. Также возник судебный прецендент, согласно которому поисковые сервисы, такие как Google, были обязаны соблюдать установленные сроки хранения данных, тем самым подчеркивалась важность соблюдения GDPR в отношении обработки и хранения персональных данных [4].

Аспекты данной проблемы также достаточно определенно проявились в деле «Гохран против Соединенного Королевства» (Gaughran v. The United Kingdom). Заявитель был задержан за вождение в нетрезвом виде в Северной Ирландии. В этот день у властей были взяты его биометрические данные, включая отпечатки пальцев и образец ДНК. Заявитель потребовал уничтожения или возврата своих данных, что было отклонено. Высший суд Северной Ирландии и Верховный суд Великобритании признали «вмешательство в права заявителя», однако посчитали это оправданным и соразмерным, поскольку вождение автомобиля в алкогольном состоянии является серьезным правонарушением. В своем решении ЕСПЧ отметил, что долгосрочное хранение биометрических данных после задержания было несоразмерным и нарушало стандарты, установленные в Конвенции о защите прав человека и основных свобод [5]. Решение отразило важность соблюдения принципов демократии, обеспечения контроля и возможности обжалования решений при сборе и хранении подобных данных. Оно ориентирует на необходимость соблюдения баланса между интересами государства и правами частных лиц. Решение ЕСПЧ послужило важным прецедентом по укреплению прав граждан в сфере сбора, сроков хранения и использования биометрических данных в контексте ситуаций, касающихся пределов сроков хранения данных.

Заметим, в современных условиях вопрос о сроках хранения данных становится особенно актуальной в связи с развитием Big Data и автоматизированной обработкой информации. Как справедливо отмечается в юридической литературе, в современных реалиях цифровой эпохи традиционные механизмы защиты персональных данных уже не могут в полной мере обеспечивать безопасность хранения информации. При этом принципы GDPR хотя и создают основу для защиты персональных данных, но не всегда отвечают требованию надлежащего хранения информации. В условиях растущего объема данных и их трансграничного перемещения усиливается значимость не только четкого определения сроков хранения персональных данных, но и эффективного механизма контроля за их соблюдением [6].

Можно констатировать, что в правовом регулировании защиты персональных данных (и в требованиях GDPR, и в законодательстве Республики Казахстан) наблюдается отсутствие установления четких временных рамок для хранения информации. Однако при этом следует отметить, что на практике в условиях реализации положений GDPR играет значимую роль прецедентная (адаптационная) практика, компенсирующая подобную неопределенность. Тогда как казахстанская система работает иначе, и фактор неопределенности в правовом регулировании затрудняет и ухудшает правоприменительную практику, создавая возможность произвольных трактовок при определении оптимальных периодов хранения данных. Подобный пробел создает широкую дискрецию в толковании соответствующих положений. Отсутствие должного регулирования сроков хранения персональных данных, на наш взгляд, на практике создает условия для ненадлежащей охраны персональных данных и их неправомерного уничтожения.

Итак, в случае с Европейским союзом неопределенность в установлении сроков хранения персональных данных является не столь критичной проблемой, по сравнению с Казахстаном, поскольку там развита прецедентная практика, которая может устранить неоднозначность толкования норм законодательства, снизив потенциальные негативные последствия.

2.2. Опыт государств-членов ЕС в отношении сроков хранения персональных данных

Государства-члены Европейского союза имеют возможность адаптировать Регламент GDPR под свое национальное законодательство. Германия, к примеру, обязана следовать GDPR, но также она вправе адаптировать те или иные его положения к национальному законодательству. В германском законодательстве сроки хранения данных подразделены на категории с учетом специфики конкретной сферы. Так, банковские и бухгалтерские документы могут храниться до 10 лет, деловые письма до 6 лет, медицинские записи от 10 до 30 лет, трудовые документы – после окончания рабочих отношений до 6 лет [7]. Возможность адаптировать регламент GDPR под свои потребности свидетельствует о гибкости в подходах к стандартам и важности их адаптации с учетом особенностей национального законодательства. Подобный подход подразумевает необходимость соответствия местным условиям, правовой культуре и правовой идентичности. В отличии от государств-членов ЕС, отсутствие конкретных норм в казахстанском законе по срокам хранения персональных данных создает ситуацию неопределенности для соответствующих организаций и влечет высокую долю субъективизма и разночтений.

2.3. Проблематика эффективности политики конфиденциальности

Политика конфиденциальности неразрывно связана с аспектами сбора, обработки и сроков хранения персональных данных и определяет обязательства, которые организации, носители информации и операторы должны соблюдать при работе с персональными данными. Она нацелена на то, чтобы защитить право граждан на конфиденциальность путем установления строгих требований по предотвращению неправомерного использования персональных данных. Политика конфиденциальности подразумевает честное, законное и безопасное обращение с личной информацией, гарантию того, что персональные данные будут использоваться в соответствии с законом и уважением к праву на защиту частной жизни каждого человека.

Следует присоединиться к мнению Элены Гил Гонсалес и Пола де Херт, согласно которому отсутствие четкости в правовом регулировании обработки и профилирования персональных данных повышает правовые риски. Субъекты персональных данных не всегда могут контролировать, каким образом информация используется в дальнейшем. Авторы подчеркивают, что принципы прозрачности и справедливости, закрепленные в GDPR, могут компенсировать возникающие неопределенности, особенно в случаях автоматизированного принятия решений. GDPR требует от компаний внедрения механизмов справедливости и подотчетности, чтобы минимизировать риски дискриминации, необоснованного профилирования и недостаточной информированности пользователей о целях обработки данных. Такой подход становится особенно актуальным в условиях стремительного роста автоматизированного анализа данных и технологий искусственного интеллекта [8].

Пробелы в регулировании и отсутствие четких стандартов создает среду, где злоумышленники могут использовать персональные данные в мошеннических целях, включая фишинг, кибератаки. Так, интернет-ресурсы могут хранить на устройствах пользователей невидимые файлы, называемые «cookie», которые отслеживают активность в сети. Эти файлы позволяют владельцам сайтов собирать и анализировать информацию о пользователях, что может нарушать их право на конфиденциальность частной жизни [9]. В литературе описывается механизм работы cookies с указанием их преимуществ (например, ускорение загрузки страниц), а также их недостатки, связанные с неконтролируемым сбором данных и рисками киберугроз. Автоматизированные алгоритмы, встроенные в маркетинговые платформы и социальные сети могут анализировать поведение пользователей, составляя их цифровые профили без согласия. Согласно статье 4 GDPR, нарушение безопасности персональных данных определяется как «событие, приводящее к случайному или незаконному уничтожению, потере, изменению, несанкционированному разглашению или доступу к передаваемым, хранимым или обрабатываемым персональным данным». Исследователи предлагают рекомендации по защите персональных данных

в интернете, включая использование VPN, отказ от хранения паролей в браузерах, применение анонимных поисковых систем и ограничение работы cookie-файлов. Эти аспекты особенно важны в условиях возрастающего цифрового отслеживания, когда пользователи часто не осознают масштаб сбора касающейся их информации [10].

2.4 Резонансные дела, связанные с нарушением персональных данных

Проиллюстрируем важность рассматриваемой проблематики в ракурсе реальных практических ситуаций. Одно из громких дел связано было с деятельностью Управления комиссара по информации Соединенного Королевства (ICO) в отношении компании «British Airways». Данный кейс произошел в сентябре 2018 года и был связан с перенаправлением трафика пользователей с сайта «British Airways» на ложный сайт, через который мошенники собирали данные клиентов, получив в результате доступ к личной информации примерно 500 000 клиентов, включая информацию о платежных картах, бронировании путешествий, имя и адрес проживания. Компания была оштрафована на 204 600 000 евро за нарушение статьи 32 GDPR о безопасности обработки персональных данных [11].

Казахстанское информационное пространство также время от времени сотрясают новости об утечке персональных данных граждан. Так, в феврале 2020 году произошла утечка информации из баз Генпрокуратуры РК. О том, что данные, которые находятся в базе указанного государственного органа, стали доступны для пользователей Сети, сообщили специалисты Центра анализа и расследования кибератак (ЦАРКА). Согласно их сообщению, «утечка охватывает данные всех граждан Казахстана и иностранцев, по которым когда-либо проводилось административное делопроизводство. Система в настоящее время передает в Интернет разнообразную информацию, включая штрафы, предупреждения, адреса проживания, фотографии нарушителей, номера автомобилей, данные из техпаспортов, информацию о владельцах имущества и многое другое. Особенно беспокойным является то, что доступ к системе позволяет не только получать данные, но и редактировать их, удалять или создавать фиктивные дела» [12].

Другой резонансный случай связан с функционированием приложения «Damumed», разработанного для удобства медицинского обслуживания населения. ЦАРКА получил анонимное сообщение, в котором утверждалось, что конфиденциальная информация «сотен тысяч пациентов» из сети клиник стала публично доступной. Вскоре была официально подтверждена информация о передаче данных третьим лицам. Аналитики ЦАРКА считают, что утечка произошла из-за элементарной ошибки – несанкционированного доступа к медицинским документам организации [13].

Стоит отметить, что Закон РК «О персональных данных и их защите» не содержит требования о необходимости уведомления государственных органов или клиентов о произошедшей утечке данных, за исключением случаев, когда утечка касается персональных данных ограниченного доступа или является критичной для общественных объектов информационно-коммуникационной инфраструктуры. Полагаем, подобное требование надо предусмотреть в указанном законе.

2.5 Особенности защиты персональных данных в положениях Регламента GDPR с позиции подходов к данной сфере в Казахстане

Регламент GDPR более эффективен в вопросе установления конфиденциальности данных по сравнению с Законом РК «О защите персональных данных». В тексте Закона РК, к примеру, отсутствует понятие «чувствительные данные», которое широко используется в европейском законодательстве. «Чувствительные данные» включают информацию, обработка которой может представлять повышенные риски для прав и свобод человека. К таким данным европейский законодатель относит сведения о расовой или этнической принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, сексуальной ориентации, генетические и биометрические данные. GDPR устанавливает сравнительно более высокие стандарты в обеспечении защиты рассматриваемого права граждан, требуя от организаций подтверждения, принимаемых ими мер безопасности. Такой подход способствует повышению кибербезопасности, снижению рисков и защите конфиденциальности личной информации. GDPR предусматривает высокие штрафы за нарушения, что стимулирует компании активнее улучшать принимаемые ими меры безопасности.

Полагаем, в Казахстане необходимо ужесточить систему санкций за нарушение и невыполнение требований законодательства

о персональных данных, поскольку ужесточение законодательства может стать серьезным стимулом для компаний и самого населения к соблюдению требований по защите персональных данных. В противном случае конфиденциальность и права человека на частную жизнь могут быть нарушены при обработке, сборе и хранении информации по вине персонала компании и самой компании, а значит, привести к серьезным инцидентам в вопросах информационной безопасности, что может повлечь непоправимый ущерб и многочисленные риски как для компании, так и для человека. Также Казахстану необходимо перенять опыт Европейского союза в информировании граждан о кибербезопасности. Сотрудничество государственных органов и общества в повышении осведомленности граждан о цифровых правах и защите персональных данных будет способствовать улучшению общей безопасности информационных ресурсов.

Необходимо отметить, важно использовать не только правовые, но и компьютерно-технические способы защиты информации. Использование технических методов, таких как «кибертуман», для защиты конфиденциальной информации является эффективным подходом. Суть «кибертумана» заключается в разбивке секретной информации на фрагменты, которые затем распределяются по различным серверам и устройствам конечных пользователей. Этот подход повышает уровень безопасности, поскольку даже в случае взлома одной части данных злоумышленнику не удается получить доступ ко всей информации. Подобный метод снижает риски преступных действий, усложняя доступ к конфиденциальной информации [14].

Следует во внимание принимать вопрос о рисках, связанных со стремительным использованием технологий искусственного интеллекта. Казахстан и другие страны нуждаются в четких международных стандартах разработки и использования технологий ИИ, в которых бы устанавливались «красная линия» для вторжения в частную жизнь отдельного человека, снижались бы риски доступа к персональным данным, в том числе биометрическим.

Заключение

В контексте обеих юрисдикций, а именно Республики Казахстан и Европейского Союза, можно выделить позитивные правовые инициативы, направленные на обеспечение безопасного сбора, обработки и хранения персональных данных. В процессе сравнительного анализа законодательных актов были выявлены схожие положения, различия и некоторые недостатки. Оба правовых документа подчеркивают важность ограничения периода хранения данных, получения согласия субъектов на их обработку, а также информирования субъектов о целях обработки, что соответствует принципу минимизации данных.

Тем не менее, выявлены определенные недостатки, такие как нечеткость и неопределенность сроков хранения персональных данных, отсутствие четких «норм» сроков хранения данных и неэффективность политики конфиденциальности, включая низкий уровень санкций за нарушение. Важно также отметить, что отсутствие ежегодных отчетов от Министерства цифрового развития и аэрокосмической промышленности (МЦРИАП) мешает предоставлению ясной картины ситуации в стране по утечкам персональных данных. Такая неопределенность может затруднить управление проблемами и угрозами в исследуемой сфере.

Релевантное ведение и хранение персональных данных требует эффективного правового регулирования. В этом контексте опыт Европейского союза весьма полезен с точки зрения установления строгих требований к обеспечению защиты персональных данных, предотвращению неконтролируемого их сбора и хранения. Пробельность в этой сфере может привести к злоупотреблениям со стороны соответствующих субъектов и росту кибер-мошенничества. Неопределенные сроки хранения данных могут стать причиной их утечки. Следует также отметить, что на данный момент законодательство РК не устанавливает обязанность уведомления государственных органов и граждан о случаях утечек данных, за исключением ситуаций, когда утечка касается персональных данных с ограниченным доступом или представляет серьезную угрозу для общественных объектов.

Опыт ЕС учит, что необходимо обеспечивать разумный баланс между безопасностью и прозрачностью в сфере обработки персональных данных. Казахстану необходимо ужесточить санкции за нарушение и невыполнение требований законодательства о персональных данных, поскольку подобная мера может стать серьезным стимулом для компаний и населения для соблюдения требований по защите персональных данных.

В завершение отметим, что существенную роль в обеспечении конфиденциальности персональной информации, а значит и кибербезопасности, играет правовая грамотность граждан. Изучение опыта Европейского союза в информировании граждан по вопросам информационной гигиены представляется особенно значимым. Осведомленные граждане менее подвержены угрозам в ракурсе сохранения персональных данных. В этом ракурсе эффективное взаимодействие государственных органов и гражданского общества в области повышения цифровой грамотности, знаний о способах защиты персональных данных является важным фактором усиления правовой защищенности казахстанцев.

Вклад авторов

Авторами статьи проведена совместная работа по исследованию перспектив имплементации GDPR в законодательство Казахстана.

Толеубек А.А. осуществила детальный анализ нормативно-правовой базы, изучила судебную практику, провела сравнительное исследование законодательства ЕС и РК, а также сформулировала ключевые выводы и рекомендации.

Аубакирова И.У., как научный руководитель, обеспечила экспертное сопровождение исследования, направляя его в соответствии с научными стандартами, участвовала в формировании аналитической базы и редактировании итогового текста. Оба автора внесли равнозначный вклад в разработку структуры статьи, анализ правоприменительной практики и подготовку выводов, что обеспечило всестороннее исследование заявленной темы.

ЛИТЕРАТУРА

1. Кужукеева Г. Право на частную жизнь и право на свободу выражения: проблемы соотношения / Портал Право и СМИ Центральной Азии. – [Электронный ресурс]. – Режим доступа: https://medialaw.asia/node/431 (дата обращения: 11.02.2025).

2. Конституция Республики Казахстан: научно-практический комментарий / рук. ред. кол.: И. И. Рогов. – Астана, 2018.

3. Аубакирова И.У., Молдабеков Б.С. Конституционно-правовые аспекты внедрения технологии искусственного интеллекта в правовую систему // Правовое обеспечение социальной справедливости и государственный суверенитет / Материалы Международной научно-практической конференции / отв. ред. Т. А. Сошникова. - М.: Изд-во МосГУ, 2024.

4. Court of Justice of the European Union. Judgment of the Grand Chamber of 13 May 2014 in Case C-131/12 "Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González". – [Electronic resource]. – Access mode: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131 (date of reference: 01.01.2025).

5. European Court of Human Rights. Case of Gaughran v. The United Kingdom, Application No. 45245/15, Judgment of 13 February 2020. - [Electronic resource]. – Access mode: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-200817%22]} (date of reference: 01.01.2025).

6. Оганесян Т.Д. Право на защиту персональных данных: исторический аспект и современная концептуализация в эпоху Big Data // Журнал зарубежного законодательства и сравнительного правоведения. – 2020. – №. 2. – С. 48-63.

7. Overview of the retention periods of business records // Hermann Schwelling Maschinenbau (HSM). - [Electronic resource]. – Access mode: http://surl.li/pgarc (date of reference: 28.12.2024).

8. Gil González E., De Hert P. Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles // Era Forum. – Berlin/Heidelberg: Springer Berlin Heidelberg, 2019. – V. 19. – №. 4. – P. 597-621.

9. Tsesis A. The right to erasure: Privacy, data brokers, and the indefinite retention of data //Wake Forest L. Rev. – 2014. – V. 49. – P. 433-484.

10. Ткаченко А.Л., Сафронов Е.С., Кузнецова В.И. Анализ эффективности защиты персональных данных и проблема cookie файлов // Дневник науки. – 2021. – №. 6(54). – С. 57-65.

11. Великобритания оштрафует British Airways из-за утечки данных клиентов // Ведомости. 2019. 8 июля. – [Электронный ресурс]. – Режим доступа: https://www.vedomosti.ru/business/news/2019/07/08/806042-velikobritaniya-mozhet (дата обращения 28.12.2024).

12. Обнаружена утечка данных из базы Генпрокуратуры РК // Казахстанское интер-

нет-издание Zakon.kz. – 2020. – 14 февраля. – [Электронный ресурс]. – Режим доступа: https://www.zakon.kz/tekhno/5007366-obnaruzhena-utechka-dannyh-iz-bazy.html (дата обращения 25.12.2024).

13. Утечка данных тысяч пациентов произошла в Казахстане // TengriNews. – 2019. – 9 июля. – [Электронный ресурс]. – Режим доступа: https://tengrinews.kz/kazakhstan_news/utechka-dannyih-tyisyach-patsientov-proizoshla-v-kazahstane-373363/ (дата обращения 25.12.2024).

14. Бегларян М.Е., Мамакаев Х.В. Кибератаки и законодательство РФ // Право и практика. – 2017. – №. 2. – С. 46-50.

REFERENCES

1. Kuzhukeeva G. Pravo na chastnuju zhizn' i pravo na svobodu vyrazhenija: problemy sootnoshenija / Portal Pravo i SMI Central'noj Azii. – [Jelektronnyj resurs]. – Rezhim dostupa: https://medialaw.asia/node/431 (data obrashhenija: 11.02.2025).

2. Konstitucija Respubliki Kazahstan: nauchno-prakticheskij kommentarij / ruk. red. kol.: I. I. Rogov. – Astana, 2018.

3. Aubakirova I.U., Moldabekov B.S. Konstitucionno-pravovye aspekty vnedrenija tehnologii iskusstvennogo intellekta v pravovuju sistemu // Pravovoe obespechenie social'noj spravedlivosti i gosudarstvennyj suverenitet / Materialy Mezhdunarodnoj nauchno-prakticheskoj konferencii / otv. red. T. A. Soshnikova. - M.: Izd-vo MosGU, 2024.

4. Court of Justice of the European Union. Judgment of the Grand Chamber of 13 May 2014 in Case C-131/12 "Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González". – [Electronic resource]. – Access mode: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131 (date of reference: 01.01.2025).

5. European Court of Human Rights. Case of Gaughran v. The United Kingdom, Application No. 45245/15, Judgment of 13 February 2020. - [Electronic resource]. – Access mode: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-200817%22]} (date of reference: 01.01.2025).

6. Oganesjan T.D. Pravo na zashhitu personal'nyh dannyh: istoricheskij aspekt i sovremennaja konceptualizacija v jepohu Big Data // Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedenija. – 2020. – №. 2. – S. 48-63.

7. Overview of the retention periods of business records // Hermann Schwelling Maschinenbau (HSM). - [Electronic resource]. – Access mode: http://surl.li/pgarc (date of reference: 28.12.2024).

8. Gil González E., De Hert P. Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles // Era Forum. – Berlin/Heidelberg: Springer Berlin Heidelberg, 2019. – V. 19. – №. 4. – P. 597-621.

9. Tsesis A. The right to erasure: Privacy, data brokers, and the indefinite retention of data //Wake Forest L. Rev. – 2014. – V. 49. – P. 433-484.

10. Tkachenko A.L., Safronov E.S., Kuznecova V.I. Analiz jeffektivnosti zashhity personal'nyh dannyh i problema cookie fajlov // Dnevnik nauki. – 2021. – №. 6(54). – S. 57-65.

11. Velikobritanija oshtrafuet British Airways iz-za utechki dannyh klientov // Vedomosti. 2019. 8 ijulja. – [Jelektronnyj resurs]. – Rezhim dostupa: https://www.vedomosti.ru/business/news/2019/07/08/806042-velikobritaniya-mozhet (data obrashhenija 28.12.2024).

12. Obnaruzhena utechka dannyh iz bazy Genprokuratury RK // Kazahstanskoe internet-izdanie Zakon.kz. – 2020. – 14 fevralja. – [Jelektronnyj resurs]. – Rezhim dostupa: https://www.zakon.kz/tekhno/5007366-obnaruzhena-utechka-dannyh-iz-bazy.html (data obrashhenija 25.12.2024).

13. Utechka dannyh tysjach pacientov proizoshla v Kazahstane // TengriNews. – 2019. – 9 ijulja. – [Jelektronnyj resurs]. – Rezhim dostupa: https://tengrinews.kz/kazakhstan_news/utechka-dannyih-tyisyach-patsientov-proizoshla-v-kazahstane-373363/ (data obrashhenija 25.12.2024).

14. Beglarjan M.E., Mamakaev H.V. Kiberataki i zakonodatel'stvo RF // Pravo i praktika. – 2017. – №. 2. – S. 46-50.