

Казахский Национальный Университет им.аль-Фараби

УДК 342.7(574)(043)

На правах рукописи

АХМЕТОВА САУЛЕ БЕЙСЕНБАЕВНА

**Государственно-правовая защита персональных данных
в Республике Казахстан**

8D04203 – Юриспруденция

Диссертация на соискание степени
доктора философии PhD

Научные консультанты:
Ибраева А.С.
Д.ю.н., профессор,
Юридический факультет,
КазНУ им.аль-Фараби

Thomas Hoffmann,
Д.ю.н., профессор,
Юридический факультет,
Таллинский Технологический
Университет

Республика Казахстан
Алматы, 2026

СОДЕРЖАНИЕ

	ВВЕДЕНИЕ	8
1	ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКАЯ ОСНОВА ПОНИМАНИЯ ПРАВА НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ	20
1.1	Общая характеристика правовых исследований относительно частной жизни и персональных данных	20
1.2	Понятие права на неприкосновенность частной жизни и защиту персональных данных	26
1.3	Функции права на неприкосновенность частной жизни и защиту персональных данных	41
2	ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РЕСПУБЛИКЕ КАЗАХСТАН И ЗАРУБЕЖОМ	49
2.1	Понятие и виды персональных данных в Республике Казахстан и зарубежом	49
2.2	Правовое регулирование операций с персональными данными в Республике Казахстан и зарубежом	63
2.3	Специальные принципы законодательства о персональных данных в Республике Казахстан и зарубежом	81
3	ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЗАРУБЕЖНЫХ СТРАНАХ И РЕСПУБЛИКЕ КАЗАХСТАН	92
3.1	Государственное регулирование защиты персональных данных в зарубежных странах	92
3.2	Государственное регулирование защиты персональных данных в Республике Казахстан	101
3.3	Пути совершенствования государственно-правового регулирования защиты персональных данных в Республике Казахстан	111
	ЗАКЛЮЧЕНИЕ	119
	СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.	127
	ПРИЛОЖЕНИЕ А	143

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей диссертации использованы ссылки на следующие стандарты:

1 ГОСТ 7.32-2001. Отчет о научно-исследовательской работе. Структура и правила оформления.

2 ГОСТ 7.1-2003. Библиографическая запись. Библиографическое описание. Общие требования и правила составления.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АППК РК	Кодекс Республики Казахстан от 29 июня 2020 года № 350-VI «Административный процедурно-процессуальный кодекс Республики Казахстан»
ГК РК	Гражданский Кодекс РК
Директива 2016/680	Директива (ЕС) 2016/680 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, выявления или преследования уголовных преступлений или исполнения уголовных наказаний, а также о свободном перемещении таких данных и об отмене Рамочного решения Совета 2008/977/ЈНА
Директива 95/46/ЕС	Директива 95/46/ЕС Европейского парламента и Совета от 24 октября 1995 г. о защите лиц при обработке персональных данных и о свободном перемещении таких данных
Европейская Конвенция (или Конвенция)	Европейская конвенция о защите прав человека и основных свобод, совершена 4 ноября 1950г.
Единые требования	Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденные Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832
ЕС	Европейский союз
ЕСПЧ	Европейский суд по правам человека (European Court on Human Rights)
Закон «О доступе к информации»	Закон Республики Казахстан от 16 ноября 2015 года № 401-V «О доступе к информации»
Закон «О масс-медиа»	Закон Республики Казахстан от 19 июня 2024 года № 93-VIII «О масс-медиа»

Закон «О персональных данных»	Закон РК от 21 мая 2013 года № 94-V «О персональных данных и их защите»
Закон «Об информатизации»	Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»
Закон «Об онлайн-рекламе»	Закон РК от 10 июля 2023 года № 18-VIII «Об онлайн-платформах и онлайн-рекламе»
ИИ	Искусственный интеллект
ИИН	Индивидуальный идентификационный номер
ИКТ	Информационно-коммуникационные технологии
Инспекция	Инспекция по защите данных Эстонии (Andmekaitse Inspektsioon)
КИБ	Комитет информационной безопасности МИИЦР РК
КоАП	Кодекс РК об Административных Правонарушениях
Конвенция 108	Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера, принятая в Страсбурге 28 января 1981 года
Конвенция 108+	Модернизированная конвенция о защите лиц при обработке персональных данных (Конвенция 108+), принятая Комитетом министров на его 128-й сессии, Эльсинор, 18 мая 2018 г.
МЦРИАП РК	Министерство цифрового развития и аэрокосмической промышленности Республики Казахстан
МИИЦР РК	Министерство искусственного интеллекта и цифрового развития Республики Казахстан
ООН	Организация объединенных наций
ОСИ	Объединение собственников имущества
РК	Республика Казахстан
УК РК	Уголовный Кодекс РК
ХЕСПЧ	Хартия Европейского союза по правам человека, (The

Charter of Fundamental Rights of the European Union), провозглашена 7 декабря 2000 года и вступившая в силу согласно Лиссабонскому договору 1 декабря 2009 года.

ФИО	фамилия, имя, отчество
AI Act	Регламент (ЕС) 2024/1689 Европейского парламента и Совета от 13 июня 2024 г., устанавливающий гармонизированные правила об искусственном интеллекте и вносящий поправки в Регламенты (ЕС) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) 2018/858, (ЕС) 2018/1139 и (ЕС) 2019/2144 и Директивы 2014/90/ЕС, (ЕС) 2016/797 и (ЕС) 2020/1828 (Закон об искусственном интеллекте), OJ L, 2024/1689, 12.7.2024
A29WP	the Article 29 Working Party (Art. 29 WP), Рабочая группа по статье 29, являвшаяся независимым консультативным органом ЕС по защите данных и конфиденциальности, созданная в 1996 году на основании статьи 29 Директивы 95/46/ЕС и сменившаяся в 2018 году EDPB в соответствии с GDPR.
Digital Services Act	Регламент (ЕС) 2022/2065 Европейского парламента и Совета от 19 октября 2022 г. о едином рынке цифровых услуг и о внесении изменений в Директиву 2000/31/ЕС (Закон о цифровых услугах), (OJ) L 277/1, 27.10.2022, стр. 1–102
ECJ	European Court of Justice, Европейский Суд
EDPB	European Data Protection Board (Европейский совет по защите данных)
EDPS	European Data Protection Supervisor (Европейский инспектор по защите данных)
e-Privacy Directive	Директива 2002/58/ЕС Европейского парламента и Совета от 12 июля 2002 г. об обработке персональных данных и защите конфиденциальности в секторе электронных коммуникаций (Директива о конфиденциальности и электронных коммуникациях)
GDPR или Европейский	General Data Protection Regulation, Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки

Регламент	персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46/ЕС (Общий регламент о защите данных)
IT	information technology (информационные технологии)

ВВЕДЕНИЕ

Общая характеристика диссертационной работы:

Первая глава посвящена теоретико-методологическим основам права на неприкосновенность личности, защиту частной жизни и персональных данных. Понятие и сущность явления частной жизни и персональных данных рассматривается в контексте исторического развития общества, его устройства, экономического и политического развития. Подчеркивается влияние социально-экономического развития, технологического прогресса и глобализации на вопросы понимания права на защиту персональных данных. В главе также приводится анализ и сравнение казахстанского и международного подхода к содержанию права на неприкосновенность частной жизни и защиту персональных данных, функциям права на неприкосновенность частной жизни в казахстанском и европейском законодательстве. Проведенный теоретический анализ содержания и функций права на неприкосновенность частной жизни формирует фундаментальное понимание права на защиту персональных данных в тесной взаимосвязи с функциями права на неприкосновенность частной жизни – свободой и самоопределением личности, автономией, установлением границ, контролем за доступом и невмешательством в частную жизнь.

Вторая глава посвящена правовым основам защиты персональных данных – основной терминологии, использованию персональных данных и принципам правового регулирования. В главе приводится анализ и сравнение казахстанского и европейского подхода к понятию «персональные данные», его интерпретации в казахстанском и европейском законодательстве. Отталкиваясь от понятия «персональные данные» во второй главе исследуются виды операций с персональными данными, их содержание, а также субъектный состав правоотношения. Кроме того, глава анализирует нормативное закрепление специальных принципов законодательства о персональных данных в Казахстане и Европе, их содержание, виды и роль в правовом регулировании. Выявляются проблемы восприятия концептуальных основ права на неприкосновенность частной жизни в государстве и в обществе, а также связанные с ним проблемы закрепления в законодательстве понятия персональные данные, субъекты регулирования, операции с персональными данными, их классификация, содержание и виды специальных принципов, а также правоприменительные проблемы.

Третья глава определяет архитектуру государственной защиты персональных данных, а также проводит комплексное исследование нормативно-правового и институционального ландшафта Казахстана и европейских стран. Проводится сравнительный анализ положений европейского и отечественного правового регулирования, определяющих деятельность системы государственных

органов, трех ветвей власти, осуществляющих защиту персональных данных, их роль и функции. Особое внимание уделяется казахстанскому уполномоченному органу по защите персональных данных в сравнении с европейским надзорным органом, вопросам его формирования, составу, функциям и полномочиям. На основе анализа выявляются существенные различия и недостатки в организации и устройстве государственного обеспечения защиты персональных данных в Казахстане. Глава демонстрирует сопутствующие актуальные проблемы в государственно-правовом регулировании защиты персональных данных в Казахстане вследствие отсутствия ясной базовой терминологии, специальных принципов защиты персональных данных, расширенных обязанностей собственников и операторов баз данных и уполномоченного органа в отношении физических лиц.

Диссертация дополняется Приложением А, где излагаются рекомендации по изменению нормативно-правовой базы, совершенствованию государственного органа в области защиты персональных данных, повышению правовой грамотности среди населения, организаций и государственных служащих в целях эффективной защиты персональных данных и неприкосновенности частной жизни.

Диссертация в целом является систематизированным базовым исследованием текущего состояния государственного-правового регулирования защиты персональных данных в Казахстане. Исследование раскрывает содержание права на уважение частной жизни и защиту персональных данных, права субъектов персональных данных, вопросы обработки персональных данных, функции надзорного органа и иных органов государства по обеспечению защиты персональных данных.

Актуальность темы исследования: Конституция Республики Казахстан закрепила в качестве высшей ценности человека, его жизнь, права и свободы. [1, 2]. Статья 18 Конституции РК защищает право на неприкосновенность частной жизни, личную и семейную тайну, защиту чести и достоинства [1]. Новая Конституция РК, принятая на референдуме 15 марта 2026 года, расширила охрану основных прав человека, особенно закрепив неприкосновенность чести и достоинства (статья 20) и неприкосновенность частной жизни, личной и семейной тайны, защиту персональных данных от их незаконного сбора, обработки, хранения и использования, в том числе с применением цифровых технологий (статья 21) [2]. Тем самым Конституция РК, принятая на референдуме 15 марта 2026 года, вывела защиту персональных данных на конституционный уровень, подчеркнув актуальность и своевременность законодательного регулирования.

В выступлениях Главы государства подчеркивается идея о первичности прав человека, необходимости защиты его прав и свобод как первоочередной задачи государства и всех государственных органов: «Нашим стратегическим приоритетом остается обеспечение безопасности граждан – фундаментальной

ценности для каждого человека и общества в целом»; «широкое проникновение цифровых технологий в повседневную жизнь людей сопровождается ростом количества разного рода мошенничеств. Поэтому в современных реалиях знание основ экономики и финансов, обладание элементарными цифровыми навыками становится особенно важным» [3].

Принята и успешно реализуется Концепция «Закон и Порядок». Сегодня «требуется интеграция традиционных ценностей справедливости и порядка в современную правовую культуру, чтобы закон воспринимался как естественная часть общественной жизни» [4].

С течением времени понимание, восприятие и регулирование права на защиту персональных данных (или конфиденциальности) приобретает все большую актуальность. В последнее время, широкое использование компьютеров и электронных средств коммуникации еще более остро ставит вопрос о защите персональных данных. Цифровизация позволила собирать, обрабатывать, искать и хранить персональные данные в масштабах, беспрецедентных для аналоговой эры. В современных условиях тревогу вызывают стремительно развивающиеся информационные технологии, а использование технологий искусственного интеллекта несет еще большие риски и угрозы для прав и свобод человека.

Для решения новых угроз, рисков и проблем в связи с защитой персональных данных важнейшая роль отводится праву как средству социального управления, инструменту осуществления функций государства по обеспечению конституционного права на неприкосновенность частной жизни, в частности защиты персональных данных. Текущая правоприменительная практика показывает, что законодательство в рассматриваемой сфере надлежащим образом не регулирует весь комплекс проблем обеспечения защиты персональных данных отдельного гражданина. Законы и подзаконные акты, принятые в целях защиты персональных данных, еще требуют доработки в соответствии с международными стандартами. Общество не осознает значимость и важность права на неприкосновенность частной жизни именно в части защиты персональных данных, не осознает последствия необдуманного предоставления и распространения личной информации. Существующие нормы в сфере защиты персональных данных не сформулированы четко и ясно, и как следствие, недостаточно эффективны. Более того, слабая информированность, правовая и цифровая грамотность как общества, так и государственных служащих, отражаются на реализации существующих законодательных требований о защите персональных данных. В особенности, существенную роль в сфере защиты персональных данных, в становлении правоприменительной практики и обеспечении защиты могут сыграть реформирование законодательства и отдельный уполномоченный (надзорный) орган исполнительной ветви власти.

Таким образом, диссертация анализирует комплекс имеющихся фундаментальных проблем в области защиты персональных данных, выявляет недостатки в законодательстве и государственном регулировании, предлагает

рекомендации по их совершенствованию с целью заложить прочный фундамент для правоприменения в любой сфере, связанной со сбором и обработкой персональных данных. Исследование вносит вклад в теоретическую и практическую сферы юриспруденции, рассматривая фундаментальные теоретические и правоприменительные пробелы в области регулирования и защиты персональных данных, которая обрела высокую востребованность в современный период.

Степень разработанности темы исследования: Тема исследования актуальна и постоянно изучается в международном и национальном академическом сообществе. Среди зарубежных ученых в области персональных данных широко известны американские ученые Дэниел Солове (Daniel Solove), Хелен Ниссенбаум (Helen Nissenbaum), и Присцилла Риган (Priscilla Regan), европейские авторы Надежда Пуртова (Nadezhda Purtova), Пол Ван Де Херт (Paul Van De Hert), Берт-Яап Коопс (Bert-Jaap Koops), австралийский правовед Грэм Гринлиф (Graham Greenleaf), и многие другие.

В зарубежной правовой литературе закладывается институциональный фундамент неприкосновенности частной жизни и демонстрируется развитие понимания частной жизни от личных пространственных границ до современных личных границ в эпоху доминирования цифровизации и развития искусственного интеллекта. Фундаментальные труды американских ученых Сэмюэла Уоррена и Луиса Брандейса (Samuel Warren and Louis Brandeis), Алана Вестина (Alan Westin) заложили теоретическую основу для права на неприкосновенность частной жизни, его содержания и функций как отдельного права человека защититься от любого постороннего вмешательства [5, 6]. Сара Эго (Sarah Ego) проследила трансформацию неприкосновенности частной жизни из деликтного института в конституционную гарантию [7].

Современные европейские исследователи, в частности Б.-Я. Коопс, развивают концепцию нормативно-закрепленной конституционной защиты неприкосновенности частной жизни, обосновывая выделение защиты персональных данных в самостоятельное право, отличное от классической неприкосновенности частной жизни [8, 9]. Особое внимание Б.-Я. Коопс уделяет развитию информационных технологий.

Вызовы цифровой экономики и алгоритмизации общества также исследуются в работах Кариссы Велис (Carissa Véliz) [10], Д. Солове [11, 12, 13, 14, 15, 16, 17] и Фредерика Боргесиуса (Frederic Borgesius) [18, 19, 20, 21]. В трудах указанных авторов раскрываются проблемы сбора и обработки персональных данных, трансграничной передачи, автоматизированной обработки и технологий искусственного интеллекта, которые создают новые риски дискриминации, профилирования и злоупотребления техниками идентификации. В работах Н. Пуртовой [22, 23] и Алессандро Мантелеро (Alessandro Mantelero) [24, 25] анализируются проблемы идентификации личности и влияние искусственного интеллекта на фундаментальные права.

Заключительным вектором современных исследований является глобализация правовых стандартов. А. Мантелеро [26] и Г. Гринлиф [27, 28, 29] констатируют глобальное стремление государств к гармонизации национальных законодательств на основе европейской модели защиты данных.

Таким образом, современная зарубежная юридическая наука движется в сторону междисциплинарного анализа, объединяющего экономические и технические аспекты обработки информации, вызовы ИИ и международную унификацию правовых режимов, обеспечивая баланс между технологическим прогрессом и основными правами и свободами человека. Вместе с тем зарубежные авторы, принимая за аксиому широкую интерпретацию концепции персональных данных, в исследованиях фокусируются на какой-либо конкретной проблеме, но не исследуют вопросы нормативного закрепления и прямого действия специальных принципов. Вопросы правового регулирования использования персональных данных остаются открытыми, требующими совершенствования государственной защиты в особенности в современных условиях алгоритмической экономики и государственного управления.

В казахстанской юридической науке вопросы защиты персональных данных получили развитие после принятия профильного Закона «О персональных данных» в 2013 году, однако современные исследования носят преимущественно фрагментарный и узкоотраслевой характер [30]. Труды таких ученых, как Э.Омурчиева, Ф.Сырлыбаева и З.Гельманова [31, 32, 33], ограничиваются областью трудовых отношений, в то время как работы А.Амирова, Д.Мухамеджановой и Д.Утеген фокусируются на биометрической идентификации и несовершенстве ее нормативного регулирования [34, 35, 36, 37]. Исследование М.Токмади сосредоточено на понимании категории «приватность» и «частная жизнь» в контексте национальной безопасности, но не затрагивает концептуальные основы, принципы сбора и обработки данных, вопросы полномочий государственных органов [38]. Ж.Искакова, А.Амиров, О.Лозовая, Б.Максутов, И.Аубакирова, А.Толеубек касаются понятия персональных данных, но фрагментировано, в контексте прикладных проблем использования персональных данных [39, 34, 40, 41, 42].

Анализ работ казахстанских правоведов приводит к выводу, что в отечественной науке сохраняется дефицит системного анализа фундаментальных основ, а также специальных принципов обработки данных и правового статуса уполномоченного органа. Прежде всего это касается целого ряда понятий, которые непосредственно связаны с личной информацией, сбором, различными видами использования и обработки персональных данных. Кроме того, теоретиками не исследовались специальные принципы защиты персональных данных - необходимый законодательно закрепленная руководящая идея и императив прямого действия. Также среди ученых ограниченно исследовалась деятельность уполномоченного государственного органа по защите персональных

данных, не рассматривалась его компетенция, в особенности его консультативные функции в комплексе других полномочий.

Критическим барьером для отечественной доктрины остается хронологический и технологический разрыв. Подавляющее большинство публикаций последних лет (2015–2022) не учитывают существенные реформы в международном и национальном законодательстве. Этот пробел в тщательном теоретическом исследовании, особенно в отношении таких основополагающих вопросов, как неэффективность законодательных принципов и проблемы, создаваемые системами искусственного интеллекта, обуславливает необходимость переосмысления казахстанской правовой модели.

Цель и задачи исследования:

Целью исследования является изучение правовых основ обеспечения защиты персональных данных в РК, нормативного закрепления основных понятий, специальных принципов защиты персональных данных, изучение регулирования и деятельности государственных органов по защите персональных данных в Казахстане и Европе, разработка рекомендаций по совершенствованию законодательства и государственного регулирования в области защиты персональных данных.

В рамках исследования были поставлены следующие задачи:

- Определить содержание права на неприкосновенность личности, уважение частной жизни, место персональных данных в закрепленном Конституцией РК праве на неприкосновенность личности;
- Обосновать авторское понятие и классификацию персональных данных, сравнить их нормативное закрепление в казахстанском и европейском законодательстве;
- Систематизировать принципы защиты персональных данных, оценить нормативное закрепление, роль и реализацию принципов в казахстанском и европейском законодательстве;
- Обобщить практику использования персональных данных, регулирование сбора, обработки и защиты персональных данных в казахстанском и европейском законодательстве;
- Анализировать права субъекта персональных данных и корреспондирующие обязанности контролёров, обработчиков персональных данных и третьих лиц, сравнить казахстанское и европейское регулирование;
- Оценить деятельность государственных органов РК по обеспечению права на защиту персональных данных, сравнить полномочия и деятельность казахстанского и европейских надзорных органов по защите персональных данных, выработать рекомендации для правовой практики;
- Систематизировать существующие проблемы и препятствия в области защиты персональных данных и выработать рекомендации для их решения с учетом зарубежного опыта.

Объектом исследования являются общественные отношения, возникающие в сфере защиты персональных данных и деятельность государства по обеспечению защиты персональных данных в контексте конституционного права на неприкосновенность личности и уважение частной жизни в современный период.

Предметом исследования являются правовые нормы, регулирующие защиту персональных данных, основные понятия и операции с персональными данными, а также основные направления деятельности государства по обеспечению защиты персональных данных в РК и компетенция уполномоченного органа по защите персональных данных в сравнении с европейским законодательством и опытом.

Научная новизна диссертационного исследования заключается в том, что в отличие от проведенных исследований оно является комплексным исследованием положений в области защиты персональных данных в стране, основных терминов, операций с персональными данными и специальных принципов защиты персональных данных. Данные положения являются фундаментальными для всего государственно-правового регулирования. Вопросы использования персональных данных не изучены в казахстанской науке в контексте теории государства и права, сущности и содержания основного права на неприкосновенность частной жизни.

В частности, казахстанская правовая наука не содержит комплексных работ, рассматривающих теоретические вопросы права человека на неприкосновенность личности, уважение частной жизни и защиту персональных данных в современных, новых условиях жизни общества и развития информационно-коммуникационных технологий. Наблюдается теоретический пробел, в казахстанской правовой науке отсутствуют актуальные теоретические исследования, где в комплексе и фундаментально раскрывается теоретическое содержание защиты персональных данных.

В новых условиях социально-экономического развития и форсирования государством цифровизации и использования информационных технологий, в том числе технологий искусственного интеллекта, данное исследование обозначает проблему упущения государством теоретических основ и содержания права на неприкосновенность личности и защиту персональных данных. Отметим принятие новых законов, касающихся регулирования применения искусственного интеллекта и регулирования цифровых отношений. Это Закон РК «Об искусственном интеллекте», а также Цифровой кодекс РК [43, 44]. В современных условиях цифровой экономики неприкосновенность личности и личная информация приобрела другое «измерение», обновленные условия существования, и соответственно требует более бережного, тщательного и внимательного регулирования и защиты. Масштаб и значение современного вторжения в частную жизнь и использования личной информации в цифровой экономике беспрецедентны. Только банки второго уровня имеют столько

информации, как ни один государственный орган и правительство не могут себе позволить. В этом направлении, Казахстану рекомендуется учесть европейский опыт регулирования защиты персональных данных.

Имеющийся пробел в правовой теории не заложен как правовой фундамент, не прослеживается, не раскрывается и не сформулирован в законодательных актах так, чтобы иметь эффективное действие, правоприменение и защиту персональных данных. Законодателем не учтены такие фундаментальные теоретические положения права на неприкосновенность личности как автономия, контроль, установление личных границ, пределы вторжения. Принципы специального права не имеют сильной формулировки и эффективного действия, не служат «путеводителем» и руководством для интерпретации, применения и устранения пробелов или конфликтов нормативного регулирования и правоприменения.

Проведенное исследование комплексно анализирует казахстанское законодательство, в особенности законодательно закрепленную терминологию, специальные принципы права на защиту персональных данных, полномочия и функции государственных органов, реализацию государством механизмов защиты персональных данных. При этом, в диссертации рассматривается «эволюция» национального законодательства, достоинства и недостатки в нормативном и государственном регулировании защиты персональных данных с учетом изменений и дополнений в казахстанское законодательство.

Исследование затрагивает анализ деятельности государственных органов, их роли и полномочий в реализации права человека на уважение частной жизни и защиту персональных данных. Особое внимание в исследовании уделяется уполномоченному органу по защите персональных данных, вопросам его формирования и компетенции. Развитие казахстанского государственно-правового регулирования противопоставляется европейскому регламентированию защиты персональных данных, функциям государственных органов. Диссертация демонстрирует анализ GDPR, e-Privacy Directive, вопросы формирования, полномочия и акты европейского уполномоченного органа (European Data Protection Board), рассматривает прецедентное право European Court of Justice, European Court on Human Rights [45, 46]. Изучение нормативной базы европейского союза и функций уполномоченного органа дает возможность определить позитивную европейскую практику с целью ее рецепции и гармонизации казахстанского законодательства с европейским и международным законодательством в области защиты персональных данных.

По результатам исследования сформулированы комплексные предложения по улучшению законодательства в области защиты персональных данных.

Методологическая основа диссертационного исследования состоит из совокупности общих и специальных методов познания: диалектического, исторического, анализа и синтеза, сравнительно-правового, системного, структурно-функционального, статистического, логико-формального и др.

Сочетание нескольких методов позволяет изучить и рассмотреть различные стороны предмета исследования, достичь цели исследования.

В исследовании использовался исторический метод, позволяющий проследить историческое развитие общества и законодательства в отношении понимания права на неприкосновенность личности и уважение к частной жизни, а также защиту персональных данных. Анализ исторического аспекта социально-экономического развития с учетом информационно-коммуникационных технологий и искусственного интеллекта влияет на оценку и понимание содержания явления частная жизнь и персональные данные и способствует корректному нормативному закреплению, правоприменению и реализации права на защиту персональных данных.

В основе диссертации заложен нормативно-правовой метод исследования, заключающийся в изучении нормативно-правовых актов и правовых институтов, регулирующих право на неприкосновенность личности и защиту персональных данных. Данный подход позволяет выявить недостатки в действующем законодательстве, закрепляющем право на уважение частной жизни и защиту персональных данных, суть и содержание базовых и фундаментальных норм Конституции и специального нормативного акта, их реализацию в отраслевых правовых актах, в том числе через формирование государственных институтов и регуляторных органов. Нормативный подход позволяет проследить согласованность различных нормативных актов, выявить несоответствия, пробелы и конфликтующие положения, разработать предложения по совершенствованию законодательной базы.

Кроме того, в исследовании активно применялся сравнительно-правовой метод, анализировались и сопоставлялись нормы национального и европейского законодательства о защите персональных данных, о роли и функциях уполномоченных государственных органов. Сравнительно-правовой анализ позволил продемонстрировать степень защищенности казахстанского населения в обеспечении права на уважение частной жизни и защиту персональных данных в сопоставлении с населением Европейского Союза. Данный подход к исследованию дает возможность изучить успешный зарубежный опыт и выработать предложения по его внедрению в национальную практику по защите персональных данных.

Исследование включало использование эмпирических методов, состоящих из анализа практики рассмотрения административно-правовых дел и применения административных санкций, судебной практики, изучение статистических данных и экспертных выводов, обращения и запросы физических лиц на платформе Открытого диалога eGov, письма государственных органов по обращениям граждан о разъяснении законодательства о персональных данных, ежегодные отчеты уполномоченного РК по правам человека. Применение эмпирических методов позволило выявить проблемы среди населения и оценить уровень защищенности персональных данных в Казахстане.

Основные положения, выносимые на защиту:

1. Выявленная неопределенность понятия «персональные данные» требует унификации законодательства с учетом взаимозависимости личной информации и частной жизни. В Закон РК «О персональных данных и их защите» предложено определить конкретные критерии идентификации данных и их типологию в зависимости от степени «ценности», «существенности» конкретного элемента или идентификатора персональной информации, его взаимосвязи с социально-экономическими правами и рисками ущерба для прав и свобод личности.

2. Предлагается внести в Закон РК «О персональных данных и их защите» дополнения, касающиеся основных терминов о регулировании использования персональных данных, при этом конкретизировать виды операций с персональными данными. Сделан вывод о том, что операция «профилирование» может быть признана самостоятельным видом обработки данных, при этом полагаем необходимым усилить правовое регулирование таргетированной рекламы и коммуникаций как высокоинтрузивной практики.

3. В государственно-правовом регулировании защиты персональных данных необходимо учесть особую значимость специальных принципов защиты персональных данных, ориентированных на европейскую модель, GDPR. При этом предлагается придать этим принципам статус универсальных регуляторов для устранения пробелов и обеспечения единообразного правоприменения.

4. Предлагается расширить и конкретизировать права субъектов персональных данных с установлением корреспондирующих обязанностей всех участников их обработки. Предложено закрепить обязанности по информированию, разъяснению целей и последствий обработки, а также обеспечению доступных механизмов защиты прав, включая конфиденциальность по замыслу и умолчанию.

5. Необходимо институциональное реформирование уполномоченного органа по защите персональных данных с приданием ему статуса самостоятельного института. При этом рекомендуется усилить его компетенции, координационную роль и определить механизмы взаимодействия с государственными органами для повышения эффективности контроля и защиты прав субъектов данных.

Диссертационное исследование обладает как теоретической, так и практической значимостью в области права на неприкосновенность частной жизни и защиту персональных данных.

Теоретическая значимость исследования состоит в восполнении теоретических пробелов в казахстанской науке, способствует ее развитию и содержит комплексный фундаментальный анализ сущности права на неприкосновенность частной жизни, расширяет и детализирует это основное право человека и право на защиту персональных данных в современных условиях развития информационно-коммуникационных технологий и технологий

искусственного интеллекта. Состояние конфиденциальности, автономии, свободы человека и контроля своей частной жизни в современном цифровом пространстве требуют правового теоретического обоснования.

Обнаруженный исследованием теоретический пробел неразрывно связан с законодательным пробелом регулирования защиты персональных данных и его исполнением на практике. Отсутствие понятных и подробных терминов, классификации персональных данных и видов обработки персональных данных ведут к несогласованной и непоследовательной правоприменительной практике, разнящимся мнениям центральных исполнительных органов, отсутствию ясности о правоприменении среди граждан и коммерческих организаций. Данная проблема осложняется отсутствием правильно сформулированных специальных принципов законодательства о защите персональных данных, которые могли бы иметь прямое действие, способствовать правоприменению, указывать направление для исполнения закона при наличии пробелов законодательства. Эффективная интеграция профильного законодательства, обеспечение реальной безопасности персональных данных и успешная реализация индивидом своих прав во многом зависят от деятельности специализированного государственного органа. Обладая консультативными полномочиями, наделенное функциями издавать четкие методические рекомендации, деятельность данного ведомства будет способствовать формированию единых стандартов правоприменения. Недавно проведенные реформы в законодательство о защите персональных данных в отношении уполномоченного органа не решают суть проблем на практике.

Практическая значимость исследования заключается в том, что проведенный сравнительный нормативный и правоприменительный анализ национального и европейского регулирования позволил выработать предложения для совершенствования национального законодательства, функций государственных органов и устранения выявленных пробелов казахстанской правоприменительной практики с целью повышения эффективности защиты персональных данных. Кроме того, результаты исследования позволяют модернизировать правовые дисциплины в подготовке юридических кадров, разработать отдельный учебный курс по защите персональных данных. Данный курс может преподаваться также и для повышения уровня осведомленности граждан о праве на неприкосновенность частной жизни и на защиту персональных данных, улучшить правовую, цифровую грамотность как среди сотрудников коммерческих организаций, так и среди государственных служащих.

Апробация результатов исследования.

Результаты диссертационного исследования в области регулирования защиты персональных данных были опробованы автором в виде выступлений и публикаций в научных конференциях, семинарах и круглых столах, посвященных вопросам правового регулирования доступа к информации. Одним из значимых результатов исследования служат предложения, озвученные в качестве эксперта

на первых парламентских слушаниях по законопроекту «Об искусственном интеллекте», проведенных в КазНУ им.аль-Фараби в сентябре 2025 года. Поскольку технологии искусственного интеллекта связаны с автоматической обработкой персональных данных, было рекомендовано переоценить принципы регулирования искусственного интеллекта, закрепив приоритетность защиты и соблюдения основных прав и свобод человека над инновациями [47]. Ключевые идеи и выводы работы отражены в пяти научных статьях, включая публикации в изданиях, рекомендованных Комитетом по обеспечению качества в сфере образования и науки Министерства науки и высшего образования Республики Казахстан.

В рамках диссертационного исследования опубликовано 12 научных работ, в том числе следующие научные статьи:

1. Принципы защиты персональных данных: сравнительный анализ национального и зарубежного законодательства // Вестник КазНУ. Серия Юридическая. 2023. – 106(2) – С. 33-46. DOI: <https://doi.org/10.26577/JAPJ.2023.v106.i2.04>.

2. The European Data Protection Model as a Global Privacy Standard // *Farabi Journal of Social Sciences*. 2023. – 9(1) – С. 79-85. DOI: <https://doi.org/10.26577/FJSS.2023.v9.i1.09>.

3. Powers of the Personal Data Protection Authority in Europe and Kazakhstan: comparative analysis, recommendations for improving the activities of the Kazakhstani Personal Data Protection Authority // Вестник Евразийского национального университета имени Л.Н. Гумилева Серия Право. – 2024. - №3(148) – С. 198-211. DOI: <https://doi.org/10.32523/2616-6844-2024-148-3-201-214>

4. Modern development of artificial intelligence technologies and problems of legal regulation of profiling and targeted advertising in Kazakhstan // Вестник Евразийского национального университета имени Л.Н. Гумилева Серия Право. – 2025. - №1(150) – С. 77–97. DOI: <https://doi.org/10.32523/2616-6844-2025-150-1-77-97>.

5. Legal regulation of profiling and targeted advertising in Kazakhstan through the lens of European experience. // *Social and Legal Studios*. – 2025. – 8(1). – P. 33-45. DOI: <https://doi.org/10.32518/sals1.2025.33>.

Структура и объем диссертации. Структура диссертации составлена согласно целям и задачам исследования, а также с учетом логики и последовательности изложения материала. Работа состоит из введения, трех глав, включающих девять параграфов, заключения, списка использованных источников и приложения А.

В структуре диссертации последовательно отражено решение научных задач, позволяющих полноценно исследовать теоретические и практические вопросы права на защиту персональных данных. Общий объем работы включает 184 страницы текста, сопровождающихся иллюстративными материалами, а также обширным списком нормативных и научных источников.

1 ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКАЯ ОСНОВА ПОНИМАНИЯ ПРАВА НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1 Общая характеристика правовых исследований относительно частной жизни и персональных данных

В конце XIX века американские авторы Сэмюэл Уоррен и Луис Брандейс (Samuel Warren and Louis Brandeis), исследуя способность закона защитить личность от вмешательства, рассуждали о «праве на уединенность» или «праве быть оставленным в покое» (right to be let alone) [5]. В своей работе они отметили, что с учетом политических, социальных и экономических изменений в обществе происходит признание новых прав. С.Уоррен и Л.Брандейс проследили возникновение и развитие правовой защиты мыслей, эмоций и чувств личности в нормах семейного права, права собственности и интеллектуальной собственности. Технологическое развитие того времени, изобретения фотоаппарата и методы ведения бизнеса, в особенности развитие газетной индустрии, сподвигло авторов на исследование, в результате которого С.Уоррен и Л.Брандейс заложили основу понимания права на неприкосновенность личности, выделив частную жизнь (приватность) как отдельное право, подлежащее законодательной защите. Уоррен и Брандейс обозначили, что личности принадлежит право определять границы информационной неприкосновенности личности – размышлений, идей, настроения, чувств, эмоций [5, стр.198]. Тем самым авторы намечают контуры будущих исследований информационной приватности и свойств права на неприкосновенность частной жизни, автономию и самоопределение личности, установление пределов и невмешательство.

С 60-х годов прошлого столетия зарубежными авторами поднимались проблемы в контексте нарушений приватности уже со стороны государства в результате использования технических средств аудио и видео фиксации в области разведывательной и правоохранительной деятельности, выделив таким образом информационную составляющую частной жизни.

Пятилетнее исследование американского профессора Алана Вестина (Alan Westin) «Конфиденциальность и свобода» о влиянии современных технологий на неприкосновенность частной жизни стало фундаментальной работой для западных правоведов [6]. Обобщая работу А.Вестина, можно сделать вывод, что человек *сам* определяет, что именно входит в его частную жизнь, какую информацию и для кого он может сделать доступной, включая органы власти. При этом содержание конфиденциальности определяется самим человеком в зависимости от того, как он воспринимает себя в социуме, от типа самого социума, установленных в нем норм и правил, уровня общественного развития,

политической системы государства. В своей работе А.Вестин также исследует и развивает теорию о неприкосновенности частной жизни, выделяя 4 функции – личную автономию, эмоциональное освобождение, самооценку, ограниченную и защищенную коммуникацию. Углубленное исследование функций частной жизни в своих работах отразили американские ученые Рут Гэвисон и Х.Ниссенбаум [48, 49].

Сара Эго (Sarah Ego) иллюстрирует как, согласно решениям американских судов, право на неприкосновенность частной жизни в США трансформировалось из деликтного права в конституционное право [7]. Методы вторжения в частную жизнь со стороны правительственных и коммерческих организаций и собранная ими личная информация имели дискриминационное влияние на трудоустройство, получение социального обеспечения, страхования, кредитов, доступа к медицинскому лечению. Сара Эго утверждает, что в современном высокотехнологичном мире частная жизнь и персональные данные подвергаются переосмыслению и реконструкции, и остается вопрос, будут ли частная жизнь и персональные данные законодательно защищаться таким образом, чтобы их сбор и обработка любыми организациями обеспечивала конфиденциальность и уважение к частной жизни, баланс национальной безопасности и гражданских свобод.

С развитием компьютерных технологий правоведы заявляли о проблемах вторжения в частную жизнь и использования личной информации уже в экономической сфере коммерческими организациями, а не только государственными органами. Европейский автор Карисса Велис (Carissa Véliz) рассматривает «экономику слежки» (*surveillance economy*), экономику данных, как корпорации используют личную информацию и нарушают частную жизнь, риски, которые возникают для личности и ценностей общества [10].

Особый интерес и научную ценность представляют публикации современного американского ученого в сфере права о частной жизни (конфиденциальности) профессора Дэниела Солове. Его исследования посвящены проблемам понимания приватности, таксономии проблем конфиденциальности и ее ущербу, базам данных и власти, которую они создают, роли согласия в операциях по сбору и обработке персональных данных, трансграничной передачи данных, а последние работы рассматривают также проблемы искусственного интеллекта в вопросах приватности [11, 12, 13, 14, 15, 16, 17].

Европейские авторы также исследуют вопросы частной жизни, концепции персональных данных, во взаимосвязи с функциями права на неприкосновенность частной жизни. В отличие от американской эволюции права на неприкосновенность частной жизни из деликтного права в конституционное, ученые Европы опираются на нормативно-закрепленную конституционную защиту права на частную жизнь и защиту персональных данных. Исследование конституций нескольких стран голландскими правоведом под руководством

профессора Берт-Яап Коопса посвящено конституционной формулировке права на неприкосновенность частной жизни или «правом на уважение личной сферы жизни», включающей защиту персональных данных и персональной информации [8]. Исследование подтолкнуло Берт-Яап Коопса к выводу, что право на защиту персональных данных может рассматриваться как самостоятельное право, поскольку охраняется Хартией Европейского союза по правам человека (ХЕСПЧ), содержащую отдельную статью 8 о защите персональных данных помимо статьи о неприкосновенности частной жизни [8, стр.537]. Его другие исследования рассматривали вопрос частной жизни в связи с развитием технологий, рассуждая о границах частной жизни, которые в современном мире размываются интернет-технологиями, делая менее полезным вопрос, где происходит вторжение в приватность [9]. Берт-Яап Коопс считает, что в современных условиях датафикации информации о человеке и его деятельности регуляторы должны найти и сформулировать инновационные, нефизические концепции архитектуры правовых границ частной жизни.

Исследования голландского профессора Надежды Пуртовой посвящены вопросам защиты персональных данных и функциям права на неприкосновенность частной жизни. Она рассматривает широкую интерпретацию понятия персональные данные, относимость данных к конкретному лицу и его идентифицируемость на основе данных и роли субъектов, использующих данные [22]. Она также отдельно исследует вопрос использования персональных данных и идентификации личности, техник ре-идентификации [23].

Дискуссии по вопросам злоупотребления техниками идентификации пользователей и профилирования, использования таргетированной рекламы и микротаргетинга, автоматизированной обработки и технологий искусственного интеллекта получили развитие как следствие постоянного развития информационных технологий. Например, исследования голландского ученого, Фредерика Боргесиуса (Frederic Borgesius), рассматривают вопросы сбора и использования персональных данных в сфере законодательства о защите прав потребителей, дискриминационных последствий электронной торговли и услуг, идентификации личности для коммерческих целей и поведенческого таргетинга [18, 19, 20, 21].

Последние исследования итальянского ученого А.Мантелеро (Alessandro Mantelero) в области защиты персональных данных касаются рисков автоматической обработки персональных данных, использования технологий искусственного интеллекта. А.Мантелеро обращает внимание на последствия, которые возникают для фундаментальных прав человека в алгоритмическом обществе. Он предлагает изменить подход к нормативному регулированию оценки рисков воздействия на права человека, дополнив оценку воздействия на права человека более широким охватом, указав на необходимость оценивать воздействие на этические и общественные ценности [24]. А.Мантелеро отдельно затрагивает вопрос об оценке влияния технологий искусственного интеллекта на

права человека, поскольку устройства и программы, оснащенные данными технологиями, все более персонализируются и используются в коммерческом и публичном секторе [25].

В другом исследовании А.Мантелеро дает оценку европейскому законодательству о защите персональных данных, отмечая гармонизацию международного регулирования защиты персональных данных с европейским подходом [26]. Австралийский ученый Грэм Гринлиф также исследует европейский подход в сравнении с нормативным регулированием других стран, вопросы глобализации и гармонизации законодательства о персональных данных в международном аспекте, стремление государств практически всех континентов к рецепции европейского регулирования [27, 28, 29].

Таким образом, исследования зарубежных ученых составляют основу юридической науки в области неприкосновенности частной жизни и защиты персональных данных. Иностранные научные публикации касаются разнообразного круга вопросов в сфере неприкосновенности частной жизни и защиты персональных данных, вместе с тем они фокусируются на какой-либо конкретной проблеме. При этом для зарубежных авторов широкая интерпретация концепции персональных данных является постулатом, а право на неприкосновенность частной жизни и функции данного права исследуются в тесной взаимосвязи с вопросами сбора и обработки персональных данных.

Глобализация социально-экономических и многих государственных процессов, их цифровизация, развитие информационных технологий и связанные с ними проблемы регулирования наблюдаются и в Казахстане. С появлением в стране Закона РК от 21 мая 2013 года «О персональных данных и их защите» казахстанские правоведы также исследуют различные вопросы в сфере защиты персональных данных. Однако, среди материалов в казахстанской науке не были выявлены работы, рассматривающие фундаментальные вопросы защиты персональных данных, в частности термины и понятия, специальные принципы, особенности операций по обработке, систему и полномочия органов по защите персональных данных. Кроме того, выявленные публикации в области защиты персональных данных большей частью совершены в период с 2015 по 2022 год, с истечением которого и казахстанское, и европейское законодательство претерпело серьезные изменения и приняло новые законы, например GDPR, Digital Services Act и AI Act в Европе, Закон РК «Об онлайн-платформах и онлайн-рекламе» в Казахстане [45, 50, 51, 52]. Следует отметить, что в последние годы и само общество претерпело значительные изменения, а стремительно развивающиеся и применяемые технологии искусственного интеллекта по сбору и обработке персональных данных требуют дополнительных исследований и совершенствования правового регулирования.

Вместе с тем более поздние казахстанские публикации за пятилетний период в полной мере не рассматривают фундаментальные компоненты защиты

персональных данных, понятия, принципы, полномочия государственного органа по защите персональных данных. Подавляющее большинство научных работ имеет узкую направленность. Например, Э.Омурчиева, Ф.Сырлыбаева, З.Гельманова исследуют вопрос защиты персональных данных в контексте трудовых отношений [31, 32, 33]. В своей публикации Э.Омурчиева проводит анализ сведений, относящихся к персональным данным работника в рамках осуществления трудовых функций, а также рассматривает проблемы сбора и обработки персональных данных работодателем. Автор указывает на общую проблему отечественного правового регулирования в области защиты персональных данных, отмечая, что понятие «персональные данные» не обеспечивает правовую определенность и нуждается в доработке. Исследование Ф.Сырлыбаевой посвящено обязанности работодателя осуществлять защиту информационных прав работника, включая защиту персональных данных в контексте трудовых отношений. Как меру защиты, автор предлагает нормативно закрепить в Трудовом кодексе РК конкретный перечень сведений, запрещенных к сбору от работников. Работа З.Гельмановой демонстрирует вопросы сбора и обработки персональных данных работников работодателями, в том числе с использованием технологий искусственного интеллекта. Автор отмечает необходимость соблюдения этических норм и внедрения технических мер защиты, а также описывает практический пример использования программного обеспечения в организациях.

Публикации А.Амирова затрагивают понятие частной жизни и персональных данных, вопросы их государственной защиты в зарубежных странах. В отдельной работе А.Амиров посвящает исследования вопросам концепции и типологии биометрических персональных данных, несовершенству нормативного регулирования сбора, обработки биометрических персональных данных [34, 35]. В своем исследовании Ж.Исхакова также рассматривает регулирование биометрических персональных данных. Она отмечает ограниченность, неясность и неточность дефиниции биометрических персональных данных, закрепленного в казахстанском законодательстве, отсутствие конкретики в регулировании их сбора и обработки. Автор считает необходимым рецепцию комплексного регулирования в области биометрических персональных данных по примеру Европы [39]. Аналогично А.Амирову и Ж.Исхаковой правовед Д.Мухамеджанова подвергает исследованию вопрос защиты биометрических персональных данных и отмечает недостаточное и децентрализованное законодательное регулирование защиты биометрических данных в Казахстане в сравнении с европейским законодательством, акцентирует внимание на необходимости комплексного регулирования и совершенствовании законодательства о защите биометрических персональных данных [36]. Д.Утеген и Б.Рахметов демонстрируют проблемы понятия биометрических персональных данных и процессов их сбора, обработки и хранения в сравнении

с зарубежным регулированием в области биометрических данных [37]. Авторы отмечают частичное соответствие казахстанского регулирования биометрических данных международным стандартам и сдержанную рецепцию зарубежного опыта. В научных работах указанных исследователей не находят системного отражения фундаментальные причины существующих в Казахстане проблем в области защиты любых персональных данных, в частности, неэффективность закрепленных в законе специальных принципов, понятийного аппарата и институциональные проблемы деятельности уполномоченного органа по защите персональных данных.

М.Токмади рассматривает защиту персональных данных как инструмент контроля государства над населением в контексте национальной безопасности, но в то же время отмечает положительную динамику в защите персональных данных, поскольку национальный интерес в технологическом развитии страны не может оставить без внимания вопросы конфиденциальности данных [38]. В исследовании М.Токмади фокусировалась на понимании приватности, частной жизни, однако в ее исследовании не затрагивались понятийный аппарат, принципы сбора и обработки персональных данных, вопросы государственного регулирования, полномочия государственных органов.

Другие отечественные авторы проводят общий сравнительный анализ казахстанского и европейского регулирования в области защиты персональных данных. О.Лозовая отмечает ограниченные права субъекта данных, узкое понятие персональных данных и исчерпывающее определение операций по обработке персональных данных [40]. Б.Максutow приводит краткий обобщенный сравнительный анализ казахстанского Закона «О персональных данных» с Европейским регламентом, тезисно останавливаясь на избранной терминологии и правах физических лиц [41]. Однако, в работах авторов не находит отражения исследование принципов законодательства о персональных данных, как базовой конструкции всего регулирования, не исследуется функционал уполномоченного органа в области защиты персональных данных.

Правоведы И.Аубакирова и А.Толеубек вместе с понятием персональные данные исследуют проблемы казахстанского регулирования операций по хранению персональных данных, срокам хранения, неэффективность политик конфиденциальности, мягкие санкции казахстанского законодательства за утечку персональных данных. Проведенный авторами сравнительный анализ с зарубежным регулированием в области защиты персональных данных приводит их к заключению о рецепции европейского опыта [42].

Е.Ерболатов и С.Жетписов исследуют проблемы утечек персональных данных и связывают их проявление с несовершенством отечественного законодательства [53]. Л.Каирбаева рассматривает нормативное регулирование в области защиты персональных данных и вопросы автоматизированной обработки персональных данных [54].

Работы отечественных правоведов концентрируются на конкретной проблематике нормативного регулирования в области защиты персональных данных и не затрагивают теоретической основы и свойств права на неприкосновенность частной жизни, а также фундаментальных проблем закрепления специальных принципов защиты персональных данных и полномочий государственного органа по защите персональных данных.

1.2 Понятие права на неприкосновенность частной жизни и защиту персональных данных

Право на неприкосновенность частной жизни является фундаментальным правом человека, закрепленным в международных правовых документах. Право на защиту от произвольного вмешательства в личную и семейную жизнь, произвольное посягательство на тайну корреспонденции, честь и репутацию предусмотрено в статье 12 Всеобщей декларации прав человека, принятой резолюцией 217 А(III) Генеральной Ассамблеи ООН от 10 декабря 1948 года [55]. Другим важным международным документом для Казахстана является Международный пакт о гражданских и политических правах, ратифицированный Республикой Казахстан в 2005 году [56]. Статья 17 указанного Пакта защищает человека от произвольного или незаконного вмешательства в его личную и семейную жизнь, произвольного или незаконного посягательства на тайну корреспонденции, честь и репутацию. Статья 14 Международного пакта о гражданских и политических правах дополнительно уточняет, что частная жизнь защищена от вмешательства печати и публики во время любых судебных разбирательств. Всеобщая декларация прав человека и Международный пакт о гражданских и политических правах закрепляют право на защиту закона от такого вмешательства или таких посягательств.

Право на уважение частной жизни является международно-признанным, закрепленным в международных актах основным правом человека. Оно закреплено в основных законах государств, став также конституционным правом.

Конституция РК в статье 1 устанавливает, что права и свободы человека являются высшей ценностью государства. В числе прав, находящихся под протекцией статьи 18 Основного закона Казахстана, находится и право на неприкосновенность частной жизни, личной и семейной тайны, чести и достоинства лица, тайны вкладов и сбережений, тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Несмотря на перечисленные в статье 18 Конституции РК объекты неприкосновенности, все они охватываются общим понятием частная жизнь.

Право на неприкосновенность частной жизни, право на невмешательство в частную жизнь и право на уважение частной жизни являются синонимами по

правовому содержанию и неразрывны с понятием «частная жизнь». Объектом охраны данного права на неприкосновенность является частная жизнь, содержание которой широко обсуждается в науке на протяжении многих лет. Право на неприкосновенность частной жизни следует рассматривать как с позиции содержания и сущности понятия частная жизнь, так и с позиции содержания и сущности самого права на неприкосновенность.

Рассмотрим понятие «частная жизнь», которое в зарубежной литературе чаще употребляется как «прайвеси», «приватность», «конфиденциальность». В настоящей работе используются все указанные определения частной жизни.

Понятие «частная жизнь» неразрывно связано с человеком, его личностью. В развитии права на неприкосновенность частной жизни англо-американская правовая мысль, особенно конституционная мысль, ставит личность в центр внимания [57, стр.24]. Так, американские правоведы С.Уоррен и Л.Брандейс в своей фундаментальной для системы общего права статье отметили, что «основополагающим принципом для неприкосновенности частной жизни является неприкосновенность личности» [5, стр.205]. Казахстанский ученый, профессор А.С.Ибраева отмечает, что понятие «личность» «характеризует человека с социальной стороны, как осознающего себя, свое место и роль в обществе» [58, с. 171].

Понятие «личность» в гуманитарных науках рассматривается как широкое понятие с некоторой спецификой, присущей конкретной науке [59, 60, 61, 62]. К примеру, в психологии «личность» интерпретируется как «особое качество человека, приобретаемое им в социокультурной среде в процессе совместной деятельности и общения» [63, стр.235]. Понятие «личность» в социологии понимается как индивид, обладающий сознанием, социально значимыми и уникальными свойствами характера и качествами, формирующимися в процессе социализации и являющимися продуктом индивидуального опыта и социального взаимодействия, в процессе которого он создает, воспроизводит и изменяет социальную реальность [64].

Само понятие «личность» не поддается постоянной интерпретации в отношении конкретного лица, отличается многообразием проявления человека в обществе и в собственной жизни. Человек как личность и социальная категория находится в постоянной динамике, подверженной влиянию извне [65]. На формирование личности влияет абсолютно все: окружение и люди разных поколений и социальных групп, с которыми человеку приходится коммуницировать в течение своей жизни в любых ситуациях - дома, в учреждениях образования, семья и друзья, работники и работодатели, государственные служащие, сотрудники общественных организаций, организаций досуга, медицинских учреждений и так далее. Этот перечень можно продолжать, и он будет корректироваться, меняться в зависимости от эволюции и развития общества и уровня взросления, становления человека как личности. Окружающая социокультурная, политическая, экономическая среда влияет на понимание

личности, на формирование его ценностей и сознания. Человека как личность характеризует множество сторон – знания, навыки, умения, убеждения, идеалы, цели, морально-психологические качества, профессия, его роль и место в общественной жизни и прочие аспекты. Все эти аспекты относятся к личности, а следовательно, и к личной, частной жизни.

Личное или частное – это не общественное и не государственное. Это убеждение можно проследить с Древней Греции. Греческий философ Аристотель говорил о разделении между публичной сферой политических дел (которую он называл полисом) и домашней (частной) сферой человеческой жизни («ойкос» - дом, хозяйство) [66, стр.376-379]. Деятельность, подпадающая под публичную сферу, отнесена к задачам государства, которое Аристотель характеризовал как объединение «общений» (обществ), а первым видом «общения» являлась семья. Такое разделение на публичную и частную сферы стало общепринятым в научной среде. Р.Костелло (Róisín Á Costello) отмечает, что частная жизнь с древних времен воспринимается в тесной взаимосвязи с семьей и собственностью, взаимосвязи, основанной на естественном желании человека территориального и семейного контроля, наличия убежища для жизни и гостеприимства [67, стр.76]. Такое восприятие частной жизни, связанное с домом и семьей, повлияло как на континентальные традиции, так и на общее право, которое включает запреты на вход в жилища и признает права на частную жизнь супружеских пар.

Содержание понятия «частная жизнь» в научной среде эволюционирует на протяжении многих столетий в тесной взаимосвязи с человеком, индивидом. Как внешнее социальное, культурное, политическое и экономическое окружение влияет на формирование и понимание личности, так это окружение воздействует и на формирование и понимание частной, личной жизни.

Эволюцию понятия частная жизнь и влияние различных факторов на его интерпретацию можно последить в работе американского профессора Алана Вестина «Конфиденциальность и свобода», написанной им в результате пятилетнего широкого исследования конфиденциальности [6]. А.Вестин демонстрирует как человек определяет личную жизнь в зависимости от того, как он воспринимает себя в социуме, от типа самого социума, норм и правил, установленных в этом социуме, уровня общественного развития, организации политической системы государства. К примеру, некоторые африканские племена не придерживаются уединенности в моменты ведения разговоров, переодевания, купания, рождения или смерти, для них обычно иметь минимум привычной для нас одежды, общее жилище и даже спальню, где проживает несколько поколений семьи. Такой образ жизни не приемлем для цивилизованного общества, в котором бытовые, этические, моральные нормы и правила организации взаимоотношений внутри семьи, различных групп людей и организаций существуют на другом уровне.

Американский ученый в сфере права о конфиденциальности Дэниел Дж. Солове также отмечает, что «то, что является общественным и частным,

формируется культурой и историей» [11, стр.1141]. На восприятие того, что представляет собой частная жизнь влияет множество факторов, таких как «урбанизация, классовый и социальный статус, этнические и религиозные подгруппы», «размер семьи, появление новых социальных мест, трансформация характера семьи, ...новое отношение к телу, увеличение богатства и пространства, отделение дома от работы, ...и многочисленные другие изменения в качестве и характере жизни» [11, стр.1141]. На примере семейной жизни Д.Солове демонстрирует, как понимание частной семейной жизни менялось со временем, со средних веков до настоящего времени [12, стр.51].

В западной цивилизации, как и во многих других странах, брак заключался по решению родителей, основываясь на экономических и стратегических интересах. Д.Солове сравнивает семью с «деловым активом, используемым в общественной торговле, сетью связей и взаимозависимых репутаций, построенных на соответствии социальным нормам», где семейный дом демонстрирует богатство и социальный статус, используется для построения деловых отношений [12, стр.51]. Тем не менее, наличие отдельных пространств в домах, отдельных помещений для прислуги, для профессиональной деятельности служили доказательством тому, что различные сферы деятельности человека имели границы, доступные для определённого круга лиц и определённой деятельности – кабинет для работы и деловых конфиденциальных бесед, помещения для прислуги, отдельные от помещений для членов семьи.

В средние века в Казахстане в источнике права «Жеті Жарғы» также можно проследить разделение между частной семейной жизнью и общественной жизнью, в основе которой также были семейные и родственные отношения. К примеру, такое преступление как кровосмешение рассматривалось в рамках «семейства, ибо преступления сего рода не передаются на рассмотрение сторонним людям» [68, стр.319]. Другой пример сохранения семейной информации внутри семьи – отсутствие наказания женщине за недонесение о воровстве со стороны мужа или отца, «ибо на старшего в семействе непозволено доносить» [68, стр.320]. Указанные положения обычного права казахов свидетельствуют о разделении частной семейной жизни и жизни в казахском обществе. Как правило, семейные раздоры между супругами тоже решались внутри членов семьи, близких родственников.

О разделении в казахском обществе частной семейной и общественной сфер жизни свидетельствует следующее положение [68, стр.320]:

«Разбирать ссоры и произносить приговор над виновным должны, если не сам хан, то правители или старейшины тех аулов, к которым принадлежат истец и ответчик».

Указанное положение свидетельствует о том, что в рассмотрении спора участвует близкое окружение истца и ответчика и родственники, живущие с ними в одном поселении, а значит, внутренние общественные дела аула не выходили за его пределы. М.А.Сарсембаев также отмечает, что в казахском ханстве семья была

ячейкой аула, состоявшего из нескольких родственных семей, и внутрисемейные споры не были подсудны суду биев [69, стр.116]. В казахском обществе существовала не регулируемая никакими нормами права «внутриаульная юстиция» [69, стр.105].

Таким образом, обычное право казахов определяло круг внутрисемейных вопросов, которые рассматривались в определенном кругу лиц аульно-семейной общины. А значит, в средние века в казахском ханстве обычное право проводило границу между частной и общественной сферами жизни.

Как отмечают зарубежные авторы, в XVIII-XIX веках исторический акцент на семье и доме как частной сфере, где государство исключено, а мужчина имеет единоличный контроль, начал смещаться в сторону современного понимания частной жизни. С указанного периода в гражданском и общем праве появились ранние права личности, которые заложили основу для современных гарантий конфиденциальности [67, стр.76, пункт 1.07, 1.10; 12, стр.60-61]. Борьба за права и свободы личности укрепила «концепцию личности как уникальной и свободной в достижении своих собственных целей», что повлекло трансформацию понимания семьи как экономического предприятия и, соответственно, семейной частной жизни в XIX веке. В результате урбанизации и индустриализации появились промышленные предприятия и офисы, дома многих стали физически отделяться от места работы. Соответственно, появилась концепция профессиональной сферы, а дом приобрел более личное, отдельное, семейное значение и смысл. Профессиональная жизнь человека стала рассматриваться как отдельная от семейной жизни сфера частной жизни.

Далее понимание частной жизни продолжало расширяться, что особенно проявилось в XX веке. Как указывает Д.Солове, понимание частных и публичных вопросов претерпевало «метаморфозы на протяжении всей истории из-за меняющихся взглядов, институтов, условий жизни и технологий» [11, стр.1133]. Сокращение размера семьи, появление новых социальных пространств, рост благосостояния и пространства, уменьшение скученности и многочисленные другие изменения качества и характера жизни повлияли на восприятие приватности [11, стр.1141].

С конца XIX века в западных странах появились прецеденты и законы, защищающие конфиденциальность писем, запрещающие вскрывать почту, публиковать в газетах изображения лица без его согласия, а также сведения, наносящие вред репутации и достоинству человека. Р.Костелло отмечает, что указанные нормы характеризуют зарождение права на неприкосновенность частной жизни, включающем частный интерес человека в контроле над своим имиджем и способности «ухаживать за своим достоинством» [67, стр.76, пункт 1.11]. С.Уоррен и Л.Брандейс называли право на неприкосновенность личности принципом, «который может быть использован для защиты частной жизни личности от вторжения либо слишком предприимчивой прессы, фотографа, либо владельца любого другого современного устройства для записи или

воспроизведения сцен или звуков» [5, стр.206]. При этом они отметили универсальную применимость этого принципа к технологическим изменениям и указывали, что закону не нужно создавать новые принципы, чтобы распространить защиту на проявления личности, ее комментарии, действия и отношения [5, стр.213]. Говоря о проявлениях личности С.Уоррен и Л.Брандейс относили к объекту защиты размышления, идеи, настроение, чувства и эмоции человека [5, стр.198]. Таким образом, внешнее проявление личности, выражающееся в ее мыслях, словах и действиях, отношении к религии, каким-либо явлениям или другим людям, тоже составляют частную жизнь.

Обобщая изложенное, в любом обществе до XX века частная жизнь была ограничена самим человеком в понимании дома и семьи, близких друзей и всех явлений, которые человек считает близким и важным для своей личности и ее существования. В прогрессивном западном обществе частная жизнь также включала личные размышления, идеи, настроение, чувства и эмоции человека, но такое понимание частной жизни не было ярко выраженным и глубоко признанным в обществе и государстве. Ограниченное внутренним личным кругом объектов восприятие частной жизни стало расширяться позднее в XX веке с форсированными индустриальными, экономическими, социальными и политическими изменениями в мире.

В начале XX века большинство конституций не предусматривало нормативное закрепление права на неприкосновенность частной жизни, которая все еще ограничивалась рамками семьи и дома. В обществе сложилось традиционное понимание тайны частной жизни, без его нормативного оформления. Но, в большинстве стран существовали отдельные законы, устанавливающие тайну переписки, а с появлением коммуникаций - тайну телеграфных сообщений, телефонных переговоров. На конституционном уровне тайна переписки была закреплена, к примеру, в статье 114 Конституции Германской империи (Веймарская) 11 августа 1919 г., статье 128 Конституции СССР [70, 71]. При этом Веймарская Конституция не предусматривала статью о защите семейной жизни, но защищала брак как основанный на равноправии полов. Также отдельно защищалась неприкосновенность жилища и свобода личности от ограничений и лишения. Конституция СССР 1936 г. тоже не устанавливала защиту частной и семейной жизни, а лишь тайну переписки и неприкосновенность жилища, а в статье 127 защищала неприкосновенность личности в физиологическом смысле. В Германии и СССР право на уважение частной жизни подверглось ограничениям в сталинском и гитлеровском режимах. При этом в Германии ограничения осуществлялись на законодательном уровне. С приходом Гитлера к власти в Германии был издан Указ президента Рейха о защите людей и государства (*Verordnung des Reichspräsidenten zum Schutz von Volk und Staat*). Первая статья Указа признала допустимыми ограничения личной свободы, права на свободу выражения, включая свободу печати, права на ассоциации и собрания, вмешательство в тайну переписки, почтовых услуг, телеграфа и телефонных

сообщений, распоряжения о проведении обысков и арестов, а также ограничения на имущество, даже за установленными законами пределами [72].

Во второй половине XX века конфиденциальность получила широкое признание в качестве права человека и повышенное признание на конституционном уровне как часть глобальных юридических реформ, последовавших за Второй мировой войной [67, пункт 1.26]. После войны ООН была принята Всеобщая декларация прав и свобод человека и гражданина, которая на международном уровне закрепила фундаментальные права человека. В статье 12 закреплено, что никто не может подвергаться произвольному вмешательству в его частную и семейную жизнь, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств. Принятие Всеобщей декларации прав человека по окончании Второй мировой войны послужило толчком для реформирования государственных систем в европейских странах, в новых конституциях было закреплено право на уважение частной жизни, получившее статус конституционного права.

Впоследствии право на уважение личной жизни было также закреплено в статье 8 Европейской конвенции о защите прав человека и основных свобод, совершена 4 ноября 1950г., 3 сентября 1953 г., статьей 17 Международного пакта о гражданских и политических правах, совершен 16 декабря 1966 г. [73, 56]

После ратификации СССР в 1973 году Международного пакта о гражданских и политических правах человека СССР последовало принятие Конституции СССР 1977 года, а также и советских республик [74]. В советской Конституции, как и в тексте Международного пакта о гражданских и политических правах право на уважение частной жизни сформулировано как право на уважение личной жизни, что не имеет различий. Однако, А.А.Смоляков отмечает, что в советский период при переводе слова “privacy” в статье 17 Международного пакта произошла подмена понятий «личная жизнь» вместо «частная жизнь», основываясь на коммунистической идеологии, отсутствии различий между личностью и социалистическим обществом [75, стр.80]. Такого подхода «общественно-индивидуальной жизни», где личная жизнь ограничивалась бытом и отсутствовали различия между личностью и социалистическим обществом, в основном придерживались исследователи советского периода [75, стр.79; 76, стр.33]. Тем не менее, советские ученые включали в содержание охраняемой личной жизни «охрану всех сторон личной жизни, оглашение которых граждане по тем или иным причинам считают нежелательными (тайна завещаний, усыновления, врачебных диагнозов, дневниковых записей, денежных вкладов, фотографий и др.)» [75, стр.80].

Советский период «коллективистского конституционализма», в котором интересы общества были выше интересов отдельного человека, сменился периодом становления независимого Казахстана [75, стр.80]. В 1993 году была принята первая Конституция Республики Казахстан [77]. Интересно отметить, что

неприкосновенность частной жизни не относилась к какой-либо категории прав и свобод человека, ни к гражданским, ни к политическим, ни к экономическим и социальным. Статья 33 о неприкосновенности частной жизни помещена в Главе 7 «Гарантии прав и свобод» Конституции РК от 28 января 1993 года. Тем не менее, не столь важно размещение нормы в документе, сколько ее содержание. Конституция 1993 года обязывала государственные органы, общественные объединения и должностных лиц ознакомить гражданина с документами, решениями и иными материалами, затрагивающими его права и интересы. Более того, на конституционном уровне Основной закон 1993 года запрещал сбор, хранение, использование и распространение информации личного характера без согласия гражданина. По этому признаку содержание статьи 33 Конституции РК 1993 года намного шире, чем статья 18 действующей Конституции Республики Казахстан, принятой на 30 августа 1995 года [2]. Сегодня Конституция РК не устанавливает такого запрета для личной информации, а содержит привычную для международных актов защиту неприкосновенности частной жизни, личной и семейной тайны. Запрет на сбор, хранение, использование и распространение информации личного характера в Конституции 1993 года можно интерпретировать как всеобъемлющую конституционную защиту частной жизни, бесспорно включавшую персональную информацию.

Статья 18 Конституции РК от 1995 года предусматривает неприкосновенность следующих объектов частной жизни: личная и семейная тайна, тайна личных вкладов и сбережений, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. В отношении неприкосновенности частной жизни в статье 18 действующей Конституции Республики Казахстан Л.Ф.Татарина выделяет два характеризующих частную жизнь как объекта правовой охраны элемента: «во-первых, это сами реальные факты и отношения и, во-вторых, информацию об этих фактах и отношениях» [78, стр.64]. В своем анализе она рассматривает неприкосновенность частной жизни как комплексную категорию, включающую свободу личности действовать без внешнего контроля, тайну частной жизни и коммуникаций, совокупность личных неимущественных прав и неприкосновенность жилища. Л.Ф.Татарина указывает на отсутствие конкретных правовых норм, касающихся индивидуальной информации, указывая на то, что Конституция допускает широкое толкование этой защиты частной жизни [78, стр.66].

Действительно, статья 18 Конституции РК не имеет заголовка и перечисляет несколько объектов неприкосновенности, в том числе самостоятельных объектов охраны - достоинство, национальная, религиозная, политическая принадлежность, жилище, самостоятельно защищаемых статьями 17, 19 и 25 Конституции РК 1995 года. Однако, понятие частной жизни статьи 18 Конституции РК не носит исчерпывающего характера и включает в том числе физическую, психическую и духовную жизнь индивида, персональные данные, сведения о человеке, дающие оценку его характеру, облику, здоровью, материальному состоянию, семейному

положению, образу жизни, отдельным фактам биографии [79]. И этот перечень не является завершенным.

Реализация конституционной нормы обеспечивается нижестоящими законодательными актами, Гражданским Кодексом РК, Уголовным кодексом РК, Кодексом РК об административных правонарушениях [80, 81, 82].

Статья 144 ГК «Право на охрану тайны личной жизни» не дает исчерпывающего определения личной жизни, а устанавливает, что может составлять тайну личной жизни - тайна переписки, телефонных переговоров, дневников, записок, интимной жизни, тайна усыновления, рождения, адвокатская тайна, тайна медицинского работника, тайна банковских вкладов и иная охраняемая законами тайна. Составители Комментария к Гражданскому кодексу РК не раскрывают исчерпывающего содержания понятия «личная жизнь» [83].

Кодексом РК об административных правонарушениях в статье 16 закреплено, что частная жизнь, а также личная, семейная и иная охраняемая законом тайна являются неприкосновенными. В то же время статья 15 КоАП устанавливает запрет на сбор, использование и распространение сведений о частной жизни, а равно сведений личного и делового характера, которые лицо считает необходимым сохранить в тайне. Таким образом, принципы производства об административных правонарушениях, закрепленные в статьях 15 и 16 КоАП, хотя не дают четкого и исчерпывающего понятия частной жизни и сведений о ней, в то же время, указывая на общий квалифицирующий признак сведений о частной жизни – необходимость сохранить сведения в тайне. В то же время, в статье 79 КоАП предусматривает административную ответственность не за нарушение неприкосновенности частной жизни, а за нарушение законодательства о персональных данных и их защите, обращаясь к понятию персональные данные и иным положениям Закона «О персональных данных».

В отличие от КоАП, положения статьи 147 Уголовного кодекса РК устанавливают, что противоправными являются действия по незаконному сбору и распространению сведений о частной жизни лица, составляющих его личную или семейную тайну. Иными словами, согласно статье 147 УК РК частная жизнь – это то, что является личной и семейной тайной. Важно отметить, что для определения «личная тайна» нормы Уголовного Кодекса «опираются» на понятийный аппарат вышеуказанной статьи 144 Гражданского кодекса, которая не дает полной интерпретации понятия частная жизнь, поскольку она «многогранна и скрывает вещи, которые не всегда можно оформлять нормами права» [84, стр.7]. Ученые в области уголовного права указывают, что для квалификации преступления, предусмотренного статьей 147 УК РК, значение имеет то, что лицо пожелало сохранить эти сведения в секрете, независимо от их характера [85].

Такая позиция о широкой интерпретации частной жизни, охватывающей различные аспекты личности, поддерживается многими казахстанскими и зарубежными юристами. Российский автор М.А.Челмакина считает, что «частная

жизнь — это многоаспектная и емкая категория, для которой сложно сформулировать исчерпывающее определение, так как каждый человек имеет право наполнять его смыслом, сформированным исходя из собственных умозаключений» [86, стр.143]. Группа голландских авторов относит к частной жизни физические объекты как имущество, документы и компьютеры, жилые и нежилые места, которые определяются физическими границами или представляют собой менее осязаемые пространства [8, стр.541,542]. Б.-Я. Коопс и другие также включают в частную жизнь личность, телесную неприкосновенность, семейную жизнь, социальные отношения, принятие личных решений, частные действия и персональные данные.

Казахстанский юрист В.И.Олейник относит к частной жизни личную и семейную тайны, указывая на широкий спектр конфиденциальных сведений разного рода, касающихся лично человека (личная тайна) или членов его семьи и близких родственников (семейная тайна) и которые человек не желает придавать огласке [87, стр.28]. Голландские правоведы также считают семейную тайну отличным от личной тайны объектом частной жизни [8, стр.541,542]. Другой казахстанский правозащитник, Л.А.Рамазанова включает в широкое понимание частной жизни защиту персональных данных [87, стр.21]. Профессор М.Ч.Когамов отмечает, что частная жизнь многогранна и не всегда может быть оформлена нормами права [84, стр.7]. Ученые Н.Н.Турецкий и Е.М.Абайдельдинов придерживаются такой же позиции, указывая, что в юридической науке, международном праве и национальных законах суверенных стран нет полного и четкого перечня, что именно относится к частной жизни [84, стр.11,20]. Профессор Л.Т.Жанузакова также отмечает, что частная жизнь охватывает широкий круг объектов [84, стр.27].

После 2022 года научно-практический комментарий к пункту 1 статьи 18 Конституции РК был дополнен более широким толкованием понятия частная жизнь [79]. Конституционная защита частной жизни включает физическую, психическую и духовную жизнь индивида, его честь и достоинство, внутренний мир человека и его интересы, сведения о человеке, дающие оценку его характеру, облику, здоровью, материальному состоянию, семейному положению, образу жизни, отдельным фактам биографии. Личная и семейная тайны являются частью частной жизни, сферой деликатных и интимных сторон жизни индивида, оглашение которых он по тем или иным причинам считает нежелательными: тайны завещания, усыновления, врачебных диагнозов, денежного вклада и др. Иными словами, казахстанское право имеет широкий неограниченный перечень объектов частной жизни, находящихся под конституционной защитой.

Таким образом, в мировой науке к частной жизни относится все, что имеет отношение к человеку, его жизни, личности, его интересам, окружению, увлечениям, привязанностям, переписке, чести, достоинству, душе и телу. Такой подход изначально характеризовался сначала домом и семьей, обосновывался правом собственности, правом на интеллектуальную собственность, защитой

чести, достоинства и репутации. Однако с XIII–XIX веков объектный состав частной жизни расширился под влиянием борьбы за права человека и личности, общественно-политических, социальных, экономических и технологических изменений во всем мире.

В этой связи, ученые единогласны в том, что понятие частной жизни динамично развивается и не может быть определено исчерпывающим образом. Объекты частной жизни приобрели новое виртуальное измерение в современном интернет-обществе, где повседневная жизнь человека пронизана технологиями в быту, общении с друзьями и коллегами, на работе и в школе, во взаимодействии с государственными учреждениями, а также в экономической, социальной и коммерческой сферах. Р.Костелло отмечает, что в современном обществе определение частной жизни должно быть гибким, чтобы приспособливаться к новым технологиям, и в то же время достаточно конкретным, чтобы обеспечивать юридическую ясность [67, пункт 2.02]. Поскольку это напряжение затрудняет определение частной жизни, более подходящим видится описательное определение объектов и содержания частной жизни. Е.М.Абайдельдинов поддерживает эту позицию, ссылаясь на ЕСПЧ, как специальный орган по толкованию и применению Европейской конвенции о защите прав человека и основных свобод, который подходит к определению частной жизни описательно [84, стр.20,21].

Обобщая практику ЕСПЧ по рассмотрению дел о нарушении статьи 8 Европейской конвенции о защите прав человека и основных свобод, можно вывести следующее описание частной жизни и ее объектов:

Понятие «частная жизнь» является широким термином, не поддающимся исчерпывающему определению, охватывает физическую и психологическую неприкосновенность человека. Оно может охватывать множество аспектов физической и социальной идентичности человека. Понятие «частная жизнь» распространяется, в частности, на аспекты, связанные с личной идентичностью, такие как имя или фотография человека, пол и сексуальная ориентация, а также репутация [88, §87; 89, §86; 90, §102]. Частная жизнь также включает деятельность профессионального или делового характера, особенно для свободных профессий и самозанятых, так как работа может настолько переплетаться с личной жизнью, что может быть сложно четко разграничить как деятельность, связанную с профессией или бизнесом, осуществляемую из частного дома, так и не связанную с ней деятельность, осуществляемую в офисах или коммерческих помещениях [91, §§29,30]. Частная жизнь включает общение на рабочем месте, телефонные разговоры и переписку, включая электронную [92, §§72, 81, 82]. Частная жизнь не ограничивается «внутренним кругом», в котором человек может жить своей личной жизнью по своему усмотрению, включает его право жить в уединении, вдали от нежелательного внимания [92, §70]. Даже в публичном контексте существует зона взаимодействия человека с другими, которая может подпадать под сферу «частной жизни», то есть в широком смысле право на «частную жизнь»

включает также право вести «частную общественную жизнь». [93, §§129-131; 92, §70].

Базируясь на объектах частной жизни, некоторые ученые определяли различную классификацию измерений конфиденциальности. При этом первые виды частной жизни как правило связывались с физическим пространством и кругом общения, дом и семья, работа и коллектив, что определяют как пространственную конфиденциальность [11, 12, 8, 9, 67]. С признанием «права быть оставленным в покое» С.Уоррена и Л.Брандейс телесное или физиологическое измерение (сокрытие наготы, манера одеваться, прикосновения) дополнилось моральным и психологическим измерением.

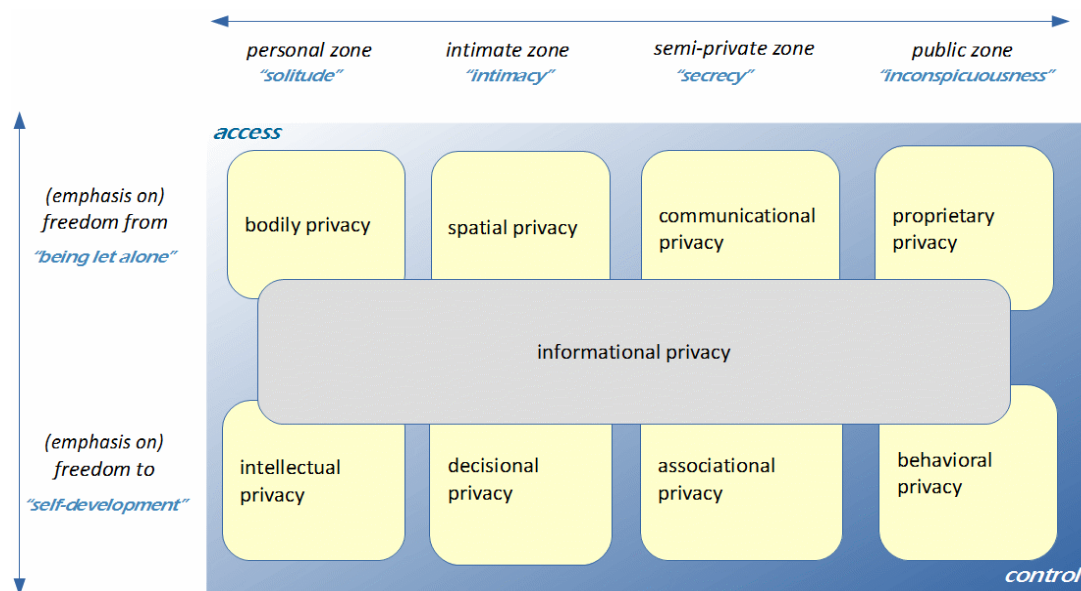
Рут Гэвисон (Ruth Gavison) подходит к изучению частной жизни с позиции потери «идеальной» конфиденциальности, которая происходит, когда другие получают информацию о личности, оказывают ей свое внимание или получают физический доступ к ней. Таким образом, она выделяет информационное, физическое и психологическое измерения частной жизни [48, стр.428].

Х.Ниссенбаум приводит три измерения частной жизни: (1) физическая конфиденциальность, характеризующаяся как «особая изоляция и уединение»; (2) информационная конфиденциальность, характеризующаяся как «конфиденциальность, секретность, защита данных и контроль над личной информацией»; и (3) собственническая (proprietary) конфиденциальность, характеризующаяся как «контроль [собственника] над именами, образами и хранилищами личной информации» [49, стр.71].

В контексте информационной конфиденциальности Д.Солове дифференцирует вмешательство в свободу принятия человеком решений, из чего выводится дополнительное измерение - конфиденциальность принятия решений [13, стр. 490,491; 11, стр.1115].

Р.Костелло также выделяет конфиденциальность принятия решений как центральный элемент личной конфиденциальности, и отмечает пространственную (физические или психологические границы) и информационную стороны частной жизни [67, пункты [2.33]-[2.38]]. Б.-Я. Коопс и его соавторы дополняют телесное и пространственное измерения частной жизни коммуникационной и имущественной (основанной на праве собственности), интеллектуальной, ассоциативной и поведенческой приватностью, а также конфиденциальностью решений [9, стр.10; 8, стр.566-568]. Б.-Я. Коопс с группой голландских ученых выделяют 8 базовых типов частной жизни, которые охватываются еще одним измерением - информационной конфиденциальностью. Они изображают типологию конфиденциальности, состоящую из 9 элементов, следующим образом [8, стр.566]:

Рисунок №1: Типология конфиденциальности по Коопсу.



Б.-Я. Коопс и соавторы называют информационное измерение конфиденциальности всеобъемлющим, поскольку каждый из 8 базовых измерений частной жизни содержит информационный элемент. Соответственно, информация о каждой стороне частной жизни для человека представляет определяемую им ценность и интерес в ограничении доступа или контроле использования информации об этом аспекте человеческой жизни [8, стр.569].

В советской научной литературе Л.О.Красавчикова выделяла интимную, семейную, организационную, оздоровительную, коммуникационную стороны частной жизни [75, стр.33].

Казахстанские авторы также отмечают информационное измерение неприкосновенности частной жизни. Л.А.Рамазанова выделяет информационную, физическую, коммуникационную и территориальную конфиденциальность [87, стр.21]. Этой позиции также придерживаются Л.Т.Жанузакова и А.А.Караев [84, стр.27]. Другие казахстанские ученые прямо не указывают на наличие информационной конфиденциальности, но тем не менее, основываясь на нормативных положениях гражданского, уголовного и административного законодательства о нарушениях в отношении частной жизни, все отмечают, что информация – это неотъемлемая сторона частной жизни, которая является объектом защиты.

Таким образом, частная жизнь является емкой и неисчерпывающей категорией, ядром которой является человек и его личность, а объектом частной жизни – все, что связано с личностью - знания, навыки, умения, убеждения, идеалы, цели, морально-психологические качества, профессия, роль и место в общественной жизни и прочие аспекты жизни человека в любом обществе – семье, школе, университете, рабочем коллективе, и другом объединении людей, основанных на их общем занятии или интересе. Частная жизнь имеет физическое (осязаемое), пространственное, имущественное, поведенческое,

коммуникационное, реляционное (отношенческое или ассоциативное), интеллектуальное и информационное измерения.

Частная жизнь является защищаемым правом как в международном, так и в национальном конституционном законодательстве большинства стран. Частную жизнь и право на неприкосновенность частной жизни следует рассматривать отдельно. Голландские правоведы отмечают, что частная жизнь это не то же самое, что право на неприкосновенность частной жизни и в научной литературе часто не проводят различия между ними [8, стр.504,571]. Частная жизнь — это само существование человека, его жизнедеятельность, своеобразный «суверенитет личности», предполагающий неприкосновенность тех сторон личной жизни индивида, которые он не желает делать достоянием других [94, стр.150]. Право на неприкосновенность частной жизни — это охраняемая законом мера возможного поведения, направленная на удовлетворение интересов человека. Это универсальная категория, которая представляет собой вытекающие из самой природы человека возможности пользоваться элементарными, наиболее важными благами в условиях безопасного, свободного существования личности в обществе [95, стр.173]. Это право реализуется путем противопоставления корреспондирующих обязанностей других лиц, установленных законом, соблюдение которого обеспечивается государством.

Персональные данные как объект права на неприкосновенность частной жизни

Понятия «данные» и «информация» в основном понимаются как сведения об окружающем мире, объекте, субъекте, их характеристиках, качествах и свойствах, протекающих процессах. Соответственно, данные и информация о личности и ее частной жизни являются персональной информацией и данными обо всех аспектах частной жизни лица. Персональные данные не всегда привязаны к физической или осязаемой форме, с точки зрения неприкосновенности частной жизни ценность заключается в содержащейся в них информации, а не их осязаемости [8, стр.543]. Многолетние дебаты по поводу интерпретации права на неприкосновенность частной жизни и отношения к этому праву защиты персональных данных приводят к единогласному пониманию того, что персональные данные не могут рассматриваться вне поля частной жизни человека. Частная жизнь в любом случае имеет информационный компонент, личная информация или персональные данные являются неотъемлемым элементом и объектом частной жизни, охраняемым правом на неприкосновенность частной жизни.

В американском праве защита частной жизни прямо не предусмотрена на конституционном уровне, реализуясь через Четвертую поправку о запрете на необоснованные обыски и аресты. В связи с этим становление в Америке конституционного права неприкосновенности частной жизни прежде всего основано на прецедентном праве в области нарушений, связанных с частной жизнью. Американский автор Сара Эго иллюстрирует развитие и переход права на неприкосновенность частной жизни в США после Второй мировой войны из

сферы деликтного права в конституционное право [7, стр. 5, 6]. Многие судебные решения на протяжении двадцатого столетия сформировали понятие информационной конфиденциальности и защиты личной информации от вмешательства государственного сектора в частную жизнь, свидетельствуя о том, что персональная информация охватывается правом на неприкосновенность частной жизни.

Европейские ученые отмечают прямое конституционное закрепление неприкосновенности частной жизни, широкая интерпретация которой включает личную информацию. Соответственно, защита персональных данных находится «под зонтиком» конституционной защиты неприкосновенности частной жизни. Но в то же время, как отмечают голландские ученые, некоторые конституции в статье о неприкосновенности частной жизни могут содержать отдельные положения о защите персональных данных, или непосредственно перечислять персональные данные в числе других объектов частной жизни [8, стр.538]. Тем самым, можно рассматривать частную жизнь и персональные данные как разные объекты защиты, защищаемые отдельными правами. Итальянские ученые тоже отмечают сосуществование двух разных объектов и прав – частной жизни и персональных данных, ссылаясь на Хартию основных прав Европейского союза (ХЕСПЧ), которая отдельно устанавливает ключевые права личности - неприкосновенность частной жизни (статья 7) и защиту данных (статья 8). Неприкосновенность частной жизни является «инструментом непрозрачности», поскольку она защищает автономию, свободу и частную жизнь личности от любого вмешательства. А защита данных является «инструментом прозрачности», поскольку обеспечивает законное использование персональных данных, предоставляя отдельным лицам контроль и поощряя справедливую обработку данных субъектами [96, стр.222; 97]. Наличие двух отдельных статей, 7 и 8, в Хартии основных прав Европейского союза может свидетельствовать об отсутствии прямой связи между правом на защиту данных и неприкосновенности частной жизни, но очевидно, что неприкосновенность частной жизни является основной ценностью, на защиту которой направлена защита данных [98, стр.32].

В казахстанской правовой науке также есть различные мнения. Например, А.М.Амиров отмечает, что персональные данные - узкое понятие в отличие от понятия частной жизни, но в то же время понятие «персональные данные» является широким неисчерпывающим определением [34, стр.255, 256]. По его мнению, персональные данные и частная жизнь не идентичны и не включаются одно в другое, но пересекаются. Казахские ученые М.Ч.Когамов, Л.Т.Жанузакова, А.А.Караев используют выражение «информация о частной жизни» неразрывно и взаимосвязанно друг с другом - и как объект частной жизни, и как самостоятельный объект права на неприкосновенность частной жизни [84, стр.8, 9, 31]. Тем самым, казахские ученые рассматривают частную жизнь, как категорию, объемлющую и персональные данные, охраняемую статьей 18 Конституции Республики Казахстан 1995 года. Научно-практический

комментарий к статье 18 Конституции РК 1995 года включает вопросы персональных данных в объект частной жизни, в то же время Конституционный суд РК относит к частной жизни персональные данные и информацию о частной жизни [79, 99]. Распространение конституционной защиты на персональные данные в Казахстане прослеживается в Конституции РК 1993 года, которая прямо включала персональные данные в право на неприкосновенность частной жизни и устанавливала запрет на сбор, хранение, использование и распространение информации личного характера. Конституционная реформа 2026 года продемонстрировала регенерацию механизмов защиты персональных данных, которые присутствовали в первой Конституции независимого Казахстана 1993 года, были утрачены в период правовой трансформации 1995-го года и вновь интегрированы в статью 21 Конституции 2026 года.

Таким образом, сложно исключить, что персональные данные являются объектом частной жизни и объектом охраны конституционного права на неприкосновенность частной жизни в Республике Казахстан. Соответственно, личная информация, персональные данные являются неприкосновенными со всеми функциями и свойствами права на неприкосновенность частной жизни и подлежат конституционной охране и защите.

Профессор Д.М.Баймаханова подчеркивает, что реализация конституционных прав человека, в том числе права на неприкосновенность частной жизни, требует конкретной детализации в действующих законах и подзаконных актах [100, стр.74]. По ее мнению, дополненные законодательными актами нормы Конституции дают «дополнительный заряд» прямому действию и реализации Конституции, «раздвигая ее границы». Научно-практический комментарий к статье 18 Конституции РК говорит о том, что частная жизнь неприкосновенна и ее защита реализуется через законодательные акты, например, Уголовный кодекс РК, Гражданский кодекс РК, Кодекс об охране здоровья населения, Закон о правоохранительных органах, Закон «О персональных данных» и другие законы [79].

Таким образом, Конституция позволяет законодательным актам раскрыть содержание права на неприкосновенность частной жизни и защиту персональных данных. Специальный Закон «О персональных данных» в статье 21 прямо и ясно устанавливает, что целью защиты персональных данных является реализация прав на неприкосновенность частной жизни, личную и семейную тайну.

1.3 Функции права на неприкосновенность частной жизни и защиту персональных данных

Право на неприкосновенность частной жизни предназначено для ее защиты, тех составляющих частную жизнь объектов, которые единогласно описаны правоведами неисчерпывающим образом. Право на неприкосновенность частной жизни выражается в его свойствах, функциях, деятельности или действии,

направленном на достижение блага или защиту интереса, которым является частная жизнь. Иными словами, частная жизнь является объектом защиты, тем самым благом, ценностью и интересом человека, которое охраняется правом на неприкосновенность частной жизни.

Рассматривая право на неприкосновенность частной жизни, ученые различным образом подходят к функциям указанного права.

С.Уоррен и Л.Брандейс отмечали, что человек сам определяет (выбирает) до какой степени его мысли, сентименты, эмоции должны быть коммуницированы другим, человек сохраняет контроль и способность определять пределы публичности [5, стр.198]. Право на неприкосновенность частной жизни имеет ценностью душевное спокойствие и защиту от душевных болей и страданий [10, стр.196, 200]. Их мнение отражает самостоятельность, автономию человека в принятии решений о раскрытии частной жизни, установлении границ и контроле за их нарушением.

А.Вестин выделяет 4 функции, которые неприкосновенность частной жизни выполняет для человека - личная автономия, эмоциональное освобождение, самооценка и ограниченная и защищенная коммуникация [6, стр.32,39]. Личная автономия необходима человеку чтобы развить и защитить свою индивидуальность, «ядро личности» и ее глубинные секреты от потенциального вторжения и предотвратить манипуляцию или доминирование со стороны других [6, стр.33]. Автономия также имеет жизненно важное значение для осознания и осуществления собственного, индивидуального выбора в жизни. Поскольку социальная среда носит стрессогенный характер и негативно воздействует на человека, неприкосновенность частной жизни дает возможность человеку уединиться для эмоциональной разрядки, минимизировать воздействие общественного пространства, что жизненно важно для физического и психического здоровья личности. Через уединение приватность также обеспечивает каждому человеку возможность абстрагироваться от внешних раздражителей и проводить интроспективный анализ полученного жизненного опыта, необходимый для переосмысления и планирования. Уединение предоставляет человеку время для «творческого одиночества», способствует его интеллектуальной продуктивности и проявлению своей индивидуальности. Право на неприкосновенность частной жизни защищает частную жизнь посредством ограниченной и защищенной коммуникации. При общении в межличностных ситуациях, начиная от самых близких и заканчивая самыми официальными и публичными, ограничение выражается в установлении необходимых границ ментальной дистанции с собеседниками. Ограничение также выражается в избирательном круге доверенных лиц, которым может быть раскрыта частная жизнь, например семья и близкие друзья, где конфиденциальность защищается социальными нормами. Сведения о частной жизни могут быть также коммуницированы другим лицам в рамках их профессиональной деятельности,

например врачи или адвокаты, где в силу профессиональной этики и закона частная жизнь обладает иммунитетом от принудительного раскрытия.

Д.Солове рассматривает такие свойства права на неприкосновенность частной жизни как (1) «право быть оставленным в покое» С.Уоррена и Л.Брандейса, (2) ограничение доступа к себе как стремление личности к уединенности и душевному спокойствию, (3) секретность как сокрытие частной жизни, которую Д.Солове характеризует скорее как признак, а не свойство частной жизни, пересекающееся с ограничением доступа, (4) контроль за личной информацией, которая рассматривается шире и включает свободу принятия решений личности относительно своего тела, воспитания своих детей и другие, (5) защита личности, а именно ее автономии, индивидуальности и достоинства личности, самоопределение личности, а также защита личных близких отношений [11, стр.1099-1129]. Эти свойства он отмечает в качестве различных подходов к изучению неприкосновенности частной жизни, предлагая свой подход, фокусирующийся на деликтах, нарушениях неприкосновенности частной жизни. Тем не менее, из его работы следует, что неприкосновенность частной жизни имеет свойство (ценность) контроля личности за своей жизнью, защиты достоинства и уважения человека в обществе, степени доступа к информации [11, стр.1144,1148,1152]. Д.Солове также подчеркивает, что «ущерб автономии включает ограничение, подрыв, подавление или чрезмерное влияние на выбор людей, [так что] людям либо напрямую отказывают в свободе принятия решений, либо их обманом заставляют думать, что они свободно делают выбор» [14, стр.845]. Таким образом, Д.Солове соглашается с другими исследователями и отмечает контроль, автономию, установление пределов секретности и вторжения как свойства неприкосновенности частной жизни.

Другой американский профессор, Рут Гэвисон, выделяет функции частной жизни в виде содействия свободе, автономии, индивидуальности и человеческим отношениям, а также содействия существованию свободного общества [48, стр.423,440-455]. Более детально она определяет свойства неприкосновенности частной жизни как свободу от физического доступа и свободу действий. Последняя включает в себя свободу от негативной общественной оценки, психоэмоциональное благополучие, автономию, свободу создавать и поддерживать различные человеческие отношения, ограничение публичности или предотвращение нежелательного раскрытия, разоблачения с тем, чтобы сохранять достоинство и индивидуальность. Р.Гэвисон также считает, что право на неприкосновенность частной жизни фундаментально ограничивает доступ других к человеку. Сами по себе элементы секретности, анонимности и уединения различны, но взаимосвязаны, что вносит свой вклад в сложную природу конфиденциальности [48, стр.428].

Ниссенбаум отмечает общепринятый подход в американской литературе к таким функциям конфиденциальности как ограничение доступа и контроль [49, стр.70]. В то же время она связывает право на неприкосновенность частной жизни

с автономией личности, самоопределением в отношении личной информации и формированием идентичности [49, стр.81]. Такая функция права на неприкосновенность частной жизни, как ограничение доступа к личной информации, помогает индивиду избегать негативных последствий публичного внимания и предвзятых суждений, способствуя формированию необходимых условий для самоопределения личности, автономии и свободы мысли и поведения [49, стр.82].

Т.Наеф отмечает, что автономия — это ценность, лежащая в основе права на защиту данных, заключающаяся в истинном самостоятельном выборе человека без «манипулирования, обмана, промывания мозгов или принуждения к совершению [выбора]» [98, стр.34].

Европейские ученые Пол Де Херт (Paul De Hert) и Серж Гуртвирт (Serge Gurtwirth), рассматривая права человека и верховенство закона как принцип правового государства, отмечают, что функциями неприкосновенности частной жизни являются невмешательство, защита автономии, свобода выбора, самоопределение личности [101, стр.511-513]. Б.-Я. Коопс и другие голландские авторы отмечают автономию, позитивную и негативную свободу, контроль и ограниченный доступ как основные свойства и функции права неприкосновенности частной жизни [8, стр.533, 556-564].

Профессор К.Велис считает, что автономия и неприкосновенность частной жизни взаимосвязаны, человек должен контролировать свою автономию, свободно действовать в собственных интересах, полностью владеть собственными независимыми решениями, иметь способность к самоуправлению, быть суверенным полноправным распорядителем своей жизни и личной информации [10, стр.36,37]. Надежда Пуртова указывает, что главным обоснованием, ключевой идеей права на неприкосновенность частной жизни является сохранение человеческой свободы и автономии и предотвращение самоцензуры из-за страха быть привлеченным к ответственности за свои действия в будущем [23, стр.183]. Хелена Врабец (Helena Vrabec), рассматривая неприкосновенность частной жизни, отмечает три измерения автономии: свобода от вмешательства других, свободный выбор и самоуправление [102, стр.6]. Р.Костелло называет автономию личности, установление и управление границами, контроль и самоопределение функциями неприкосновенности частной жизни [67, пункт [2.15]].

Историческое решение Федерального конституционного суда Германии от 1983 года относительно соответствия Основному закону норм Закона о переписи населения ознаменовало фундаментальный сдвиг в правовой доктрине права на неприкосновенность частной жизни и защиту персональных данных [103]. Суд сформулировал право на информационное самоопределение как свойство, присущее защите частной жизни, ее имманентный элемент. Федеральный конституционный суд обосновал данное свойство путем юридического синтеза двух фундаментальных положений Основного закона Германии: ценность и достоинство личности, а также свободное развитие личности, что позволило

выделить информационное самоопределение, гарантирующее право на общее развитие личности в той мере, в какой оно не нарушает права других. Данное решение Федерального Конституционного суда закрепило право на информационное самоопределение как конституционную гарантию, обеспечивающую индивиду право «в принципе, самостоятельно решать, раскрывать ли и в какой степени аспекты своей личной жизни» [103, §144]. В контексте развития автоматизированной обработки данных суд усмотрел риски неограниченной обработки и создания профилей для человека и закрепил свободу решения индивида о совершении определенных действий как необходимое условие индивидуального самоопределения [103, §§145, 146]. Данная конституционная гарантия предотвратила трансформацию человека из активного субъекта права в пассивный объект алгоритмического наблюдения.

Развитие данной доктрины и ее последующая рецепция на наднациональном уровне в Директиве 95/46/ЕС привели к тому, что аналогичные ценностные ориентиры стали фундаментом европейской системы защиты прав и международными стандартом современности [104]. В судебных решениях ЕСПЧ право на неприкосновенность частной жизни предусматривает такие свойства как автономия и информационное самоопределение, развитие личности, контроль частной жизни. Перечисленные свойства, как важные принципы, заложены в основе толкования неприкосновенности частной жизни [93, §137; 88, §89; 92, §70]. Таким образом германская конституционная концепция 1983 года послужила идеологическим прообразом для современной интерпретации статьи 8 Европейской Конвенции и утвердила информационную автономию как необъемлемый атрибут правового статуса личности в цифровую эпоху.

Особо следует затронуть такое свойство права на неприкосновенность частной жизни, как «разумное ожидание конфиденциальности». Это свойство по содержанию сложно отнести к функции автономии, самоопределения, контроля и ограничения доступа, свободе действий или выбора. Формулировка «разумное ожидание приватности» появилась в американской прецедентной практике после Второй мировой войны. Большей частью иски о нарушении неприкосновенности частной жизни подавались против американских правительственных органов, которые злоупотребляли слежкой, незаконным получением сведений от частных лиц с использованием новейших технологий видео и аудиозаписи, в том числе электронных, таким образом вторгаясь в частную жизнь вопреки конституционному праву на неприкосновенность личности. Американские суды как правило подходили с «физической» стороны к неприкосновенности частной жизни, аргументируя защитой физических пространств. Переломным стало дело Чарльза Каца, который был осужден на основании разговоров о совершении незаконных ставок, записанных с помощью подслушивающего устройства, прикрепленного к телефонной будке [105]. Суд постановил, что закрытая телефонная будка обеспечивает конституционно защищенное ожидание уединения, и что как электронное, так и физическое вторжение может нарушать

неприкосновенность частной жизни. Судом был сформулирован тест «разумного ожидания конфиденциальности»: человек должен продемонстрировать «фактическое (субъективное) ожидание конфиденциальности», и «ожидание [должно] быть таким, которое общество готово признать «разумным» [105, стр.361,362].

Ожидание приватности также отмечается в судебной практике ЕСПЧ. ЕСПЧ указывает в своих решениях, что право на неприкосновенность частной жизни включает ожидание анонимности или нераскрытия информации о частной жизни лица, законное ожидание защиты и уважения его или ее личной жизни, разумное ожидание неприкосновенности частной жизни [89, §109; 93, §29; 92, §§73, 80; 88, §§89, 93,103,125]. Состояние ожидания конфиденциальности индивида относится к разным измерениям частной жизни. В своих ключевых решениях ЕСПЧ приводит аргумент о разумном ожидании приватности в отношении видеонаблюдения на рабочем месте и в общественных местах, в отношении информации налогоплательщика, сведений о привлечении к уголовной ответственности, личной переписки. Кроме коммуникационной, пространственной, информационной конфиденциальности, разумное ожидание неприкосновенности частной жизни очевидно относится к телесной приватности, например, в момент переодевания человек разумно ожидает отсутствие посторонних взглядов.

Частная жизнь и сохранение ее в тайне исходит от самой личности, от ее понимания, восприятия и ожидания конфиденциальности в определенных условиях.

Разумное и законное ожидание приватности сложно отнести к какому-либо другому свойству неприкосновенности частной жизни, поскольку оно не подконтрольно человеку, не выражает самостоятельное принятие решений, установление границ и невмешательство, свободу и автономию. Разумное ожидание приватности подразумевает действия другого лица, выражающиеся в невмешательстве в любую сферу частной жизни человека. Действия другого лица исходят из уважения к личности и его частной жизни, понимания границ вмешательства, которые установлены этическими, моральными нормами или положениями закона. К примеру, находясь в доме человек ожидает, что он, его действия, мысли, занятия защищены от внешнего вмешательства. Склеивая конверт с письмом, человек ожидает, что его конверт дойдет до адресата без чьего-либо вскрытия. Проходя через службу безопасности аэропорта человек ожидает, что его багаж будет просканирован, а сам он может быть подвергнут личному досмотру, все, к чему служба безопасности имела доступ, сразу же будет «забыто». Беседа с профессиональным консультантом (адвокатом, врачом) также ожидает, что сведения о частной жизни станут известны и могут быть необходимы консультанту, но не будут распространены или раскрыты третьим лицам. Соответственно, человек имеет право и ожидание того, что его частная жизнь не будет нарушена, либо ставшая известной другому лицу информация о его частной

жизни будет сохранена в тайне или забыта, уничтожена, не будет раскрыта, опубликована или распространена кому-либо. Разумное ожидание приватности допускается рассматривать как одно из свойств неприкосновенности частной жизни поскольку его сложно отнести к какой-либо из функций неприкосновенности частной жизни, и оно может относиться к любой сфере, любому измерению частной жизни.

Казахстанские ученые также косвенно рассматривали свойства и функции неприкосновенности частной жизни. Л.Ф.Татарина выделяет право на свободу располагать собой и находиться без внешнего контроля [78, стр.66]. Н.Н.Турецкий подчеркивает исключительную важность права на неприкосновенность частной жизни и автономии человека, способствующей реализации других прав и свобод человека, творческому развитию личности, демократизации общества и государства [87, стр.13,14]. Он также придает важное значение свободе мысли, совести и вероисповедания, самостоятельному и независимому выбору человека осуществлять действия и реализовывать свои права и свободы [84, стр.11,12]. Л.Т.Жанузакова выделяет право человека вести жизнь по собственному усмотрению, но больше фокусируется на невмешательстве третьих лиц в частную жизнь [84, стр.27]. При описании объектов частной жизни Н.Р.Весельская и Ю.Н.Еремин прослеживается детерминация таких функций неприкосновенности частной жизни как субъектная автономия и управление режимом доступа [84, стр.35,36]. С.А.Жижис в попытке дать доктринальное толкование неприкосновенности частной жизни исходит только из объектов частной жизни и связанных с ней деликтов, но не описывает свойства или функции права на неприкосновенность частной жизни [106, стр.10-15].

В казахстанской правовой мысли наблюдается консенсус относительно широты и многоаспектности объектного состава частной жизни. Однако, в отечественных исследованиях наблюдается дефицит анализа функциональных характеристик права на неприкосновенность частной жизни, включающих самостоятельность и автономию человека в принятии решений о раскрытии частной жизни, установлении границ и контроле за их нарушением, свободу в выборе своего поведения и мировоззрения, выборе и контроле степени своей публичности и определении степени близости отношений и коммуникации.

Тем не менее, в научно-практическом комментарии к статье 18 Конституции РК 1995 года отмечено субъективное право каждого человека на всемерную государственную защиту тех условий, которые создают ему возможность беспрепятственно пользоваться своими благами для реализации личных потребностей. Соответственно, Конституцией закладывается функция свободы частной жизни. Дополнительно в контексте сохранения личной тайны отмечается право индивида определять свое поведение в обществе, самостоятельно регулировать режим информации, что говорит о таких свойствах, как автономия, самоопределение личности, ограничение и контроль доступа к информации [79]. Иными словами, в отечественной науке прослеживается

согласие зарубежными авторами в том, что частная жизнь служит для защиты человека, его автономии, свободы, идентичности и самосозидания, контроля своей частной жизни, определении границ и степени доступа, контроля за коммуникациями и информацией. Данная позиция о функциях права на неприкосновенность личности подтверждена постановлением Конституционного Суда РК, что свидетельствует об их единственном нормативном закреплении в законодательстве РК [99, пункт 2].

Доктринальное понимание частной жизни как комплексного, неисчерпаемого понятия с выраженным информационным ядром обуславливает тесную взаимосвязь права на неприкосновенность частной жизни с институтом защиты персональных данных. В данном контексте функциональное назначение права на неприкосновенность частной жизни выступает концептуальным фундаментом для обеспечения защиты персональных данных.

Функциональные параметры неприкосновенности частной жизни служат базовым инструментарием индивидуума, обеспечивающим автономную защиту сведений о его личной сфере. Через призму субъектной автономии человек осуществляет демаркацию собственных границ конфиденциальности информации и градирует степени ее секретности. Уровень конфиденциальности детерминирует волевые решения личности относительно модальности, объемов и целесообразности раскрытия сведений третьим лицам. Обладая дискреционными полномочиями, индивид дифференцирует состав передаваемой информации в зависимости от категории получателей – от личностно-бытового окружения до профессиональных и публичных сообществ. В данном контексте информационное самоопределение вступает в комплиментарную связь с механизмами установления пределов вмешательства и управлением ими. Таким образом, совокупность функциональных компонентов приватности – от субъектной автономии до механизмов администрирования коммуникативных барьеров — служит опорной конструкцией для обеспечения правового иммунитета личности от необоснованного вмешательства, трансформируя абстрактную неприкосновенность частной жизни в защищенный режим персонального информационного суверенитета.

2 ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РЕСПУБЛИКЕ КАЗАХСТАН И ЗАРУБЕЖОМ

2.1 Понятие и виды персональных данных в Республике Казахстан и зарубежом

Понятие персональных данных является предметом дискуссий на протяжении не одного десятилетия. В зарубежном праве во второй половине XX века вопрос защиты личной информации поднимался в ответ на внедрение новых технологий и рост использования коммерческих компьютерных баз данных [107, стр. 81]. С начала XXI века развитие более современных технологических достижений, как, например, камеры мобильных телефонов, социальные сети и различные цифровые помощники привлек более пристальное внимание к вопросу понятия «персональные данные».

Первым шагом нормативного закрепления понятия «персональные данные» стала Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера, принятая в Страсбурге 28 января 1981 года (Конвенция 108) [108]. Конвенция разработана как специальный инструмент для защиты права на уважение частной жизни, предусмотренного статьей 8 Европейской Конвенции о защите прав человека и основных свобод 1950 года [107, стр.81]. Конвенция 108 вводит ключевые термины «персональные данные» и «автоматизированная обработка», а также устанавливает принципы обработки персональных данных.

В статье 2 Конвенции 108 персональные данные определяются как «любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу». Принятая на ее основе Европейская Директива 95/46/ЕС, и заменивший ее Европейский Регламент (GDPR) дублируют это понятие [104, 45].

В GDPR понятие персональных данных (статья 4(1)) означает любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу («субъект данных»). Важным признаком, определяющим сведения как персональные данные, является (1) относимость этих сведений к лицу и (2) возможность идентификации лица на основе этих сведений.

Данное понятие «персональные данные» в GDPR основывается прежде всего на Конвенции 108, правоприменительной и судебной практике применения предшествующей Директивы 95/46/ЕС о защите данных. До принятия GDPR Европейский уполномоченный орган по персональным данным издал руководство о понятии «персональные данные» [110].

Определение «персональные данные» в Европе сосредоточено на четырех ключевых взаимосвязанных элементах: «любая информация», «относящийся к», «идентифицированное или идентифицируемое» и «физическое лицо». Элемент

«любая информация» имеет широкое значение и означает, что объективная и субъективная информация о человеке в любом качестве, независимо от характера или содержания информации и технического носителя, на котором она содержится, может рассматриваться как «персональные данные». Элемент атрибутивности «относящийся к» играет решающую роль в определении содержательной сферы применения концепции, особенно в отношении объектов и новых технологий. Три самостоятельных элемента - содержание, цель или результат – определяют, «относится ли» информация к человеку. Это включает информацию, которая явно влияет на то, как человека воспринимают или оценивают. Наконец, элемент «идентифицированный или идентифицируемый» фокусируется на условиях, при которых лицо следует считать «идентифицируемым», и особенно на «средствах, которые, вероятно, разумно будут использованы» для идентификации этого лица.

Согласно GDPR понятие «идентифицируемое физическое лицо» означает:

«идентифицируемое физическое лицо» — это лицо, которое можно идентифицировать прямо или косвенно, в частности, посредством ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении, онлайн-идентификатор, или на один или несколько факторов, специфичных для физической, физиологической, генетической, психической, экономической, культурной или социальной идентичности этого физического лица;»

Признак идентификации, возможность установления личности лица, имеет особое значение. При этом немаловажен тип сведений, который позволяет установить личность самостоятельно или в совокупности с другими сведениями, обозначенными в понятии «идентифицируемое физическое лицо». Наряду с традиционным использованием имени для идентификации человека, определение в статье 4 четко дает примеры других личных данных как «идентификационный номер» и «один или несколько факторов», характерных для какой-либо идентичности физического лица. Большая часть сведений, собранных в Интернете, отличается от традиционных сведений о человеке, например онлайн-идентификаторы, транслируемые устройствами пользователя, приложениями, сетевыми инструментами и протоколами, такими как IP-адреса, файлы cookie, метки радиочастотной идентификации или другие идентификаторы (GDPR, пункт 30 Преамбулы). Например, веб-сайты используют IP-адреса для идентификации пользователей, которые совершают онлайн-покупки, поиск в Интернете и загрузку мультимедиа [111]. Также владельцы веб-сайтов или третьи стороны по всему миру собирают данные о пользователях через cookie, текстовый файл, сохраненный на устройстве пользователя. Когда пользователь возвращается, cookie помогает распознать устройство и связать предыдущие посещения с текущей информацией, что приводит к подробным профилям пользователей. Файлы cookie могут хранить данные пользователя, такие как просмотренные страницы, нажатые объявления и идентификационные номера пользователя [112].

Сетевые реквизиты обладают потенциалом идентификации физического лица в цифровой среде в сочетании с иными атрибутами и способствуют формированию уникальных цифровых профилей, достаточных для индивидуализации личности.

Практика Европейского Суда (ЕСJ) показывает, что к персональным данным относятся такие данные о коммуникациях человека, как дата, время, продолжительность и тип коммуникации, информация об устройствах связи пользователя и их местоположении, имя и адрес абонента, номер телефона человека и многое другое [113]. В одном из прецедентов ЕСJ подтвердил расширительное толкование категории персональных данных, относя к ним письменные экзаменационные ответы и любые комментарии экзаменатора относительно этих ответов. Суд подчеркнул, что отсутствие у проверяющего сведений о личности экзаменуемого в момент оценки не лишает сведений статуса персональных данных, поскольку наличие уникального числового кода на бланке сохраняет потенциал восстановить связь с личностью экзаменуемого, то есть присутствует возможность опосредованной идентификации субъекта [114].

Персональные данные могут включать следующее: (1) регистрационные данные аккаунта в социальных сетях, публикации, фотографии, подписчики или «социальный граф»; (2) идентификаторы IMEI, MAC-адреса и другие идентификаторы устройств; (3) Аудиоданные, как голосовые шаблоны и разговоры, собранные смарт-устройствами; (4) любые данные онлайн-датчиков (смарт часы, датчики программного обеспечения транспортных средств и др.

Идентификационный потенциал рассматриваемых сведений детерминирует методологию Европейского регламента GDPR, закрепляющего значимость способа идентификации – прямой или косвенный. Существование самого факта, вероятности или возможности даже косвенно определить лицо по какому-либо сведению уже является достаточным основанием для признания этого сведения персональной информацией. Учитывая стремительное совершенствование инструментария обработки данных и интеграцию систем искусственного интеллекта, нормы GDPR имеют адаптивный к новым технологиям характер, положения данного нормативного акта рассчитаны на долгосрочную перспективу, обеспечивая универсальную защиту в динамично меняющемся цифровом пространстве.

Нормативное закрепление понятия «персональные данные» в специальном Законе Республики Казахстан «О персональных данных и их защите» в подпункте 2) статьи 1 закреплено следующим образом:

«персональные данные - сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе».

Отечественная правовая модель придерживается широкой интерпретации понятия «персональные данные», поскольку отсутствует жесткая детерминация перечня сведений, понимаемых под персональными данными. Научно-

практический комментарий к статье 18 Конституции РК подтверждает открытую интерпретацию информации, которая может относиться к персональным данным, включая «сведения о человеке, дающие оценку его характеру, облику, здоровью, материальному состоянию, семейному положению, образу жизни, отдельным фактам биографии» [79]. Более того, следуя позиции Конституционного Суда РК частная жизнь включает сведения о профессиональных, творческих, социальных, имущественных, политических, религиозных, гендерных, экономических, поведенческих и любых других сторонах частной жизни лица [99, п.2].

В современной правоприменительной практике Казахстана наблюдается тенденция к сужению понятия персональные данные. В частности, при оценке правомерности видеонаблюдения и видеосъемки в процессе трудовых отношений и коммерческой деятельности между физическими лицами и субъектами бизнеса МВД, Министр труда и МЦРИАП в своих ответах фактически исключают широкое толкование понятия персональные данные [115, 116, 117]. МЦРИАП, как уполномоченный государственный орган в области защиты персональных данных, не относит видеоизображения человека к персональным данным и биометрическим данным, обосновывая отсутствием дополнительных сведений и возможности характеризовать физиологические и биологические особенности человека. Данная правовая интерпретация была фактически транслирована и в позицию Конституционного Суда, который в своем нормативном постановлении использовал диспозитивную оговорку, допускающую ситуацию, при которой изображение может не признаваться персональными данными [99, п.4]. Судебная практика также подтверждает охраноспособность изображения отдельно от персональных данных или в контексте врачебной тайны [118, 119]. Другой пример узкой интерпретации касается индивидуального идентификационного номера (ИИН) физического лица, который по мнению профильного органа не относится к персональным данным, поскольку в отдельности от других дополнительных сведений о лице ИИН не позволяет идентифицировать личность [120]. Иные примеры также демонстрируют, что государственные органы, рассматривая обращения граждан, ограничиваются репродуцированием формулировок законов, без контекстуального анализа и должной конкретизации относительно квалификации сведений как персональных данных [121, стр.408, 409].

Аналогичная противоречивость прослеживается и в судебной практике толкования понятия «персональные данные», где суды расходятся в оценке тождественных наборов данных [122, 123]. В одном из решений суд признал, что сведения в квитанции об оплате коммунальных услуг (ФИО, расходы на содержания жилья, адрес места жительства жильцов), определяют физических лиц, в том числе как собственников имущества, и, следовательно, данные сведения признаются персональными данными [122]. С этой позицией совпадало мнение суда первой инстанции в другом деле, где указание в общедомовом чате фамилии, имени и номера квартиры квалифицировано распространением персональных данных. Однако, суд апелляционной инстанции вынес

противоположное решение, отметив, что фамилия, имя и номер квартиры без ИИН не являются персональными данными [123]. Вместе с тем, такие сведения, как ФИО, семейное положение, ФИО супруга, место его работы и сведения о детях, суды все-таки склонны признавать персональными данными и без ИИН [118, 124].

Подобная двойственность интерпретации норм закона свидетельствует о том, что, государственные органы и суды следуют формально-буквальному тексту закона, подразумевая, что каждая отдельная личная информация, как например, видеоизображение человека, дактилоскопия, ИИН, при отсутствии дополнительной информации не подлежит защите Закона «О персональных данных». Проблема усугубляется тем, что формулировки Закона РК «О персональных данных» не акцентируют внимания на признании сведения персональными данными, если оно позволяет определить личность не только самостоятельно, но и в сочетании с другими сведениями. Ведь степень и точность идентифицируемости человека по дате рождения, индивидуальному идентификационному номеру, номеру телефона, видеоизображению очень высока по сравнению с данными смарт-устройств или почерка человека. Некоторые сведения позволяют определить человека напрямую, некоторые – очень близко подойти к идентификации, а для некоторых сведений потребуются дополнительная информация и сложные технологии для сопоставления информации и установления личности. В условиях перманентного технологического развития подобный формально-юридический подход казахстанских государственных органов к понятию «персональные данные» вступает в концептуальное противоречие с онтологической сущностью права на неприкосновенность частной жизни. Для устранения противоречия требуется императивная детализация профильного законодательства путем закрепления тезиса об автономной правовой ценности отдельных сведений о личности. Режим правовой охраны дискретных данных должен осуществляться безотносительно наличия комплементарной информации, постулируя обязанность третьих лиц обеспечивать защищенную обработку любых данных, потенциально идентифицирующих субъекта.

Данная потребность в расширении границ правовой защиты отдельных сведений и пересмотре критериев идентифицируемости находит свое отражение в актуальных дискуссиях зарубежных авторов. В области правовых исследований ведутся серьезные дискуссии относительно того, что определяет идентификацию в цифровой сфере. Это включает в себя то, можно ли считать данные о человеке, найденные в сети, его личной информацией, особенно в случаях, когда обрабатываются анонимные данные, или неточные, ложные, «подставные» сведения о человеке (например, ложное имя, ложный почтовый адрес, номер телефона и другие типы информации) [125, стр.83].

Большинство ученых утверждают, что даже если данные нельзя напрямую связать с именем, они позволяют идентифицировать людей с помощью «безымянных данных» [20, стр.17, 31]. Сара Эго утверждает, что технологии,

которые обычно служили уголовному правосудию, стали удобными формами идентификации в частном секторе [7, стр.359]. Рафаэль Геллерт (Raphaël Gellert) отмечает, что хорошо анонимизированные данные все равно могут привести к повторной идентификации в 99% случаев [126, стр.205, 206]. К.Кунер подчеркивает, что технология может идентифицировать неизвестных лиц с помощью косвенной информации, сопоставив его изображение с профилями в социальных сетях и в интернете [127]. К.Велис приводит примеры повторной идентификации с использованием личных данных, таких как дата рождения, местонахождение, пол, почтовый индекс и даже оценивание рейтинга фильмов [10, стр.13]. В онлайн пространстве «все становится информацией» и «в контексте «умной» среды данные всегда будут относиться к людям» [126, стр.199, 202]. Частицы информации, которые пользователь оставляет в Интернете, и которая не поддается идентификации, может стать идентифицированной» и «почти однозначно» и «ясно» идентифицировать человека [16, стр.1891; 128, стр.37]. Идентификация ограничивает способность человека быть анонимным или псевдонимным и может негативно повлиять на личность [12, стр.123].

Н.Пуртова приводит три подхода к идентификации личности: «гражданская идентичность» Лиенса (Leenes), определяемая такими характеристиками, как паспортные данные и имя; социологическая типология Гэри Маркса (Gary Marx), противопоставляющая идентификацию анонимности; и точка зрения Хелен Ниссенбаум, утверждающей, что ценность анонимности заключается в «обеспечении недостижимости» [23, стр.167-169]. Анонимность является ключевым аспектом неприкосновенности частной жизни [6].

Таким образом, признак идентификации имеет огромное значение в зарубежном праве. Существование самого факта, вероятности или возможности даже косвенно определить лицо по какому-либо сведению уже является достаточным основанием для признания этого сведения персональной информацией. Принцип потенциальной идентифицируемости заложен в дефиниции персональных данных Европейского регламента GDPR.

В отличие от GDPR в Казахстане нормативное закрепление понятия персональные данные допускает использование отдельных сведений, сочетание различной информации о человеке, косвенную идентификацию личности, способствуя утрате анонимности, вопреки праву на неприкосновенность частной жизни. Тем самым, Закон «О персональных данных» не обеспечивает реализацию права на неприкосновенность частной жизни и защиту лица, поскольку допускает произвольное прямое и косвенное вмешательство любых лиц в его частную жизнь.

Принятый Цифровой Кодекс РК не вносит ожидаемой ясности в правовое регулирование защиты персональных данных и их дефиницию. Напротив, нормативный анализ терминологии Цифрового Кодекса РК, понятий «персональные данные», «цифровые данные», «данные», позволяет констатировать проблему смешения критериев классификации по содержанию и по форме.

Цифровой Кодекс РК детерминирует цифровые данные через их технологическую природу и функциональное назначение, как *информацию*, предоставленную в цифровой форме, доступную для программно-аппаратного воздействия и аналитической обработки [44, ст.17]. В то же время Закон «О доступе к информации» закрепляет субстантивный подход, определяя широкую дефиницию «*информация*» как *сведения*, зафиксированные в любой форме вне зависимости от их содержательного состава – лица, предметы, факты, события, явления и процессы [129, ст.1]. Таким образом, Цифровой Кодекс РК дифференцирует данные по критерию формы представления, обладающей свойством операционной пригодности для цифровых технологических инструментов. При этом, содержательная составляющая цифровых данных коррелирует с общеправовым понятием «информация».

Параллельно с этим АППК РК закрепляет дефиницию «данные» как *информацию* в формализованном виде, пригодную для обработки [130, ст.4]. В отличие от узкотехнологического подхода Цифрового Кодекса РК, в АППК РК сведения классифицируются не по содержательному свойству, а по форме их представления, допускающей любую форму представления, которая обладает операционной способностью как цифровой, так и в аналоговой среде.

Законом «О персональных данных» персональные данные определяются через признак атрибутивности как данные, относящиеся к физическому лицу. Формально-юридический анализ показывает, что закон, не ограничивая содержательную сторону персональных данных, акцентирует внимание на их пригодности для полного цикла информационного оперирования (от сбора до удаления) как в автоматизированных системах, так и в традиционном документообороте.

Особого внимания заслуживает трансформация дефиниции «персональные данные». С 11 июля 2026 года в Закон «О персональных данных» вносятся изменения, согласно которым персональные данные определяются как сведения или совокупность сведений о субъекте персональных данных, дополненные одним или несколькими идентификаторами персональных данных [131]. Примечательно, что проект Цифрового Кодекса на стадии обсуждения содержал попытку детализации этого понятия через введение неисчерпывающего термина «идентификатор персональных данных», к которым относились ФИО, ИИН, номер мобильного телефона, изображение лица и биометрический вектор лица субъекта персональных данных, или их производные, которые могут быть восстановлены обратным преобразованием до первоначального значения [132]. Однако в окончательной редакции Цифровой Кодекс РК и Закон «О персональных данных» воздержались от предоставления точного определения «идентификатора», ограничившись признанием ИИН в качестве уникального идентификатора физических лиц [44, ст. 41].

Толкование слова «идентификатор» обычно относится к уникальному атрибуту субъекта или физического лица, который облегчает его идентификацию

или дифференциацию от других субъектов. В отношении отдельных лиц такие уникальные атрибуты могут включать в себя широкий спектр характеристик, в том числе, помимо прочего, имена пользователей, ИИН, номера удостоверяющих документов, почерк и физические особенности, такие как выступающий нос, выпуклые глаза или вьющиеся волосы. Эти идентификаторы могут включать физиологические, поведенческие, социальные или другие отличительные характеристики субъекта. Отсутствие законодательной дефиниции «идентификатор» в условиях расширения его толкования (от поведенческих характеристик до физических особенностей) подчеркивает сложность и многогранность идентификации персональных данных в цифровую эпоху и создает почву для неоднозначных интерпретаций.

Синтез дефиниций «данные», «цифровые данные», «персональные данные» подтверждает идентичную онтологическую природу и наличие единой содержательной основы – сведения о лицах, предметах, фактах, событиях, явлениях и процессах. Однако, правовые акты различаются в методологической защите личной информации. Методология Закона «О персональных данных» конструируется вокруг личности и атрибутивном свойстве информации, предоставляя защиту любой форме ее представления, пригодной для восприятия и анализа. Цифровой Кодекс РК имеет техноцентричную, формально-объектную методологию, для которой содержание охраняемой информации имеет факультативное значение.

В контексте развития цифровой экономики и платформенной среды рестриктивный подход Цифрового Кодекса РК не охватывает возможные риски для основных прав и свобод, может иметь пробелы в правовой защите неприкосновенности личности в том числе и в цифровой среде. К примеру, Цифровым Кодексом РК вводятся понятия «цифровая идентичность», «цифровая аутентификация», «цифровое пространство», которые не обеспечивают в адекватной мере защиту права на уважение частной жизни и защиту персональных данных. Ограничение понятия «цифровое пространство» исключительно личным кабинетом гражданина Республики Казахстан в «электронном правительстве» оставляет за периметром охраны обширные массивы данных как казахстанских граждан, так и иных резидентов Республики Казахстан, на частных негосударственных платформах и в социальных сетях. Кроме того, признание Цифровым Кодексом РК цифровой идентичности неимущественным правом без детальной регламентации механизмов его защиты со стороны государства превращает данную норму в декларативную.

Таким образом, взаимодействие Цифрового Кодекса РК и Закона «О персональных данных» вынуждает субъектов правоотношений адаптироваться к гибриднему и сложному режиму защиты персональных данных. Сосуществование техноцентричного и атрибутивного подходов регулирования персональных данных создает риски правовых коллизий, что обременяет бизнес и дезориентирует физических лиц в вопросах защиты своих прав. Для минимизации

рисков ущерба субъектам персональных данных и правовой определенности в применении «гибридного» правового регулирования Закон «О персональных данных» требует совершенствования таким образом, чтобы в нем законодательно закреплялся доминирующий общий правовой режим защиты персональных данных вне зависимости от формы их представления, а также устанавливались единые права и обязанности контролеров и операторов, гарантирующих соразмерную защиту субъектов в любой среде информационного взаимодействия.

Виды персональных данных

В научной сфере многие авторы предпринимают попытки систематизировать и классифицировать персональные данные.

К примеру, используемые среди государственных органов личные данные можно классифицировать по следующим категориям: демографическая информация, личная идентификационная информация, медицинская информация, финансовая информация и судебные данные [133, стр.8]. Внутренняя составляющая каждой из категорий отличается в различных государствах. К примеру, судебные данные, помимо наличия судимости могут включать наличие и административных санкций, примененных к лицу. Перечень медицинских данных во многих странах имеет отличие от общей широкой формулировки как любые данные, относящиеся к здоровью лица, так и с более конкретным указанием конкретных сведений, к примеру, грудное вскармливание, зависимости, или сведения, связанные с принятием мер, направленных на здоровье человека [133, стр.8]. Через множество приложений на устройствах (смартфоны, смарт-часы и тому подобные) о пользователе собирается информация, в том числе о физиологических параметрах (рост, вес и т.п.), диете и потреблении калорий, физических и спортивных нагрузках, сведения для женского здоровья, устанавливаются программы для напоминания о приеме медицинских препаратов, медицинские записи врачей, мониторинг сна, сердцебиения, частоты дыхания и прочая информация [133, стр.10].

В финансовом секторе круг собираемой и используемой личной информации помимо личных идентификационных данных может содержать информацию о проводимых финансовых операциях. Однако, из таких сведений косвенно можно вывести и иные личные данные, к примеру, анализируя произведенные платежи с банковской карты, по произведенным покупкам можно идентифицировать предпочтения владельца. Например, сегодня технологические разработки и возможности казахстанских банков второго уровня позволяют собирать невероятное количество информации о клиентах банка. В мобильных приложениях банков физические лица получают не только доступ к банковским услугам, но и другим сервисам, таким как осуществление любых покупок, от продуктов и лекарственных средств до любой техники, путешествий и любых услуг. Более того, интеграция банковских платформ в Казахстане с платформой электронного правительства и предоставление банками государственных услуг в

электронной форме дает коммерческим банкам беспрецедентный доступ к личной информации физических лиц [134, стр.48-53].

Применение новых технологий позволяет выделить и другие личные данные, например, связанные с безопасностью (видеокамеры наблюдения, аудиозаписывающие устройства), а также отдельный класс данных составляют биометрические данные (отпечатки пальцев и ладоней, контуры лица и его частей, рост, вес, цвет глаз), в том числе психологическая и поведенческая биометрия, жестикуляция и прочее. Помимо этого, теоретики приводят и ряд других классификаций личных данных [133, стр.10].

Казахстанский Закон «О персональных данных» выделяет две основные группы персональных данных по признаку доступности: общедоступные персональные данные и персональные данные ограниченного доступа (ст.6). Указанная классификация персональных данных ограниченного доступа определяется типом доступности или «секретности». При этом доступ к каким-либо данным устанавливается либо законом, либо субъектами правоотношения в сфере защиты персональных данных.

Соответственно, персональными данными ограниченного доступа являются те, которые другие законы относят к таковым.

Так, Закон РК от 24 ноября 2015 года «Об информатизации» дает классификацию электронных информационных ресурсов по типу содержащихся в них персональных данных [135]. Перечень таких сведений Законом РК «Об информатизации» не закреплен. Далее, Закон РК от 19 марта 2010 года «О государственной статистике» (пункт 1 статьи 8) указывает, что первичные статистические данные являются конфиденциальными, кроме перечисленных в пункте 4 статьи 8, как например ФИО и ИИН индивидуального предпринимателя-физического лица [136]. Следовательно, *любые другие* данные, кроме ФИО и ИИН, относятся к конфиденциальным статистическим данным, что говорит о широкой интерпретации понятия конфиденциальных данных.

Предпринимательский кодекс (пункт 13 статьи 28) относит к общедоступной информации ФИО, ИИН, место нахождения индивидуального предпринимателя, что практически всегда совпадает с его домашним адресом [137]. Не являются конфиденциальными ФИО и ИИН индивидуального предпринимателя, что также подтверждает уполномоченный орган, ставя под угрозу не только финансовую безопасность личности, но и безопасность его семьи [138]. Министерство юстиции РК поддерживает данную позицию, но считает ИИН участника юридического лица персональными данными ограниченного доступа [139]. Напротив, Министерство внутренних дел в целом определяет ФИО, ИИН, дату рождения, национальность и адрес как персональные данные ограниченного доступа [140]. МЦРИАП не предоставило конкретных указаний относительно того, что представляют собой персональные данные ограниченного доступа [141].

Требования к публикации сведений индивидуальных предпринимателей на уровне закона отменяют недоступность персональных данных, лишая физического

лица защиты частной жизни. Такой казахстанский подход не согласуется с судебной практикой ЕСПЧ, который установил, что размещение личной информации в публичном доступе, в том числе в государственных базах данных, автоматически не отменяет защиту частной жизни, предусмотренную статьей 8 Конвенции [93, §134]. ЕСПЧ выразил серьезные опасения о публикации личной информации и домашнего адреса в государственных источниках [90, Concurring opinion of Judge KÜRIS]. По его мнению, очень сложно обосновать законную причину и ясную, насущную общественную потребность для размещения личной информации, особенно если может касаться членов семьи, включая детей. Никто не имеет законного интереса знать домашний адрес человека против его воли. Таким образом, раскрытие адреса заявителя не служит законной цели и угрожает безопасности человека и его семьи, особенно для детей. Кроме того, ЕСПЧ отмечает, что сведения о налогооблагаемом доходе, активах налогоплательщиков явно касаются их частной жизни, соответственно доступ к ним должен обеспечиваться строгими правилами [93, §138].

Специфический режим доступности персональных данных закреплен Законом РК от 22 декабря 2003 года «О государственной правовой статистике и специальных учетах», который регулирует порядок сбора, хранения и обработки персональных данных для специальных учетов, касающихся правоохранительной и исполнительной сферы общественных отношений [142]. Данным Законом в специальные учеты могут быть внесены любые сведения о физическом лице, при этом, не требуется его согласие. Примечательно, что закон не относит к личной и семейной тайне ФИО, дату и место рождения физического лица. Уполномоченный орган по защите персональных данных не оспаривает такую позицию и относит ФИО к персональным данным ограниченного доступа в сочетании с финансовой тайной, тайной медицинского работника и иной охраняемой законом тайной [143].

В связи с не ясным нормативным закреплением понятий персональных данных ограниченного доступа на практике расходятся позиции регуляторных органов. Сам уполномоченный орган по защите персональных данных не дал конкретного ответа на вопрос, что входит в перечень персональных данных ограниченного доступа [141]. Существующая вариативность интерпретации в классификации персональных данных по признаку доступности свидетельствует о дефиците правовой определенности среди органов исполнительной власти и нарушении принципа единообразного применения закона.

Неясность Закона «О персональных данных» также прослеживается в отношении биометрических данных. Закон дает общую характеристику, но не раскрывает ее подробно и не указывает, относится ли в общем такая информация к персональным данным ограниченного доступа. Закон РК «О дактилоскопической и геномной регистрации» содержит дефиниции «геномная информация» и «дактилоскопическая информация», с помощью которых можно идентифицировать лицо, установить его личность и персональные данные [144, Статьи 1 и 8]. При этом дактилоскопическая информация определена как

биометрические данные. Тем не менее, и геномная, и дактилоскопическая информация отнесены к персональным данным ограниченного доступа. Иными словами, существует вероятность, что какая-либо иная биометрическая информация может быть общедоступной, поскольку Закон «О персональных данных» не содержит общего прямого указания о том, что любая биометрическая информация имеет ограниченный доступ.

Дефицит терминологической определенности понятия «биометрические данные» в казахстанском законодательстве выступает фактором возникновения существенных рисков в правоприменительной практике. Дефинитивная размытость и несовершенство законодательной базы создают возможности для неоднообразной интерпретации. Тезис о терминологической неопределенности понятия «биометрические данные» находит свое подтверждение при сравнительном анализе специальных актов. Отраслевое законодательство в области здравоохранения оставляет вопрос биометрии открытым. Кодекс РК «О здоровье народа и системе здравоохранения» не содержит термина либо разъяснения [145]. Императивные требования банковского законодательства о проведении биометрической аутентификации по изображению лица позволяют путем логической дедукции классифицировать изображение лица как биометрические данные, исходя из терминологии «биометрическая идентификация» и «биометрическая аутентификация» [146, п.9 ст.58; 147]. В то же время, уполномоченный орган по защите персональных данных не относит поведенческие особенности к биометрическим данным [148]. Проект Цифрового Кодекса по состоянию на апрель 2024г. в статье 60 косвенно указывает, что к биометрическим данным относятся «данные изображения, видео- и аудиозаписи; дактилоскопическая и геномная информация; информация о радужной оболочке глаза; результаты анализов ДНК и другие». В формулировках пунктов 1 и 4 статьи 48 Цифровой Кодекс РК в принятой редакции усматривается функциональная тавтологичность. Признание данных биометрическими персональными данными ставится в зависимость от их использования в целях аутентификации, которая, в свою очередь, содержательно сводится к верификации этих же данных. Это свидетельствует о семантическом дублировании смыслов, при котором процесс и объект определения взаимно подменяют друг друга. Подобная дефинитивная закольцованность в Цифровом Кодексе РК свидетельствует о том, что законодатель сужает сущность биометрии до её технической функции, создавая при этом логически замкнутую, но содержательно пустую конструкцию. Дефицит дефинитивной ясности в отношении термина «биометрические данные», отсутствие унифицированного понятия в различных законах, а также общего императивного требования об ограниченности доступа к биометрическим данным с повышенными обязательствами по защите, создают существенную правовую неопределенность для субъектов регулирования.

Ввиду отсутствия дефинитивной ясности в отношении категорий и видов персональных данных ограниченного доступа в национальном законодательстве,

обосновывается необходимость перехода к модели гармонизированного регулирования. В данной архитектуре специальный закон должен детерминировать унифицированный понятийный аппарат и базовый правовой режим для всей совокупности персональных данных ограниченного доступа, в то время как отраслевое законодательство дополняет его с учетом специфики конкретной сферы общественных отношений.

В казахстанской классификации персональных данных по типу доступности следует иметь в виду, что к общедоступным персональным данным могут относиться не только те, которые прямо указаны в законах РК, но также и те, которые стали известны в силу реализации права на доступ к информации или свободы слова. Закон «О персональных данных» в статье 9 предусматривает исключение для журналистов и масс-медиа на размещение персональных данных без согласия физического лица, что согласуется со свободой слова и правом на информацию. Далее, статьи 14 и 67 Закона РК «О масс-медиа» от 19 июня 2024 года позволяют размещать в средствах массовой информации и масс-медиа персональные данные несовершеннолетних, признанных виновными в тяжких или особо тяжких преступлениях, а также их родителей или законных представителей [149]. Публикация информации о несовершеннолетнем преступнике преследует общественный интерес в информации о противоправном деянии, нарушении общественного порядка. Однако, деятельность журналиста имеет последствием широкое распространение информации, а в современных условиях интернет-технологий такое распространение является неконтролируемым. Следовательно, опубликованные журналистами в соответствии с Законом РК «О масс-медиа» персональные данные могут стать общедоступными. Масштабы и возможности распространения информации, которыми владеют масс-медиа, эффект и последствия для общества от такого распространения часто не соразмерны тем последствиям и ущербу, которые могут быть причинены родителям и законным представителям несовершеннолетних преступников, их чести и достоинству. Публикации неопределенного объема персональных данных и широкий доступ общественности к различным масс-медиа оказывают психологический дискомфорт, моральное влияние на личность родителей и законных представителей. Кроме того, подобные публикации могут воздействовать на получение каких-либо благ, повлечь какие-либо ограничения и предвзятое отношение общественности к родителям и законным представителям, их дискриминацию. Независимо от интересов общества, права на доступ к информации, свободу слова, каждый человек имеет конституционное право на неприкосновенность частной жизни, защиту чести и достоинства, закрепленные в статьях 20 и 21 Конституции РК 2026 года. Размещение в масс-медиа персональных данных родителей и законных представителей без их согласия является чрезмерным вторжением в частную жизнь. Фактически статьи 14 и 67 Закона РК «О масс-медиа» лишают таких родителей и законных представителей автономии, возможности распоряжения личной информацией и контроля за ее

распространением. В целях сохранения баланса общественных и частных интересов законодательство не должно лишать родителей и законных представителей несовершеннолетних преступников инструментов для защиты частной жизни, чести и достоинства. В Законе РК «О масс-медиа» необходимо предусмотреть механизм, с помощью которого можно соблюсти пределы и соразмерность вмешательства в частную жизнь. К примеру, в статьи 14 и 67 Закона РК «О масс-медиа» рекомендуется включить условие о получении согласия родителей и законных представителей несовершеннолетних, в отношении которых вынесен приговор в тяжких и особо тяжких преступлениях, на размещение в масс-медиа персональных данных.

Проведенный нормативный анализ регулирования персональных данных открытого доступа в Республике Казахстан – от государственных баз до медийного пространства – свидетельствует о кризисе правоприменения и ослабляет защищенность частной сферы человека. Данный кризис является следствием концептуального дефекта, заложенного в нормативной базе: отечественное законодательство ограничивается дихотомией «общедоступные / ограниченного доступа», игнорируя другие критерии классификации персональных данных.

В отличие от казахстанского законодательства GDPR выделяет категорию *специальные* персональные данные (или *чувствительные* данные), при обращении с которыми статьями 4 и 9 GDPR тоже применяются особые требования. Чувствительные персональные данные — это подмножество персональных данных, которые считаются настолько персональными (очень личными), что для защиты от злоупотреблений при их обработке необходимы особые меры предосторожности.

GDPR относит к специальным категориям персональных данных персональные данные, раскрывающие расовую или этническую принадлежность, политические взгляды, религиозные или философские убеждения, членство в профсоюзах, генетические данные, биометрические данные, данные о здоровье, данные о половой жизни или сексуальной ориентации физического лица (статья 9). Специальные категории персональных данных также обозначены законом как «чувствительные» данные (пункт 10 Преамбулы).

Обработка специальных категорий персональных данных запрещена согласно GDPR, за исключением установленных случаев. К таким случаям относятся законом предусмотренные требования в сфере трудоустройства, социальной защиты или здравоохранения, защита жизненно важных интересов, защита юридических требований в право исполнительной и судебной деятельности, другие четко очерченные случаи при условии обеспечения баланса между защитой данных и индивидуальными правами и конкретными потребностями.

Одной из современных проблем в классификации персональных данных является различие между данными, которые могут повлиять на

конфиденциальность и благополучие человека — как в финансовом, так и в эмоциональном плане — и данными, которые не представляют такого риска. Европейский Регламент подошел к классификации персональных данных с позиции приоритета интересов человека, что ясно прослеживается в выделении на законодательном уровне чувствительных персональных данных.

Обработка чувствительных персональных данных создает риски для прав и свобод физических лиц, которые могут различаться по вероятности и серьезности. Эти риски включают потенциальную дискриминацию, кражу личных данных, финансовые потери, ущерб репутации и потерю конфиденциальности. Это также может помешать физическим лицам осуществлять контроль над своими данными, особенно когда речь идет о конфиденциальной информации, такой как расовое или этническое происхождение, политические убеждения, данные о состоянии здоровья или судимости.

Проведенный компаративный анализ выявляет принципиальное различие в классификации персональных данных в казахстанском и европейском праве. Казахстанская классификация носит технико-правовой характер и ограничивается признаком доступности, определяемым либо законом, либо самим физическим лицом. В условиях нормативной неопределенности имеет следствием противоречивую интерпретацию среди центральных государственных органов Казахстана. Европейский Регламент имеет человекоцентричный и рискориентированный подход, устанавливая классификацию персональных данных по признаку их значимости и влияния на интересы и благополучие человека.

2.2 Правовое регулирование операций с персональными данными в Республике Казахстан и зарубежом

Регулирование правоотношений в области персональных данных непосредственно направлено на осуществляемые с ними действия различными лицами и закрепление их статуса через систему прав и обязанностей. Архитектура субъектного состава в Законе «О персональных данных» базируется на четырехзвенной модели (субъект персональных данных, собственник и оператор базы персональных данных, третье лицо). Системный анализ в совокупности с Законом «Об информатизации» и Цифровым Кодексом РК выявляет превалирование вещно-правового (титульного) подхода, разграничивая роли собственника и владельца цифровых ресурсов на основе права собственности, а не исходя из их функциональной роли в процессе обработки персональных данных. Таким образом, категория *субъект правоотношения* в области защиты персональных данных носит собирательный характер, объединяющий *субъекта персональных данных*, собственника и оператора базы персональных данных, третье лицо.

Европейский Регламент, GDPR, базируется на функциональном распределении ролей (ст.4), что принципиально отличает его от казахстанской модели, ориентированной на титульное владение (собственник и оператор базы персональных данных). GDPR вводит дихотомию «контролер – обработчик», основанном на степени контроля и дискреции в отношении действий с персональными данными: контролер детерминирует цели и операции с персональными данными, а обработчик выступает в роли технического исполнителя от имени контролера. Значимым нормативным решением стало закрепление в GDPR института «совместные контролеры данных» (ст.26), что позволило устранить правовой вакуум в регулировании сложных цифровых экосистем (например, облачных услуг). Субъектную архитектуру GDPR дополняют категории «получатель» и «третье лицо», обеспечивающую четкое разграничение ролей участников информационного оборота.

Таким образом, европейская субъектная архитектура детерминруется не титульным владением базой персональных данных, а функциональной ролью субъекта, определяемой характером совершаемых им операций. Данная модель обладает высокой степенью прагматизма, поскольку правовой интерес индивида состоит в информационной безопасности и легитимности фактического использования его персональных данных, а не реализация вещного права на базу данных.

Казахстанская правоприменительная практика характеризуется устойчивым приоритетом вещно-правового (титульного) подхода над функциональным, что нередко ведет к подмене понятий и манипулированию терминологией в ущерб правам субъектов данных. Анализ судебных актов выявляет системную проблему: суды при вынесении актов апеллируют к праву собственности или владения на базу персональных данных. Фактическая роль участника в процессе обработки персональных данных игнорируется поскольку не предусмотрена должным образом законодательством.

Примером подтверждения данного тезиса является административный спор о доступе акимата к персональным данным в информационной системе без предварительного согласия [150]. Акимат утверждал, что фактическое право собственности и управление информационной системой и программой принадлежат другой компании, ответственной за сбор и обработку данных, в то время как акимат является лишь ее пользователем. Анализ суда был сосредоточен в основном на соблюдении процессуальных норм государственным органом, вынесшим протокол об административном правонарушении. В судебном акте Административный суд не осуществил критической оценки сбора и обработки персональных данных, а также обязанностей Акимата как обработчика данных. Хотя Акимат использовал терминологию, например, «собственник базы персональных данных», термин «обработчик» является более точным описанием его роли в архитектуре рассматривавшегося общественного отношения. Указанное различие имеет решающее значение для повышения ясности и эффективности

защиты прав личности в сфере защиты персональных данных. Аналогичный подход, базирующийся на приоритете титула над функцией, прослеживается в деле о привлечении председателя ОСИ за нарушение законодательства о персональных данных, выразившееся в указании персональных данных жильца в мессенджере [123]. Суд апелляционной инстанции указал, что председатель ОСИ не является собственником базы персональных данных, общедомового чата, так как чат был создан другим лицом. Суд также использовал терминологию закона о вещном праве на базу данных, в то время как данная логика игнорирует сущность цифрового правоотношения: в рамках архитектуры чата председатель фактически выступала контролером, определяющим условия доступа к информации в мессенджере [123]. Даже в случае привлечения к ответственности суды продолжают использовать вещно-правовую лексику, не учитывая функциональную специфику субъектов правоотношения. Так, производственный кооператив был привлечен к административной ответственности за нарушение законодательства о защите персональных данных путем рассылки счетов за коммунальные услуги в почтовые ящики владельцев квартир незащищенным способом, что сделало их доступными для посторонних лиц. Суд в своем решении отметил, что кооператив совершил нарушение, являясь юридическим лицом, осуществляющим право владения, пользования и распоряжения базой персональных данных. Несмотря на то, что по своей сути функционально кооператив является обработчиком данных, суд не оценивал функциональную роль кооператива и апеллировал к категориям имущественного права, что еще раз подчеркивает концептуальный разрыв между казахстанским правоприменением и европейскими стандартами [122].

Закон «О персональных данных» дифференцирует операции с персональными данными на три категории – сбор (получение), защита (меры по защите), обработка. Последняя является собирательным термином, включающим исчерпывающий перечень из девяти действий: накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных. Примечательно, что в отличие от остальных операций с персональными данными Закон «О персональных данных» не раскрывает содержание операций «изменение» и «дополнение», что предполагает их буквальное юридическое толкование.

Понятие «обработка персональных данных» в европейском GDPR более широкое в сравнении с казахстанским определением. В GDPR понятие «обработка» означает *любую операцию или набор операций*, которые выполняются с персональными данными или наборами персональных данных, независимо от того, автоматизированы они или нет. В определении также перечисляются виды операций, действий с персональными данными: сбор, запись, организация, структурирование, хранение, адаптация или изменение, извлечение, консультация, использование, раскрытие путем передачи, распространения или иного

предоставления, согласования или комбинирования, ограничения, стирания или уничтожения.

В Европе в интерпретации термина «обработка» персональных данных значительную роль сыграла правоприменительная прецедентная практика European Court of Justice (ECJ). Базовые правовые позиции, изложенные в решениях *Lindqvist* и *Google Spain*, позволили расширительно толковать обработку персональных данных, включая размещение ссылки на персональные данные другого лица в интернете и деятельность поисковых систем [151, §§27,47, §1 резолютивной части; 152, §§28,29, §1 резолютивной части]:

а) *Lindqvist*: прецедент автоматизированной публикации. В рамках данного разбирательства ECJ постановил, что указание (действие) физическим лицом ссылки на частной интернет-странице на третьих лиц и идентификация их различными способами (указание номера телефона, информации об условиях работы, увлечениях), представляет собой «обработку персональных данных полностью или частично автоматическими средствами». Более того, подобная публикация данных в Интернете становится доступной для «неопределенного числа людей».

б) *Google Spain*: концепция ответственности поисковых агрегаторов. Данный прецедент закрепил за поисковыми системами статус обработчиков персональных данных. ECJ постановил, что технологический цикл поиска осуществляется операторами поисковых систем при автоматическом, постоянно и систематическом исследовании Интернета в поисках запрошенной информации. Оператор поисковой системы осуществляет собирает, извлекает, записывает и организует данные в рамках своих алгоритмов индексации, хранит на своих серверах, впоследствии раскрывает и предоставляет информацию пользователям в виде списков результатов поиска. Перечисленные действия классифицируются как «обработка» независимо от того, что эти операции осуществляются с любыми данными, в том числе персональными, ранее размещенными в Интернете.

GDPR также выделяет такие *виды обработки* персональных данных, как «профайлинг», «псевдонимизация», «трансграничная обработка». GDPR не случайно дополнительно дает определение указанным видам обработки персональных данных и закрепляет отдельные положения и нормы поскольку современное технологическое развитие и указанные виды обработки персональных данных содержат риски для личности и для общества в целом.

Закон «О персональных данных» определяет общие условия для всех действий по обработке персональных данных, однако, категория «профайлинг» не получила в нем закрепления как самостоятельный вид операций. Фактически «профайлинг» подменяется расширительной категорией «использование персональных данных», ориентированной на реализацию целей собственника и оператора баз данных, что размывает специфику алгоритмической обработки. Тот факт, что дефиниция «профайлинг» как алгоритмов, используемых для определения предпочтений и интересов пользователя, содержится лишь в Законе

«Об онлайн-рекламе» свидетельствует о фрагментарности правового регулирования [52]. Отсутствие единой законодательной квалификации профайлинга как особого способа обработки персональных данных в профильном законе порождает дефицит процессуальных требований к его осуществлению.

На практике операции по профайлингу помогают выявить максимально правильного человека, чтобы сделать ему целенаправленное предложение. Профайлинг включает в себя обработку онлайн-поведения и предпочтений человека, таких как заказы еды, выбор одежды, покупки в интернете, привычки в путешествиях, предпочтения в туристическом размещении и развлечениях, а также другие особенности поведения и предпочтений. Эти данные помогают создать портрет личности, раскрывая подробности о характере человека, привычках, образе жизни, социальном и экономическом статусе. Лучше понимая пользователей, поставщики онлайн-услуг и продуктов могут делать целевые предложения, увеличивая прибыль и предоставляя более релевантные преимущества клиентам [125, стр.80].

Указанные целевые предложения, направляемые в коммерческой цифровой среде через веб-браузеры, различные платформы и приложения, казахстанский Закон «Об онлайн-рекламе» обозначил как «таргетированная онлайн-реклама», направляемая пользователям, выявленным в результате профайлинга. Закон запрещает использовать для профайлинга сведения о расовой или национальной принадлежности, о политических взглядах, биометрические данные, информацию о состоянии здоровья пользователя, а также персональные данные, идентифицирующие физическое лицо. Рестриктивная интерпретация казахстанского понятия «персональные данные», центрированная исключительно на прямой идентифицирующей способности отдельной единицы информации, де-факто легитимизирует тотальное наблюдение, мониторинг и анализ пользователей. Игнорирование законодателем механизмов косвенной идентификации путем синтеза отдельных данных создает условия для беспрепятственного профилирования лиц, чьи базовые идентификаторы уже интегрированы в системы онлайн-платформ. В сочетании с нормативным вакуумом в сфере негосударственного оборота биометрических персональных данных законодательство Казахстана допускает дальнейшее наблюдение онлайн-платформами за деятельностью физического лица в цифровой среде.

Закон «Об онлайн-рекламе» характеризуется высокой степенью нормативной абстракции: статьи 10 и 12 не содержат императивных требований к содержанию политик конфиденциальности и пользовательских соглашений в отношении сбора и обработки персональных данных пользователей, ограничиваясь ссылками на Закон «О персональных данных». Критическим дефектом выступает внедрение модели «презумпции согласия» на профайлинг или «opt-out» (отказ по инициативе пользователя), соответственно, закон «программирует» платформу на нарушение права на неприкосновенность частной жизни. Законодатель не ставил целью урегулировать профайлинг и защитить

конституционное право на неприкосновенность частной жизни, а скорее рассматривал его как стандарт деятельности платформ, легализовав инвазивный мониторинг частной жизни в коммерческом секторе [125, стр.81]. Таргетированная реклама в контексте Закона «Об онлайн-рекламе» трансформируется из информационного сервиса в инструмент внушения, что обуславливается отсутствием в статье 4 указанного закона превентивных принципов, направленных на обеспечение автономии и приватности пользователя.

В противовес отечественному подходу, европейское регулирование устанавливает строгий запретительный режим в отношении несанкционированных рекламных сообщений. Директива об электронной конфиденциальности (e-Privacy Directive) выступает специальным нормативно-правовым актом (*lex specialis*) по отношению к общему регламенту GDPR [46]. Квалифицируя средства автоматической коммуникации (автодозвон, e-mail, SMS) как «нежелательные сообщения» или «незапрошенные сообщения», предназначенные для прямого маркетинга, e-Privacy Directive постулирует, что подобные действия являются вторжением в частную жизнь, требующим предварительного, явного, информированного согласия физического лица (п.(40) Преамбулы). Дополнительно, статья 13 e-Privacy Directive закрепляет модель «opt-in», согласно которой отсутствие предварительного согласия на получение маркетинговых сообщений делает их противоправными.

Таким образом, казахстанское законодательство характеризуется дефицитом превентивных механизмов защиты права на неприкосновенность частной жизни от интрузивных рекламных сообщений, допуская неконтролируемое использование персональных данных широким кругом участников коммерческой рекламной среды.

Такие зарубежные ученые как, Омер Тене (Omer Tene), Кристина Касагран (Cristina Casagran) и Матиас Вермёлен (Mathias Vermeulen), Хосе Эстрада-Хименес, Н.Фурберг (N.Fourberg), Бернд Скиера (Bernd Skiera) подробно рассмотрели экосистему интернет-рекламы и процесс профилирования и таргетинга [153, стр.16; 154, стр. 349-352; 128, стр.34,35; 155, стр.16-27; 156, Sections 2,3]. Омер Тене характеризует поисковую систему Google как «базу данных намерений», которая предоставляет доступ к интересам, потребностям и личной информации пользователей [153, стр.22]. Западные исследователи отмечают, что Google стал основоположником внедрения и использования инновационных техник в профилировании пользователей, анализируя их данные и действия в Интернете, фактически «запустил экономику слежки» для улучшения своего рекламного бизнеса [10, стр.19]. Имдад Уллах (Imdad Ullah) проводит структурно-функциональный анализ профилирования пользователей, сбор данных и механизмы доставки и показа рекламы [157]. Автор раскрывает архитектуру типичной рекламной экосистемы, включающей рекламодателей, рекламные агентства, рекламные сети, аналитические компании, издателей и конечных потребителей. И.Уллах иллюстрирует, как участники экосистемы

взаимодействуют между собой посредством технологических цифровых инструментов. Мобильные приложения и аналитическое программное обеспечение сообщают об активности пользователей и отправляют запросы на рекламу в сети, которые агрегируют и анализируют данные, монетизируют показы и управляют рекламными кампаниями. Таким образом, происходит обмен персональными данными между различными сторонами экосистемы, создаются сложные профили пользователей, которые реализуются как объект рыночного оборота с помощью алгоритмических аукционных механизмов [128, стр.36].

Мобильные приложения и Интернет стали неотъемлемой частью современного общества, и пользователи проводят в них значительное время. Это приводит к появлению «нечеловеческих наблюдателей» в рекламной экосистеме, которые осуществляют латентное аккумулирование и обмен персональными данными, что приводит к обширным знаниям о повседневной жизни людей [4, стр.356]. В результате отслеживаемый человек может стать «прозрачным гражданином» или «чрезвычайно известным гражданином», а алгоритмы профилирования могут предоставлять информацию, которая позволяет участникам экосистемы сформировать высокодетализированные, всесторонние цифровые профили пользователей, превосходящие осознанные когнитивные способности личности [153, стр.22; 7, стр.359; 158, стр.3].

Зарубежные ученые утверждают, что целевая реклама и профилирование вторгаются в частную жизнь из-за навязчивых методов работы с данными и постоянного наблюдения, влияя на поведение пользователей [159]. Напротив, коммерческие участники экосистемы утверждают об абсолютном отсутствии вторжения в частную жизнь, поскольку в их деятельности в преобладающей степени эксплуатируются анонимные или псевдонимизированные данные, которые соответствуют законам о защите данных и напрямую не идентифицируют пользователей. Тем не менее, концептуальное единство ученых проявляется в том, что в содержательном плане процесс «выделения» кого-либо подразумевает идентификацию, даже без атрибуции имени личности к ее данным, а высокотехнологичные современные инструменты, включая искусственный интеллект, позволяют генерировать результаты с высокой степенью детализации и точности [20, стр.17, 31].

Пользователь Интернета становится потенциальной целью с помощью сбора и анализа личной информации, что приводит к потере анонимности, которая является ключевым аспектом конфиденциальности. Н.Пуртова утверждает, что таргетинг направлен на более глубокую индивидуализацию и персонализацию, она вводит термин «Т-идентификации», которая позволяет проводить уникальное профилирование [23, стр.168, 169]. Использование современных персональных устройств, мобильных телефонов, планшетов, компьютеров и других портативных электронных устройств, позволяет получить высокоточную идентификацию пользователя, а вместе с современными техническими возможностями может

потребовать признания фундаментального права на анонимность [160, стр.472; 126].

В условиях перманентного присутствия личности в цифровой среде, доступности личной информации, использование инструментов высокой идентифицируемости ограничивают возможности индивида оставаться "неразличимым" в цифровой среде [161, стр.147]. Подвергаясь цифровому анализу и экстрагированию на основе собранной персональной информации, физическое лицо утрачивает субъектную анонимность, а также контроль над своими данными, что нарушает его право на неприкосновенность частной жизни.

Современные технологии профайлинга и таргетинга содержат угрозу свободе личности действовать в собственных интересах и принимать независимые решения без какого-либо влияния и манипуляций, тем самым вторгаясь в личную автономию, право на защиту персональных данных и право на неприкосновенность частной жизни. Однако, профайлинг и таргетинг сопряжены с рисками нарушения других прав и интересов личности, общества и государства, поскольку направлены на идентификацию лица с целью оказать воздействие на его решения и поведение. В рамках рассматриваемой проблемы следует учесть, что аналитическая детализация поведенческого профиля обеспечивает высокую точность интерпретации когнитивных установок и склонностей личности. Сбор и анализ персональных данных о предпочтениях, вкусах, убеждениях, действиях, поведении, решениях пользователей из социальных сетей, с различных платформ и приложений, позволяет идентифицировать и анализировать поведенческие черты человека для генерации его высокоточного поведенческого профиля [162, стр.78-81]. Вследствие этого алгоритмические механизмы реализуют стратегии персонализированного воздействия, предоставляя субъекту контент, который актуализирует его внутренние интенции и детерминирует его выбор в пользу определенных моделей поведения, в том числе с помощью техник манипулирования.

Операции по профилированию и созданию цифровых портретов пользователей с помощью алгоритмов влияет на их поведение [10, стр.37]. Работы зарубежных исследователей демонстрируют, что в цифровой среде воздействие на поведение человека возможно в любой сфере жизни, коммерческой, политической, социальной. Джейк Голденфейн (Jake Goldenfein) утверждает, что ««код» [программирует] рациональное поведение [человека] для достижения определенных целей» [158, стр.161]. Эли Паризье (Eli Pariser) отметил, что программный код «сам определит, что смотреть, читать и видеть» [163, стр.51]. К.Касагран и М.Вермёлен описывают методы профилирования и инструменты микротаргетинга, чтобы выявить и достичь физических лиц для участия в политической кампании [154]. Ученые единогласны, что автономия личности находится под угрозой вмешательства со стороны техник профилирования. Целенаправленная реклама или профилирование подвергают субъекта данных риску манипулирования или возникновения аддиктивного поведения, такого как

зависимость от азартных игр, вредные привычки, сверхурочное вождение и другие виды поведения, которые могут причинить вред субъекту данных. Таким образом, современные технологии сбора и обработки информации о человеке, профилирование и таргетирование могут иметь следствием нарушение фундаментальных прав и свобод человека, включая честь и достоинство.

Защита человеческого достоинства и репутации приобрела новый виток развития с ростом использования населением интернет-технологий и социальных сетей. Объем информации, который пользователи размещают и распространяют в интернете, обладают потенциалом «разрушить жизнь за считанные минуты» [7, стр.361]. В онлайн-среде «право на неприкосновенность частной жизни... призвано предвещать широкую защиту достоинства человека и неприкосновенность прав личности» [7, стр.165]. Д.Голденфейн утверждает, что «защита личности не обязательно связана с распространением частной информации», не всегда касается человеческого достоинства или клеветы [158, стр.6]. Угрозы защите личности могут иметь разнообразные формы и последствия. Помимо репутационных рисков развитие цифровых масс-медиа и коммуникационных технологий, скорость распространения информации и ее легкая доступность актуализировали угрозы киберпреследования и несанкционированной диссеминации сексуализированного контента, а также утраты профессионального статуса и академических санкций [7, стр.361].

Профилирование может быть использовано критически вредным образом и повлечь за собой высокие риски для жизни человека. В течение продолжительного времени в научном дискурсе не получала концептуализации проблема законности сбора и обработки данных и рисках неправомерного использования массива пользовательских данных, которые хранятся рекламными платформами и передаются другим участникам рекламного рынка [128, стр.36]. В работах И.Уллах подчеркивается потенциал деструктивных субъектов экстракции идентификатора устройства и в дальнейшем посредством фальсифицированного программного обеспечения, имитированного рекламного контента, несанкционированного перехвата информационных потоков в сетях коммуникаций получить доступ к конфиденциальной информации пользователя [157, стр.657]. Хосе Эстрада-Хименес (José Estrada-Jiménez) и другие ученые отмечают, что сложная конструкция архитектуры рекламной экосистемы с участием множества посредников, обменивающихся данными пользователей, объективно детерминируют тесную взаимосвязь между конфиденциальностью данных и информационной безопасностью [128, стр.37].

На современном этапе развития цифровой среды угрозы нарушений конфиденциальности ассоциируются главным образом с утечкой и несанкционированным использованием данных третьими лицами, а обеспечение защиты данных преимущественно направлена на применение технологического инструментария [98, стр.51]. Именно поэтому возникает объективная необходимость ужесточения регуляторных правил информационной безопасности

как превентивную меру надежной защиты персональных данных. Документы ранее функционировавшего европейского регулятора, A29WP, особо выделяли обязательства издателей, рекламных сетей, рекламодателей по установлению соответствующих инструментов безопасности и технических мер для сбора, хранения, удаления персональных данных [164, стр.24-28; 165, стр.12-21; 24, стр.761,765].

При всей значимости технологической защиты персональных данных критически важно сохранять акцент на правовой природе охраняемых ценностей. Исследование К.Касагран, посвященное персональному микротаргетингу, подчеркивает, что существующие модели оценки рисков фокусируются на качестве и безопасности данных, упуская из виду характер защищаемых интересов и принцип законности из-за отсутствия согласия пользователя и неадекватной идентификации контролеров и обработчиков данных [154]. А.Мантелеро поддерживает ее позицию, утверждая, что помимо внимания к информационной безопасности, применению новых технологий и широкому спектру деловых операций необходимо переосмыслить возможные последствия и ущерб правам и свободам человека [24, стр.763, 764]. Профилирование и таргетирование имеют более далеко идущие последствия для других фундаментальных прав, поскольку право на неприкосновенность частной жизни тесно связано с другими ценностями.

Алгоритмическая систематизация поведенческих характеристик личности в цифровой среде выступает фундаментальной базой для последующей реализации стратегий поведенческой рекламы. Исследователи отмечают, что поведенческая реклама несет в себе риски нарушения прав и свободы личности, с неопределенным или возможным в будущем вредом без детализации, как такая перспектива влияет на фундаментальные права и свободы. Нарушение правил о защите персональных данных чаще связывают с защитой репутации, чести и достоинства. Однако, ученые, регуляторы и пользователи также связывают профилирование как предпосылку для нарушения права на недискриминацию. Материалы Агентства Европейского Союза по фундаментальным правам иллюстрируют нарушения права на недискриминацию [166]. Органы по защите данных подчеркивают, что поведенческая реклама в онлайн-среде, автоматическое принятие решений и профайлинг могут «увечивать существующие стереотипы и социальную сегрегацию», а также повысить риск предвзятости [25, стр.13].

Положения национальных законов в основном сосредоточены на традиционных условиях дискриминационной практики (например, раса, цвет кожи, пол, язык, религия, политические взгляды), в то время как современная «алгоритмическая дискриминация основана на более размытых и менее четких категориях» [25, стр.765]. Сегодня дискриминация затрагивает также «потребительскую роль субъекта данных в коммерческой отрасли» [160, стр.459]. На основе собранных данных, однозначно идентифицируя и классифицируя пользователей различные организации-посредники дифференцируют модели поведения пользователей [128, стр.45]. Поскольку в логику функционирования

алгоритмов заложена возможность создавать кластеры, группы людей, А.Мантелеро прогнозирует переход дискриминации с индивидуального уровня на групповой уровень [24, стр.763]. А.Мантелеро акцентирует внимание более широком влиянии профилирования на общество, так как кластеризация людей и профайлинг создают серьезные риски не только для права на недискриминацию, но и для права на неприкосновенность частной жизни, на образование, на равенство перед законом, для свободы передвижения, мысли, выражения мнений, собраний и свободы на рабочем месте [24, стр.762].

Дискриминационная практика, основанная на профилировании, может иметь негативные социально-политические последствия. Поскольку профилирование связано с автоматической обработкой данных, алгоритмический инструментарий позволяет сегментировать группы людей в экономических, социальных целях, в том числе для достижения политических результатов. Сегрегация или фильтрация лиц по причине поведенческого эффекта удобна при поиске кандидатов для работодателей, для общественных организаций при продвижении определенных социальных интересов, для государства при назначении социальных выплат и так далее. В своем исследовании Сара Эго иллюстрирует дискриминационное влияние профилирования на трудоустройство, получение социального обеспечения, страхования, кредитов, доступа к медицинскому лечению для американских граждан в результате вторжения в частную жизнь со стороны правительственных и коммерческих организаций [7]. Кэтрин Галанис (Kathryn Galanis) также демонстрирует дискриминационный эффект алгоритмической сегментации и таргетинга в сфере занятости, социальной и политической жизни общества [167].

В условиях современной цифровой трансформации оперирование массивами данных и механизмы алгоритмического профилирования становятся конституирующим фактором реализации экономических и политических целей. Политические кампании коммуницируют «удобную» информацию для целевой узкой группы (микротаргетинг) и влияния на электорат, тем самым манипулируя правом на информацию и подрывая демократию. К.Касагран и К.Велис акцентируют внимание на риске, создаваемом профилированием для общества и демократии. Техники таргетинга «могут действовать как вектор дезинформации, могут использоваться для усиления поляризации электората, а также идентификации и воздействия на слабые места» с целью воздействия на уязвимые группы [154, стр.349]. Таким образом, влиятельные организации манипулируют восприятием и убеждениями, воздействуя на людей, чья автономия слаба [10, стр.37]. Более того, как утверждает К.Велис, идентификация, персонализация и таргетинг могут представлять собой угрозу национальной безопасности, демократии, свободному обществу и безопасности отдельных лиц [10, стр.46-54]. Она отмечает угрозы национальной безопасности, поскольку неконтролируемый доступ к личным данным позволяет «выявлять потенциальные цели для вербовки лиц в качестве шпионов» [10, стр.47].

Латентный характер алгоритмических инструментов профилирования, применяемые широким кругом участников цифрового пространства, формируют значительный вектор угроз, связанный с их эксплуатацией криминальными и экстремистскими структурами для манипуляции уязвимыми группами населения и несовершеннолетними, детерминируя эрозию фундаментальных прав и подрыв государственного суверенитета. Риски для прав и интересов личности, общества и государства усугубляются современным развитием технологий искусственного интеллекта [168, стр.3]. Таким образом, методы профилирования, выявления и определения субъектов влекут за собой риски для других прав и свобод человека и общества.

Прецедентная практика ЕСПЧ демонстрирует взаимосвязь защиты персональных данных, в том числе операций по профилированию, с другими фундаментальными правами и свободами, защищаемыми Конвенцией о защите прав человека и основных свобод. Прецедентная практика ЕСПЧ содержит значительное количество дел о нарушении статьи 8 Европейской Конвенции, которая защищает право на уважение частной и семейной жизни и распространяется на персональные данные.

Иллюстрацией того, как механизмы профилирования могут приводить к нарушению фундаментальных прав служат два случая о составлении сотрудниками полиции профилей на основе этнических критериев и в связи с правом на недискриминацию [169; 170]. По мнению ЕСПЧ, профилирование на основе физических или этнических характеристик может сказаться на репутации и самоуважении человека; привести к стигматизации и чувству унижения [169, §§25,26]. Суд акцентировал, что при обработке сведений об этнической принадлежности лица «власти должны обеспечить уважение без дискриминации фундаментальной ценности» [169, §33].

Профилирование по данным о прекращенных уголовных делах, погашенных и снятых судимостях также касается дискриминационной практики при приеме на работу, когда на основании данной информации лиц либо увольняли, либо отказывали в приеме на работу [171]. В прецедентной практике ЕСПЧ о незаконном доступе к медицинским данным и профилировании на их основе также демонстрируется дискриминационный эффект в трудовых правоотношениях, влекущих утрату профессионального статуса [172].

Дело *Catt v the UK* показывает, как вмешательство в частную жизнь путем неправомерного профайлинга человека как экстремиста и хранения личных данных связано с реализацией свободы собраний и ассоциаций, а также свободы выражения мнений [173].

Вмешательство в частную жизнь и осуществление свободы выражений мнений демонстрируется в споре *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [93]. Запрет финским медиа-компаниям распространять персональные налоговые данные, включая подробности налогооблагаемого дохода и активов в том числе самых богатых граждан, был признан ЕСПЧ правомерным, так как

подобная информация не способствует дебатам общественного интереса и не защищается свободой выражения мнения (ст. 10 Конвенции) [93, §§178,198]. ЕСПЧ подчеркнул, что обработка персональных данных, предназначенных для публикации в газете, массовый сбор и широкое распространение данных выходят за рамки исключительно журналистской обработки. Более того, распространенные сведения налогоплательщиков могут стать элементом, своего рода «ингредиентом», для профилирования людей по суммам уплаченных налогов, имеющимся доходам и имуществу. Публикация такой информации могла использоваться в качестве критерия для составления профиля и явно касалась частной жизни этих лиц. В таком случае права человека превалируют над общественными интересами. В отношении публикации данных о налогообложении дело *L.B. v Hungary* демонстрирует, что ненадлежащая обработка данных «может повлиять на репутацию человека и его отношения с органами власти», «вызвать общественное неодобрение и привести к стигматизации субъекта данных» [90, §§51,52]. Личная информация, предоставленная государственными органами в открытый доступ, позволяет «составить профиль относительно благосостояния человека, [произведенных инвестиций]», материального и финансового положения человека [90, §53]. Более того, публикация домашнего адреса влечет за собой риски для безопасности членов семьи человека [90, Concurring Opinion of Judge Küris §§11,25,27].

Судебная практика ЕСПЧ также демонстрирует, что профилирование и выделение отдельных лиц или их групп на основе типа используемой личной информации влечет за собой риски для других основных прав и свобод.

Нормативно-сравнительный анализ регулирования профайлинга в Казахстане позволил выделить два критических отличия от GDPR. Во-первых, GDPR определяет профайлинг как любую автоматизированную обработку персональных данных, в то время как Законы «О персональных данных» и «Об онлайн-рекламе» содержат менее ясные положения. Во-вторых, GDPR содержит четкие правила о том, как определенная информация и идентификаторы используются для распознавания и понимания людей, их выделения и выбора. В пункте (30) Преамбулы и статье 4(4) GDPR устанавливается, что онлайн-данные, идентификаторы и онлайн-«следы» помогают формировать представления о производительности труда человека, финансовом положении, здоровье, предпочтениях, интересах, надежности, поведении, местоположении и перемещении. Такое отсутствие ясности в казахстанских законах наделяют контролеров и обработчиков данных дискрецией действий, что потенциально ставит под угрозу права и свободы лиц [125, стр.81]. Угрозы фундаментальным правам и свободам личности в национальном контексте интенсифицируются ввиду существующей правовой асимметрии: объем правомочий казахстанских субъектов данных остается существенно лимитированным в сопоставлении с высокими европейскими стандартами защиты приватности. В отличие от GDPR, устанавливающего императивные требования к транспарентности

автоматизированных процессов принятия решений и наделяющего правом возражать против профайлинга и прямого маркетинга, казахстанский Закон «О персональных данных» до недавнего времени ограничивал информирование субъектов лишь случаями прямого влияния на их права. Реформирование национального законодательства в связи с принятием Закона «Об искусственном интеллекте» в ноябре 2025 года сократило регуляторный разрыв с GDPR, внедрив обязанности собственников и операторов разъяснять порядок и потенциальные последствия автоматизированной обработки, а также законодательное закрепление права на возражение против такой обработки. Тем не менее, несмотря на сближение национальных стандартов с европейской моделью защиты приватности, вне поля нормативного регулирования в Казахстане остается обязанность контролеров данных оценивать влияние обработки персональных данных на права или свободы лиц, что приводит к отсутствию подотчетности. Дополнительным фактором угрозы правам и интересам физических лиц служит отсутствие обязательств собственников и операторов баз персональных данных и уполномоченного органа в области защиты персональных данных по повышению информированности и правовой грамотности субъектов данных [125, стр.87].

Операции по уничтожению и обезличиванию персональных данных.

В период пандемии COVID-19, совершение онлайн покупок и развитие сервисов доставки значительно возросло, население стало активнее использовать интернет и передавать свои данные различным онлайн-сервисам. Наряду с конструктивным социальным эффектом технологии также стали инструментом злоупотреблений в целях причинения вреда физическим лицам, в особенности финансового ущерба. Необходимость минимизации рисков мошенничества стала катализатором актуализации вопросов информационной безопасности среди граждан, обуславливая необходимость внедрять практику удаления своих данных в интернете. Так, например, в период пандемии COVID-19 казахстанское население чаще обращалось с требованиями удалить персональные данные, размещенные на различных сайтах в открытом доступе [174].

Платформа Открытого диалога eGov получила многочисленные запросы на удаление персональных данных. Однако существуют опасения относительно того, как эти запросы обработаны. Государственные органы указали, что при отправке запроса на платформе пользователи «по умолчанию» соглашаются с условиями использования платформы о том, что их персональные данные (полное имя) и содержание запроса будут общедоступны [175, 176, 177, 178]. Ответные действия платформы Открытого диалога eGov по запросам граждан сохранили в запросах некоторые данные, такие как имена, номера телефонов и индивидуальные идентификационные номера (ИИН), и эти сведения по-прежнему остаются доступными. Разработанная и предложенная нами ранее концепция интеграции института «псевдонимизации» в практику обработки обращений граждан на платформе eGov приобретает особую актуальность в современных цифровых реалиях [179]. Нами было обосновано, что имплементация положений статьи 4(5)

GDPR позволит защитить авторов запросов, не лишая сами обращения их содержательной ценности для общества. В то же время, констатируя нормативное отсутствие «псевдонимизации» персональных данных в действующем казахстанском законодательстве, в своих предыдущих трудах мы акцентировали внимание на концептуальное смешение данного процесса с безвозвратным обезличиванием данных, что существенно ограничивает гибкость правового регулирования [179; 180, пункт 21].

Иллюстрацией указанного дефицита регулятивной гибкости служат предписания статьи 17 Закона «О персональных данных», где законодатель императивно фиксирует перечень оснований для применения операции по обезличиванию персональных данных. Согласно данной норме, обезличивание осуществляется в целях статистических, социологических, научных, маркетинговых исследований, а также при осуществлении аналитической деятельности государственными органами. Ключевым дескриптивным признаком операции по обезличиванию персональных данных выступает безвозвратная утеря связи с личностью и техническая невозможность реставрации исходных идентификаторов. При этом Закон «О персональных данных» воздерживается от регламентации процедур сокрытия данных в иных правовых режимах, что формально легитимизирует, но регулятивно не обязывает собственников и операторов баз данных осуществлять данную операцию с персональными данными для других целей. Следовательно, в запросах Открытого диалога eGov личные данные граждан объективно могли и должны были подвергаться операции по обезличиванию. Однако в реальности констатируется формально-догматическая интерпретация положений Закона «О персональных данных» государственными органами: рестриктивное правоприменение искусственно снижает потенциал защиты приватности, сводя ее лишь к нормативно закреплённому перечню целей обезличивания.

Закон «О персональных данных» является специальным правовым актом, регулирующим операции по обезличиванию. Но в отношении сбора и обработки персональных данных и операции по обезличиванию в целях статистических исследований возникает правовая неопределенность. В особенности нормативная фрагментированность прослеживается при осуществлении переписи населения, которая является видом статистической деятельности по сбору первичных статистических данных.

Закон РК от 19 марта 2010 года № 257-IV «О государственной статистике» (п.1 статьи 8) закрепляет в отношении первичных данных физических лиц режим априорной конфиденциальности, подразумевающий ограничение доступа и защиту от разглашения. В то же время статья 17 Закона «О персональных данных» вводит императивное требование об обезличивании персональных данных уже на стадии их сбора для статистических целей. Возникает правовой парадокс: требование об обезличивании в момент первичного получения данных ставит под сомнение техническую возможность проведения переписи, где

идентификация субъекта является необходимым условием качества выборки. Несмотря на закрепленный статьей 3 Закона «О персональных данных» приоритет специальных норм в области персональных данных, неопределенность в отношении режимов конфиденциальности и обезличивания порождает правоприменительную проблему: следует ли рассматривать перепись как особый правовой режим, где защита обеспечивается не уничтожением идентификационных связей (обезличиванием), а строгим ограничением доступа (конфиденциальностью)? Решением указанной проблемы представляется законодательное признание переписи населения как особого правового режима, где идентификация субъекта на стадии сбора является правомерной при условии обеспечения абсолютной конфиденциальности на последующих этапах.

Существует и другая правовая неопределенность между указанными законами, связанная с переписью населения. Согласно Закону «О государственной статистике» и Правилам проведения национальных переписей следует, что первичный сбор информации для целей национальной переписи осуществляется переписным персоналом и интервьюерами, привлекаемыми уполномоченным органом на договорной основе [181]. При этом Законом «О государственной статистике» и Правилами не установлены конкретные требования к переписному персоналу и интервьюерам, их права и обязанности в связи со сбором и обработкой персональных данных респондентов. Нет также положений в самом Законе «О государственной статистике» об обязательности соблюдения требований Закона «О персональных данных» относительно сбора и обработки личной информации. Закон «О персональных данных» не требует согласия физического лица на сбор и обработку персональных данных для статистических целей, но данное требование не означает, что персональные данные для статистических целей выводятся из-под защиты Закона и статьи 18 Конституции 1995 года. Статус государства как монопольного субъекта в области государственной статистики, а также собственника и оператора базы персональных данных, детерминирует необходимость соблюдения правовых, технических и организационных мер. Тем не менее, при проведении переписи населения наблюдается институциональная недостаточность организационно-правового сопровождения, что свидетельствует о существенном разрыве между законодательными требованиями и их практическим воплощением.

Сопоставление операции по псевдонимизации Европейского Регламента GDPR и операции по обезличиванию казахстанского Закона «О персональных данных» демонстрирует различные последствия и результат указанных действий с персональными данными. Обезличивание приводит к безвозвратности персонализации данных и невозможности идентифицировать лицо. Псевдонимизация персональных данных, напротив, сохраняет возможность определить связь с конкретным лицом, но только при условии наличия дополнительной информации о нем. Требования GDPR по защите данных распространяются и на псевдонимизированные данные, и на дополнительные

сведения о лице. Императив GDPR о раздельном хранении псевдонимизированных данных и идентифицирующих сведений направлен на исключение возможности их неуполномоченного объединения и сопоставления с целью идентификации лица. Тот факт, что казахстанское законодательство (в редакции до апреля 2023 года) содержало аналогичные требования к раздельному хранению применительно к обезличенным данным, позволяет констатировать концептуальное смешение двух различных правовых институтов. Настаивая на раздельном хранении и детальном описании алгоритмов стойкости к различным атакам, национальный законодатель, по сути, наделил «обезличивание» признаками псевдонимизации, ошибочно отождествив необратимый процесс утраты связи с личностью и техническую процедуру временного сокрытия идентификаторов [180, пункт 22]. Резюмируя вышеизложенное, следует подчеркнуть концептуальное различие операции обезличивания и «псевдонимизации», для которых GDPR устанавливает различные режимы регулирования. Казахстанский законодатель исключил операцию по псевдонимизации из предмета правового регулирования, ограничившись институтом обезличивания, что определяет отсутствие сопоставимых правовых гарантий и стандартов безопасности для таких. Псевдонимизация как действие с персональными данными и обязательные требования к нему отсутствуют в казахстанском праве. Отсутствие в казахстанском законодательстве операции «псевдонимизация» при наличии исчерпывающего перечня оснований для обезличивания создает нормативный тупик, вынуждающий операторов данных прибегать к уничтожению или длительному хранению данных и мнимому обезличиванию. В результате для субъекта данных сохраняется угроза оставаться узнаваемым в базе данных, а значит, уязвимым перед злоупотреблениями.

Компаративный анализ европейских стандартов и отечественного законодательства, предпринятый в более ранних публикациях, позволил выявить принципиальный онтологический разрыв в трактовке правовой природы модифицированных данных [179]. В отличие от казахстанских норм об обезличивании, Европейский Регламент исходит из презумпции потенциальной идентифицируемости лица до тех пор, пока сохраняется изолированная связующая информация. Как обосновывалось ранее, сведения, прошедшие процедуру псевдонимизации, не утрачивают статус персональных данных и остаются в периметре строгой правовой охраны [179]. Связано это с тем, что пункт 26 Преамбулы GDPR императивно предписывает учитывать любые разумно вероятные технические и организационные способы косвенного или опосредованного установления личности. Более того, европейская регуляторная модель накладывает на контролеров и операторов данных сквозную универсальную обязанность по внедрению «псевдонимизации» в качестве базовой защитной превенции, которая носит общий характер и не зависит от телеологических установок или целей обработки. В развитие этой сформулированной ранее идеи следует подчеркнуть, что использование

алгоритмов псевдонимизации при модерации публичных запросов на платформе *Открытого диалога* eGov позволило бы эффективно защитить приватность авторов обращений. При этом полностью сохранилась бы общественная, аналитическая и научно-практическая ценность содержания самих запросов. На фоне принятия Цифрового Кодекса РК, который в итоге воздержался от нормативной регламентации псевдонимизации, данный научно-практический вывод приобретает статус нерешенной, но крайне актуальной системной проблемы.

Право на удаление в казахстанском законе предусмотрено как право на уничтожение персональных данных, предполагающее невозможность восстановления персональных данных. Закон «О персональных данных» предусматривает случаи, при которых персональные данные подлежат уничтожению. Европейский Регламент закрепляет схожее право, сформулированное именно как «право на удаление», а не «право на уничтожение», и аналогичные основания для удаления персональных данных. Однако, в отличие от казахстанского права об удалении персональных данных GDPR *расширяет* это право путем возложения обязанности на контролера данных не только удалить персональные данные, которые он сделал общедоступными, но и проинформировать других контролеров, обрабатывающих эти данные, о запросе физического лица на удаление персональных данных. Это право получило широкую известность после судебного дела *Google Spain* как «право на забвение», означающее что конкретный контролер данных, во-первых, сам должен удалить ставшие публичными личные данные физического лица, и, во-вторых, осуществить разумные действия, способствующие удалению ссылок на эти персональные данные, в том числе путем обращения к другим контролерам об удалении любых ссылок на эти персональные данные, а также их копий или репликаций [152]. Иными словами, «право на удаление» в европейском законодательстве включает «право на забвение», которое расширяет обязательства в отношении объекта и субъектов удаления.

Операции по обработке персональных данных имеют схожее регулирование в казахстанском и европейском праве, однако, европейское законодательство представляется более конкретным в описании действий с персональными данными, обогащено прецедентной практикой и правоприменительной практикой среди населения и уполномоченных органов. Проведенный сравнительный анализ Закона РК «О персональных данных» и GDPR приводит к следующим выводам:

1. Казахстанский закон не обеспечивает должной транспарентности операций по обработке, ограничиваясь формальным перечислением прав и обязанностей сторон без раскрытия их фактического содержания. Сравнительный анализ с GDPR показывает, что отсутствие в национальном праве четкой детализации того, как именно оператор должен выполнять свои обязательства, порождает устойчивую правовую неопределенность. Практическим подтверждением данного тезиса выступает потребность субъектов в

дополнительных разъяснениях регулятора относительно сущности операций по сбору, обработке и использованию данных, включая трансграничную передачу. Устранение указанных пробелов через внедрение детальной правовой регламентации представляется обязательным условием для минимизации рисков неверного толкования и повышения уровня защищенности частной жизни.

2. Казахстанское законодательство не содержит подробного регулирования профайлинга и таргетированной рекламы, автоматизированной обработки. Нормы и положения о профайлинге, таргетированной рекламе и автоматизированной обработке ограничены, имеют целью констатацию запрета на причинение вреда правам и интересам человека, без ясного и детального регулирования процесса профайлинга, задействованных данных и процесса идентификации личности и степени идентификации. Отсутствие в законодательстве РК императивных требований к содержательному наполнению политик конфиденциальности и критериям допустимости в отношении таргетированного контента формирует условия для неограниченного регуляторного усмотрения собственников и операторов баз данных и онлайн-платформ. Несмотря на точечные гарантии, закрепленные в Законе «Об онлайн-рекламе», отсутствие системного законодательного запрета на систематический мониторинг и профайлинг («по умолчанию») де-факто легитимизирует перманентное наблюдение за пользователями в цифровой среде, что нивелирует конституционные принципы неприкосновенности частной жизни и защиты персональных данных вследствие фактического допущения всеобъемлющего профилирования личности без надлежащих правовых преград.

3. Казахстанское законодательство характеризуется отсутствием операции «псевдонимизация», ограничиваясь операцией «обезличивания», которая имеет рестриктивный характер и узкое целевое применение. Данная нормативная ограниченность усугубляется выраженной правовой неопределенностью в сфере статистических исследований. Она проявляется в отсутствии четких правовых алгоритмов анонимизации данных непосредственно в момент их сбора, дефиците императивных требований к деятельности переписного персонала как временных распорядителей персональных данных, в наличии противоречий между законодательством о персональных данных и государственной статистике относительно конфиденциальности первичных статистических данных.

Проект Цифрового Кодекса РК по состоянию на апрель 2024 ознаменовал попытку модернизации понятийного аппарата через внедрение новых дефиниций, таких как анонимизация, псевдоанонимизация, распространение персональных данных по типу доступности источника информации, деперсонификация [132]. Однако новая терминология и стремление законодателя к детализации операций по обработке данных могли привести к избыточности терминологии, лишенной четкой семантической демаркации. В положениях проекта Цифрового Кодекса наблюдалось смешение правовой природы смежных процессов (обезличивания, анонимизации и деперсонификации), что порождало закономерный вопрос об

идентичности правовых последствий этих операций и имело потенциал нивелировать определенность и предсказуемость правового регулирования защиты персональных данных.

В принятой редакции Цифрового Кодекса не содержит нормативных новелл в части регламентации видов операций по обработке или использованию персональных данных. Вопросы профилирования (профайлинга) и псевдонимизации персональных данных остаются вне поля правового регулирования Цифровым Кодексом, сохранив таким образом существующие проблемы и стагнируя актуализацию законодательного регулирования, отвечающего современному технологическому развитию.

2.3 Специальные принципы законодательства о персональных данных в Республике Казахстан и зарубежом

Одной из проблем казахстанского регулирования является правовое закрепление принципов сбора и обработки персональных данных в Законе «О персональных данных», которые отличаются от принципов, закрепленных европейскими источниками права.

Статья 14-3 Закона РК «О правовых актах» закрепляет, что законом устанавливаются принципы, на основе которых осуществляется регулирование конкретных общественных отношений, с раскрытием конкретных механизмов их реализации [182]. Принципы имеют приоритет и прямое действие в случае противоречия им иных норм законов.

В теории права принципам отдается первостепенное значение, так как они являются исходными началами, выражают основополагающие, «сквозные и генеральные» идеи, в которых выражается общий «дух» и направленность правового регулирования. [183, стр.5] Принципы либо основаны на общем смысле законов, либо прямо изложены в законе для устранения пробелов в правовом регулировании общественных отношений.

В статье 5 Закона «О персональных данных» сформулированы пять принципов сбора и обработки персональных данных: соблюдения конституционных прав и свобод человека и гражданина, законности; конфиденциальности персональных данных ограниченного доступа; равенства прав субъектов, собственников и операторов; обеспечения безопасности личности, общества и государства. Принципы соблюдения конституционных прав и свобод человека и гражданина, законности, обеспечения безопасности личности, общества и государства являются *общеправовыми* принципами поскольку свойственны всем отраслям права и праву в целом. Принцип конфиденциальности персональных данных ограниченного доступа и принцип равенства прав субъектов, собственников и операторов являются *специальными* для регулирования отношений в сфере защиты персональных данных.

Отсутствие в профильном законе содержательного раскрытия нормативных принципов предопределяет возникновение серьезных правоприменительных барьеров, на что обоснованно указывается в совместном исследовании С.Б.Ахметовой и соавторов [184].

В частности, практическое воплощение *принципа конфиденциальности персональных данных ограниченного доступа* наталкивается на отсутствие чётких законодательных критериев и системного перечня таких сведений. Данная проблема усугубляется дуалистической природой самих оснований для сужения доступа, который детерминируется либо дискреционным волеизъявлением самого физического лица, либо императивными нормами права. В отсутствие унифицированной нормативной спецификации персональных данных ограниченного доступа принцип конфиденциальности персональных данных ограниченного доступа лишается предсказуемости, что препятствует формированию транспарентных ориентиров как для самих физических лиц, так и для любых участников информационного оборота.

Вместе с тем, *принцип равенства прав субъектов, собственников и операторов* является неэффективным в правоотношениях о персональных данных из-за глубокой асимметрии их правового статуса. В рамках данных правоотношений физические лица выступают априорно слабой стороной, не обладающей сопоставимыми с государством или коммерческими организациями экономическими и технологическими преимуществами и ресурсами. Концентрация властных и инфраструктурных возможностей у собственников и операторов позволяет им осуществлять обширный сбор персональных данных. Подобный дисбаланс возможностей и технологический перевес собственников и операторов баз данных превращает обработку персональных данных в латентный, неконтролируемый процесс, нивелируя саму идею паритетности сторон.

Таким образом Закон «О персональных данных» включает как общие, так и специальные принципы защиты персональных данных, однако толкование и применение этих принципов вызывают трудности.

Европейская нормативная модель характеризуется ясностью и детализацией принципов, регулирующих сбор, обработку и защиту персональных данных. Статья 5 GDPR устанавливает 7 принципов обработки персональных данных и раскрывает их значение:

- *Принцип законности, справедливости и прозрачности* предписывает осуществлять обработку персональных данных исключительно на законных основаниях и законным способом, справедливо и прозрачно по отношению к субъекту данных;

- *Принцип ограничения цели* устанавливает запрет на сбор персональных данных без четко сформулированных, явных и законных целей, а также исключает возможность дальнейшего использования в целях, несовместимых с первоначальными;

- *Принцип минимизации данных* ограничивает объем собираемой информации критерием строгой необходимости. Персональные данные должны быть адекватными и релевантными по отношению к конкретным целям обработки («ничего лишнего»);

- *Принцип точности* накладывает обязательства по поддержанию точности и актуальности персональных данных. Неточные или устаревшие сведения подлежат немедленной коррекции или удалению;

- *Принцип ограничения хранения* устанавливает временные рамки нахождения персональных данных в системе. Идентификация субъекта должна быть невозможна после того, как достигнуты цели обработки, что требует своевременного уничтожения или анонимизации архивов;

- *Принцип целостности и конфиденциальности* требует адекватного технико-организационного инструментария для предотвращения утечек, несанкционированного доступа или случайной потери, уничтожения или повреждения данных;

- *Принцип подотчетности* возлагает на контролера бремя доказывания комплаенса принципов защиты персональных данных, а также иметь верифицируемые доказательства их реализации.

Опираясь на сравнительно-правовые исследования отечественных правоведов, детально изучивших европейские модели (в частности опыт Эстонии и Великобритании), можно систематизировать зарубежные специальные принципы следующим образом [184].

Во-первых, Закон Эстонии «О защите персональных данных» (Personal Data Protection Act), выступающий примером гармонизации национального права с регламентом GDPR, постулирует систему принципов, обеспечивающих высокий уровень защиты персональных данных [185]:

- *законности* – императив сбора персональных данных исключительно законными и добросовестными методами;

- *целенаправленности* – ограничение сбора и обработки заранее определенными и законными целями и запрет на их произвольную смену;

- *минимализма* – соответствие объема собираемых персональных данных критерию строгой необходимости;

- *ограниченного использования* – запрет на использование персональных данных в иных целях без согласия субъекта или разрешения компетентного органа;

- *качества данных* – поддержание точности, актуальности и полноты персональных данных в контексте целей обработки;

- *безопасности* – обязательная имплементация мер безопасности против несанкционированной обработки, раскрытия или уничтожения;

- *индивидуального участия* – наделение субъекта данных правом на транспарентность обработки, доступ к касающимся его данным, и правом требовать коррекции недостоверных данных.

Во-вторых, комплексную многоуровневую систему регулирования формирует Закон о защите Данных Великобритании (Data Protection Act 2018), где в зависимости от сферы деятельности выделяются самостоятельные нормативные блоки [186]. В рамках раздела 2 (Part 2) закон обеспечивает имплементацию положений и принципов GDPR в национальное правовое поле. В то же время раздел 3 (Part 3) устанавливает специальный режим для правоохранительной деятельности, базирующийся на шести принципах: *законности и справедливости обработки, строгом ограничении целеполагания, информационной соразмерности (адекватности), обеспечении технико-организационной защищенности, поддержании актуальности данных и лимитировании сроков хранения персональных данных*. Аналогичная по структуре, но адаптированная к специфике деятельности органов государственной безопасности (Службой безопасности, Секретной разведывательной службой, Штабом правительственной связи) система шести принципов закреплена в разделе 4 (Part 4), что позволяет обеспечить баланс между интересами национальной безопасности и защитой приватности. Закон о защите Данных Великобритании также раскрывает содержание и значение каждого принципа [186].

Анализируя условия правомерности обработки информации, в более ранних исследованиях указывались ключевые отличия европейских критериев законности от казахстанских аналогов [179]. Развивая данный тезис, следует подчеркнуть, что если GDPR связывает легитимность с добровольностью и информированностью субъекта, то отечественный законодатель смещает фокус на формальное содержание согласия и сроки его действия [180]. Хотя закон позволяет собственникам и операторам баз данных запрашивать дополнительную информацию в согласии, уполномоченный орган пояснил, что перечень собираемых персональных данных не может быть открытым и неисчерпывающим [187]. Как было отмечено ранее, подобный подход уполномоченного органа РК является методологически нецелесообразным [179]. Закон «О персональных данных» не предусматривает четкие критерии действительности согласия, такие как свободно предоставленное, без давления или принуждения, и информированное (осознанное). В то же время Кодекс РК от 7 июля 2020 года № 360-VI «О здоровье народа и системе здравоохранения» как специальный правовой акт требует информированного согласия от лиц (пациентов) [145].

Анализ отечественной правоприменительной практики свидетельствует о декларативном характере института согласия, который зачастую не отвечает критериям информированности и волеизъявления. Собственники и операторы баз данных игнорируют обязанность по разъяснению необходимого объема персональных данных и целей их сбора и обработки, что ведет к необоснованной избыточности собираемых сведений и нарушению принципа пропорциональности. Легитимность такого «формального» согласия остается дискуссионным вопросом, решение которого осложнено отсутствием основополагающих специальных

принципов, регулирующих обработку персональных данных. Данная ситуация усугубляется дефицитом правовой грамотности среди населения и организаций.

В качестве ключевого индикатора действительности согласия лица на сбор и обработку персональных данных в казахстанском законодательстве выступает доказуемость согласия. Отсутствие данного признака детерминирует недействительность волеизъявления и, как следствие, незаконность совершаемых операций с персональными данными, что демонстрируется в материалах судебной практики [188, 189, 118]. Зачастую субъекты данных апеллируют к отсутствию письменной формы согласия как характеристике доказуемости. В одном из споров организация аргументировала правомерность своих действий получением устного согласия лица на сбор и обработку персональных данных. В судебном акте не прослеживаются доводы сторон спора, но поскольку закон не содержит спецификации относительно формы и требует подтверждаемого согласия, организация могла избежать ответственности в случае фиксации устного согласия, например, в виде аудиозаписи со всеми требованиями закона к содержанию согласия, таким образом доказав получение согласия. При наличии подтвержденного согласия государственные органы руководствуются целями использования персональных данных, для которого было получено согласие. Примером такого подхода является спор с участием иностранной компании, где работник при трудоустройстве предоставил согласие на сбор и обработку сведений о себе и членах своей семьи для целей страхования в рамках компенсационного пакета работодателя [124]. Суд признал правомерным сохранение доступа работодателя к корпоративной электронной почте бывшего сотрудника, содержащей указанные персональные данные, квалифицировав действия работодателя соответствующими предоставленному согласию без передачи сведений третьим лицам после увольнения.

Контрастируя с казахстанским регулированием, статьи 13 и 14 GDPR устанавливают четкие требования к информации, которую контролер данных *обязан* предоставить субъекту *на момент сбора* персональных данных. Императивная обязанность контролеров включает предоставление определенного спектра сведений, включая контактные данные для защиты данных, цели обработки, условия передачи данных, продолжительность хранения и права субъекта данных, включая право на защиту в надзорном органе по защите персональных данных. Фундаментальным отличием является наличие в GDPR требований к модальности изложения: информация должна быть предоставлена в лаконичной и доступной форме. В то же время казахстанское законодательство не содержит ни аналогичного исчерпывающего перечня обязательных реквизитов, ни стандартов «понятного языка», что создает условия для сокрытия юридических рисков в сложных формулировках политик конфиденциальности.

Принципы минимизации данных, целевого ограничения и ограничения хранения персональных данных подробно описаны в GDPR (статьи 5.1(b), (c), (e)). Европейский Регламент на уровне исходных основополагающих начал закрепляет,

что персональные данные собираются в строго необходимом минимуме для определенных, явных и законных целей, обрабатываются способом, совместимым с этими целями, не хранятся дольше, чем необходимо для достижения цели их обработки.

Современные казахстанские принципы защиты персональных данных в качестве специальных основополагающих положений не в полной мере соответствуют международным стандартам и не задают четкого вектора правоприменения для всех участников правоотношений. Действующий Закон «О персональных данных» содержит положения, корреспондирующие международным требованиям, однако они представлены в виде обязанностей собственников и операторов баз данных (пп. 8 и 9 ст. 7). Данные положения устанавливают, что обработка персональных данных должна быть совместима с целями их сбора, а содержание и объем обрабатываемых данных не должны быть избыточными по отношению к целям обработки.

Комплексный нормативно-юридический аудит статей 1, 7 и 12 профильного закона Республики Казахстан детерминирует латентный деструктивный дисбаланс в механизме правового регулирования. Прежде всего, дескриптивную неопределенность порождает регламентация процедуры накопления персональных данных. Нормативные предписания статьи 1 Закона «О персональных данных» трактуют накопление как внутреннюю операцию по упорядочиванию и систематизации уже аккумулированных персональных данных, в то время как положения статьи 12 связывают данный процесс с моментом первичного сбора. Подобная несогласованность приводит к доктринальному парадоксу: стадия сбора фактически выведена законодателем за рамки легального определения обработки, что нивелирует установление четких фильтров (целеполагания) на этапе получения персональных данных. Подобная дефрагментация норм усложняет интерпретацию закона участниками правоотношений, в особенности в силу различий в цифровой грамотности.

Параллельно с этим обнаруживается глубокий содержательный разрыв при реализации принципа минимизации данных. Императивные требования статьи 7, предписывающие обрабатывать информацию в пределах избыточного и достаточного объема персональных данных, функционально ограничены стадией их обработки. На этапе сбора персональных данных лимитирующим критерием выступают не легитимные цели, а весьма размытые задачи, стоящие перед собственником и (или) оператором, а также третьим лицом. Данная дихотомия порождает регулятивную коллизию: стадия обработки подчинена строгому целевому ограничению по цели, тогда как стадия сбора детерминирована субъективным вектором задач владельца, оператора или третьей стороны. На существование данной регулятивной коллизии, создающей риски необоснованного расширения состава собираемой информации собственниками и операторами, обращают внимание исследователи С.Б.Ахметова, А.С.Ибраева с соавторами. Правоведами аргументировано, что дефрагментация норм между

стадиями сбора и обработки усложняет понимание правовых гарантий рядовыми субъектами, фактически легитимизируя дискреционные полномочия собственника и оператора базы данных по произвольному формированию перечней собираемых персональных данных [184].

В рамках правоприменительной практики собственники и операторы обязаны по мере необходимости анализировать свою деятельность, связанную с персональными данными, детерминируя правовые основания и необходимый объем данных для реализации своих целей и задач, и на основе этого анализа утверждать и корректировать перечень требуемых персональных данных [190]. Субъекты, в свою очередь, должны дать согласие на сбор и обработку перечисленных конкретных данных в соответствии со статьей 8 Закона «О персональных данных».

Тем не менее, практика свидетельствует о недостаточной эффективности указанных норм. Характерным примером является повсеместное требование предоставить индивидуальный идентификационный номер (ИИН) при заключении каких-либо гражданско-правовых договоров с физическим лицом, помимо его имени, документа, удостоверяющего личность, и контактной информации. Необходимость ИИН при заключении гражданско-правовых сделок вызывает вопросы о достаточности и совместимости данной личной информации с целями обработки персональных данных. Согласно положениям статьи 15 Гражданского Кодекса РК и пункта 3 статьи 6 Закона Республики Казахстан от 29 января 2013 года № 73-V «О документах, удостоверяющих личность» физическое лицо приобретает и осуществляет права и обязанности, совершает гражданско-правовые сделки под своим именем, фамилией и именем, по документам, удостоверяющим личность [191]. Следовательно, фамилия и имя, подтвержденные удостоверяющим личность документом, являются юридически достаточными персональными данными для заключения гражданско-правовых сделок. Таким образом, систематический сбор и хранение ИИН в большинстве случаев могут квалифицироваться как нарушение пунктов 8 и 9 статьи 7 Закона, а регулятивная неопределенность затрудняет восприятие правовых гарантий рядовым субъектом правоотношений.

Иллюстрацией институционального дефицита в механизмах защиты субъектных прав выступает критический анализ ведомственной практики, осуществленный в исследованиях С.Б.Ахметовой и соавторов. На примере рассмотрения официальных разъяснений Министерства труда по вопросам внедрения дактилоскопических систем на предприятиях, учеными констатируется игнорирование регулятором условий соразмерности, закрепленных статьей 7 профильного закона. Внедрение подобных систем верификации зачастую носит характер технологической избыточности, не обусловленной спецификой и реальными задачами трудовых правоотношений на предприятиях. Схожий формально-декларативный подход уполномоченных органов обнаруживается и при оценке правомерности систем видеомониторинга в коммерческом секторе.

Вместо глубокого анализа совместимости собираемых данных с заявленными целями контроля, государственные структуры ограничиваются репродуцированием нормативного текста, оставляя без должного внимания императивный запрет на аккумуляцию избыточной информации. [184, 192, 115, 116, 117]

Определенные надежды на преодоление указанных пробелов связывались с проектом Цифрового Кодекса. Однако на стадии разработки его положения вызвали определенные вопросы: так принцип законности (статья 4 проекта) неоправданно сужался до соответствия только Конституции, а принцип приоритета прав человека (статья 5 проекта) ограничивался лишь защитой от дискриминации при автоматизированной обработке, игнорируя человеческий фактор. [132]

В принятой редакции Цифрового Кодекса РК принципы регулирования цифровой среды значительно пересмотрены и обеспечивают конституционное право на уважение частной жизни и защиту персональных данных, реализуют функции данного конституционного права. В частности, содержание принципов Цифрового Кодекса защищают автономию личности, контроль и самоопределение, управление границами и доступом. Статья 5 Цифрового Кодекса РК закрепляет принцип уважения прав, свобод и законных интересов, который устанавливает, что решения в цифровой среде должны основываться на волеизъявлении индивида. Это условие о волеизъявлении имеет первостепенное значение и включает в себя три существенные характеристики: (1) оно должно быть свободным от принуждения или манипуляций, (2) оно должно быть осознанным, и (3) оно должно быть явно выраженным. Отсутствие любого из этих существенных качеств в процессе принятия решений подрывает его легитимность, тем самым влияя на действительность любых вытекающих из этого правовых последствий. Кроме того, этот принцип требует определенной степени прозрачности в сфере алгоритмического и автоматизированного принятия решений. Он требует, чтобы индивиды обладали базовым пониманием механизмов работы алгоритмов и процессов принятия ими решений. Эта прозрачность является неотъемлемой частью обеспечения осознанного выражения воли. Более того, принцип запрещает дискриминацию и навязывание неравных преимуществ или недостатков, возникающих в результате алгоритмических и автоматизированных решений. Это также подчеркивает важность индивидуального контроля над частной жизнью, доступом и обменом информацией. Согласование этого принципа с аналогичными положениями Закона «О персональных данных» подчеркивает его значимость и выделяет повышение его статуса в правовом регулировании, закрепляя его в кодексе, а не просто в законе.

Тем не менее, инкорпорация этих принципов в Цифровой Кодекс РК порождает проблему «правового дуализма». Принцип соблюдения прав и свобод человека, закрепленный статьей 5 Цифрового Кодекса, служит руководством для

операций в цифровой среде. За ее пределами продолжает действовать Закон «О персональных данных», который не раскрывает содержание аналогичных принципов, оставляя внецифровую среду в зоне регуляторной неопределенности.

Сравнительный анализ нормативных положений показывает, что европейские источники права о защите персональных данных предлагают гораздо более детализированный базис отраслевых принципов, чем казахстанское законодательство. В научных публикациях данный феномен обоснованно связывается с процессом необходимости легального закрепления для изменения устоявшейся правоприменительной практики [184, стр.42]. Представляется, что именно свойство высшей императивности, имманентно присущее европейским принципам-нормам, делает их эффективным инструментом для регулирования отношений в сфере защиты персональных данных [183, стр.6]. Это актуализирует необходимость модернизации отечественного Закона посредством рецепции аналогичных устойчивых правовых конструкций.

Нормативная фиксация принципов защиты персональных данных имеют существенное и даже первостепенное значение для устойчивости всей системы обеспечения защиты. Существующая практика официальных разъяснений государственных органов РК по обращениям физических лиц демонстрирует фрагментарный и непоследовательный характер, что является прямым следствием несовершенства понятийного аппарата Закона «О персональных данных». Подобный подход государственных органов неизбежен в силу требований статьи 59 Закона Республики Казахстан от 6 апреля 2016 года № 480-V «О правовых актах» поскольку, разъясняя положения Закона «О персональных данных», представители министерств руководствуются принципами Закона «О персональных данных», отличными от европейской модели. Как справедливо отмечают А.Гусарова и С.Джаксылыков, отсутствие в отечественном праве стратегии имплементации ключевых принципов GDPR создает существенные препятствия для эффективного правоприменения [193, стр.5]. При этом частичная инкорпорация принципов в Цифровой Кодекс РК, как правовой акт более высокого уровня в отношении Закона «О персональных данных», лишь подчеркивает проблему правового дуализма, оставляя внецифровую среду в зоне регуляторной неопределенности с действующими принципами Закона «О персональных данных». В этой связи представляется необходимой ревизия Закона «О персональных данных» в части закрепления в нем императивных принципов и четких механизмов их реализации в соответствии с требованиями статьи 14-3 Закона «О правовых актах».

Резюмируя вышеизложенное, представляется необходимым осуществить концептуальную ревизию архитектуры Закона «О персональных данных» посредством имплементации универсальных постулатов, признанных мировой доктриной. Инкорпорация таких начал, как «законность, справедливость и прозрачность», «минимизация данных», «ограничение хранения», «ограничение цели», «точность», «целостность и безопасность», «подотчетность» должна носить

не формально-технический, а основополагающий характер. Будучи закрепленными в качестве фундаментальных принципов, а не частных процедурных условий, данные нормы приобретают статус ценностно-ориентирующего вектора. Подобный подход позволяет рассматривать отраслевые императивы в качестве базового регулятивного ориентира, детерминирующего правомерность сбора и обработки персональных данных. В рамках данного телеологического подхода исследователь Х.Врабец обосновывает тезис о том, что ключевая функция принципов заключается в демаркации пределов обработки данных и формирования директивных инструкций для участников информационного оборота осуществлять действия законным и ответственным образом» [184, стр.43; 102, стр.33]. Вектор европейского законодательства, в противовес отечественному правотворчеству, ориентирован на сквозную интеграцию фундаментальных постулатов во всю архитектуру Европейского Регламента. Обязательства контролеров, операторов и третьих лиц содержательно детерминированы указанными принципами, которые находят свое эксплицитное выражение в последующих статьях. Принципы выступают не просто декларациями, а аксиоматическим фундаментом, предопределяющим содержание прав и обязанностей всех участников информационного оборота – от индивидов до государственных институтов. Подобная структура обеспечивает высокую адаптивность правоприменения на современном этапе и в перспективе.

Юридическая суть закрепления принципов права в нормативно-правовом акте играет важную роль на практике [194, стр.5]. Конституционная реформа 2026 года, инкорпорировавшая защиту персональных данных в текст статьи 21 Основного закона, детерминирует логическую модернизацию принципов в Законе «О персональных данных» согласно новому иерархическому статусу института защиты персональных данных.

Текущее нормативное содержание и оформление принципов, лишенное четкой терминологической определенности и конкретных механизмов реализации вступает в диссонанс с духом обновленной Конституции РК. Требуется качественное переформатирование принципов защиты персональных данных: из «условий обработки» их необходимо трансформировать в автономные правовые гарантии. Это предполагает не только лингвистическое обновление формулировок, но и наделение их качеством высшей нормативности, позволяющим использовать принципы как прямой инструмент государственного, в том числе судебного, контроля над деятельностью участников информационного оборота, в том числе государства.

В этой связи требуется концептуальный переход от казахстанской модели «условий обработки» к рецепции международного подхода «высших императивных директив». Инкорпорация принципов именно в качестве основных постулатов регулирования защиты персональных данных обусловлена ролью персональных данных в составе конституционного права на неприкосновенность частной жизни. Как обосновано в компаративных исследованиях С.Б.Ахметовой и

соавторов, следование формуле «самостоятельное право – самостоятельные принципы ограничений» требует закрепления в законе системы высокоточных фильтров (минимизация данных, ограничение цели, ограничение хранения, подотчетность, прозрачность), которые формируют пределы допустимого воздействия на автономию личности. [184; 195, стр.34].

Выступая в качестве базовых ориентиров, принципы права предназначены не только для текстуального закрепления в законе, но и для непосредственной проекции на сферу реальных правоотношений, где они задают генеральный вектор и динамику правоприменительной практики. Их содержательное воплощение должно пронизывать любые юридически значимые действия, корпоративные соглашения, политики конфиденциальности и иные регламенты субъектов, задействованных в сборе, обработке и хранении персональных данных. В теории права справедливо подчеркивается, что подобные отправные точки гарантируют «единство правотворчества, интерпретации и реализации правовых норм, являются ценностными ориентирами создания и реализации права» [183, стр.7]. Именно поэтому императивное законодательное закрепление данных принципов-норм имеет первостепенное значение для формирования единообразной правоприменительной практики и полноценного обеспечения конституционных гарантий защиты персональных данных и неприкосновенности частной жизни.

3 СИСТЕМА ГОСУДАРСТВЕННЫХ ОРГАНОВ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЗАРУБЕЖНЫХ СТРАНАХ И В РЕСПУБЛИКЕ КАЗАХСТАН

3.1 Государственное регулирование защиты персональных данных в зарубежных странах

Право на защиту персональных данных охраняется в составе фундаментального права человека на неприкосновенность частной жизни, закрепленного во Всеобщей декларации прав человека и Международном пакте о гражданских и политических правах. Международный пакт о гражданских и политических правах ко Всеобщей декларации прав человека ООН 1948г. в статье 17 закрепляет право человека не подвергаться произвольному или незаконному вмешательству в личную и семейную жизнь, на неприкосновенность жилища и тайну корреспонденции [56].

Проблемный анализ показывает, что международные обязательства имеют приоритет над внутренним правом: государство не может оправдывать несоблюдение международных обязательств, в том числе по защите основных прав и свобод человека, пробелами в национальном законодательстве. Как подчеркивал Торкел Опсал, бывший член Европейской комиссии по правам человека и Комитета ООН по правам человека, «первейшим обязательством по любой конвенции является ее воплощение в национальном законодательстве. Это альфа и омега прав человека...» [196, стр.66]. В контексте национального законодательства для любого государства-участника Всеобщей декларации прав человека и Международного пакта о гражданских и политических правах это означает, что формальное наличие специальных законов о защите персональных данных является лишь первым шагом, в то время как «альфой и омегой» должна стать реальная имплементация механизмов защиты, сопоставимых с международными стандартами.

В Европейском союзе помимо Всеобщей декларации прав человека и Международного пакта ООН право на неприкосновенность частной жизни предусмотрено в Европейской Конвенции о защите прав человека и основных свобод 1950г. В развитие права на неприкосновенность частной жизни в Европе 28 января 1981 года был принят другой международный документ - Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера (Конвенция 108), закрепляющая защиту персональных данных [108]. Несмотря на региональный и императивный характер Европейской Конвенции и Конвенции 108 для европейских государств, с 90-х годов XX века Конвенция 108 распространила свое влияние и за пределы Европы, а обновленная Конвенция 108+ фактически стала международным документом, к которой присоединились

неевропейские страны, признавая ее «глобальным золотым стандартом» защиты персональных данных [107, 197].

Система охраны прав в государстве представляет собой сложный механизм, включающий нормативный и организационный компоненты, направленный на исключение или уменьшение прав человека [198, Стр.127]. В своей основе система государственно-правовой защиты персональных данных представляет собой целостное явление, состоящее из определенных элементов (частей), взаимосвязанных и взаимодействующих между собой [94, стр.296]. Компоненты данной системы обладают определенной иерархичностью и функционируют согласованно, обеспечивая необходимый уровень координации между всеми ее элементами [94, стр.200].

В современных условиях защита фундаментального права на неприкосновенность частной жизни и защиты персональных данных обрела уровень конституционной защиты в большинстве стран. Основываясь на конституциях и законах, защита персональных данных реализуется путем государственного и правового регулирования.

Наиболее репрезентативным и успешным примером реализации данного нормативного и институционального подхода выступает Европейский Союз. В Европейском Союзе нормативная база функционирует как целостная экосистема, которая не только интегрирует региональные международные акты, GDPR, профильные Директивы, национальные конституции и законы, но и опирается на активную деятельность системы государственных и независимых надзорных органов, обеспечивающих практическую реализацию, мониторинг и исполнение правовых норм. На протяжении нескольких десятилетий государственно-правовая система защиты Европейского Союза демонстрирует высокую степень операционной эффективности и системной завершенности.

Европейская архитектура государственного обеспечения защиты персональных данных представляет собой многоуровневую систему с распределением функций между наднациональными институтами Европейского Союза и национальными органами государств-членов. Наднациональный уровень системы государственных органов базируется на деятельности Европарламента, Совета Европы, Суда Европейского Союза (ЕСJ), функционирующих на основе Договора о функционировании Европейского союза (Рим, 25 марта 1957 г., в редакции Лиссабонского договора 2007 г.) [199].

Законодательный процесс в Европейском Союзе осуществляется посредством совместного принятия законодательных актов Европейским парламентом и Советом Европейского Союза на основе предложений Европейской комиссии в соответствии процедурой, предусмотренной статьей 294 Договора о функционировании Европейского Союза.

Важнейшим элементом институциональной структуры выступает Европейский совет по защите данных (EDPB) — независимый орган, обеспечивающий последовательное применение GDPR и Директивы 2016/680,

регламентирующей защиту персональных данных в сфере правоохранительной и уголовно-исполнительной деятельности государств [200]. В состав наднационального органа EDPB входят руководители национальных органов по защите данных государств-членов ЕС и Европейский инспектор по защите данных (EDPS). EDPB и EDPS обеспечивают соблюдение законодательства о защите данных как на национальном, так и на трансграничном уровне через механизмы сотрудничества, включая систему «одного окна». Кроме того, EDPB также наделен полномочиями по принятию обязательных решений по неурегулированным вопросам и трансграничной обработки данных.

Судебный контроль и гарантии единообразной интерпретации и имплементации законодательства ЕС, в том числе GDPR, обеспечивается Судом Европейского Союза (ECJ). Данный институт обеспечивает последовательное соблюдение законодательства ЕС как государствами-членами, так и институтами ЕС, в том числе посредством разрешения правовых конфликтов между национальными правительствами и институтами ЕС. Кроме того, в определенных ситуациях частные лица, предприятия или организации могут использовать Суд Европейского Союза и обращаться с индивидуальными жалобами для оспаривания деятельности органа ЕС в случае нарушения ими прав и законных интересов лица.

Параллельно с этим судебная защита права на неприкосновенность частной жизни и защиту персональных данных, гарантированного статьей 8 Европейской конвенции по правам человека, осуществляется Европейским судом по правам человека. Являясь международным судебным органом, ЕСПЧ осуществляет судебный надзор за исполнением положений Европейской Конвенции странами-участницами данного международного акта. В компетенцию ЕСПЧ входят вопросы интерпретации и обеспечение исполнения положений Европейской Конвенции, включая межгосударственные споры и индивидуальные обращения физических лиц.

Наряду с общеевропейскими, наднациональными государственными органами (EDPB, ECJ), основная задача которых единообразное применение общеевропейского законодательства во всех странах-членах Европейского Союза, государства-члены обладают автономными национальными механизмами защиты. На национальном уровне каждое государство имеет свою нормативно-правовую систему и систему государственных органов по защите персональных данных, включающую законодательные, исполнительные, правоохранительные и судебные органы.

Развивая тезис о системно-институциональном характере европейской модели, следует подчеркнуть, что законодательное регулирование защиты персональных данных в Европе императивно предполагает наличие специализированного органа, обеспечивающего практическое исполнение закона, способствующего соблюдению прав человека. Фундамент данного требования заложен в статье 13 Конвенции 108 и статье 15 Модернизированной Конвенции

108+, которые обязывали каждое государство-подписант сформировать уполномоченный орган в сфере защиты персональных данных. Как отмечает Г.Гринлиф, страны, стремящиеся к тому, чтобы их законодательство признавалось «адекватным» стандартам ЕС, обязаны создать «институциональный механизм, позволяющий [осуществлять] независимое расследование жалоб», а также сформировать «рамки для независимого судебного разбирательства или арбитража, которые допускают компенсацию и санкции в случае необходимости» [201, стр.7].

Эволюция нормативных требований демонстрирует переход от консультативных функций к контрольно-надзорным: если статья 13 Конвенции 108 фокусировалась преимущественно на функции по повышению осведомленности общественности о правах субъектов данных и консультировании по законодательным и административным мерам обработки данных, то статья 15 Модернизированной Конвенции 108+ прямо требует учреждения органа, ответственного за обеспечение соблюдения положений Конвенции [197].

Конвенция 108, являясь обязывающим международным инструментом, послужила концептуальной основой Европейской Директивы 95/46/ЕС 1995 года, на смену которой в 2018 году пришел GDPR [108, 104, 45]. И Директива 95/46/ЕС 1995 года, и заменивший ее GDPR, постулируют наличие независимого надзорного органа по защите персональных данных в каждом государстве ЕС как обязательное условия легитимного функционирования системы защиты права на защиту персональных данных. Согласно правовой позиции суда ECJ, наличие такого регулятора является обязательным условием для обеспечения адекватной защиты персональных данных в других странах, то есть «по сути эквивалентной гарантированному правовым порядком ЕС» [202, §§73,74,96]. Исключительное значение и императивность наличия органа по защите данных было ярко продемонстрировано в прецедентном деле *Schrems I*, где отсутствие надзорного органа по защите персональных данных в третьей стране было признано критическим препятствием для международной торговли с европейскими странами [202]. В прецедентном праве ECJ квалифицирует уполномоченные органы по защите персональных данных как «хранителей основных прав и свобод человека и важнейший компонент защиты персональных данных физических лиц» [203, §23].

Особый акцент в европейской доктрине делается на атрибутах независимости и самостоятельности органов по защите персональных данных. Для эффективного выполнения своих функций надзорные органы должны «действовать объективно и беспристрастно, оставаться свободными от любого внешнего влияния, включая прямое или косвенное влияние государства» [203, §24]. Таким образом, институциональная независимость уполномоченного органа по защите персональных данных является не просто организационным требованием, а фундаментальным условием жизнеспособности правовой экосистемы защиты персональных данных.

Логическим продолжением развития указанных институциональных стандартов стала детальная нормативная регламентация статуса надзорных органов в Европейском Регламенте GDPR. Данный Регламент предусматривает развернутый комплекс положений в Главе 6 (статьи 51-59), регламентирующий вопросы создания, функционирования и компетенций надзорного органа.

Статья 53 GDPR устанавливает общие требования к процедуре назначения членов надзорного органа, предъявляя высокие требования к их квалификации, профессиональному опыту и навыкам в области защиты персональных данных. Детализация требования на уровне общеевропейского регламента призвана минимизировать риски политического влияния и обеспечить экспертный характер деятельности регулятора.

Функциональный профиль надзорного органа, согласно нормам GDPR, включает комплекс задач, направленных на всестороннее обеспечение режима защиты персональных данных: мониторинг и обеспечение соблюдения GDPR, повышение правовой информированности общества по вопросам защиты данных, предоставление консультаций, рассмотрение жалоб субъектов данных, проведение расследований по вопросам применения GDPR. Доктринально компетенция надзорного органа классифицируется «на три основные группы: следственные полномочия (доступ к информации и помещениям, проведение проверок защиты данных, уведомление о нарушениях); корректирующие полномочия (вынесение предупреждений и выговоров, предписание по выполнению запроса субъекта данных, наложение ограничения, включая запрет на обработку, или наложение административного штрафа); а также разрешительные и консультативные полномочия (издание разъяснительных заключений, выдача сертификатов и определенных разрешений)» [204, стр.462].

Европейский Регламент GDPR наделяет уполномоченные органы по защите данных диверсифицированным объемом полномочий, среди которых наряду с традиционными следственными и корректирующими полномочиями, присущими большинству государственных органов, стратегическое значение имеют консультативно-разъяснительные функции. Превентивная природа данных функций ориентирована на обеспечение корректной интерпретации и эффективной имплементации законодательства о защите персональных данных, что позволяет минимизировать риск правонарушений в сфере приватности. Практическая реализация этого направления в европейских государствах выражается в издании официальных руководств и экспертных разъяснений, нацеленных на формирование у операторов и контролеров единого вектора применения нормативных актов по защите персональных данных. В частности, официальный сайт EDPB содержит специальный раздел, (https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en?page=1), посвященный консультативной работе, на котором на данный момент содержатся более 60 методических документов, включая руководства, рекомендации и передовую практику. В западной

юридической доктрине подчеркивается авангардная роль надзорных органов в архитектуре контроля за соблюдением правовых норм. Исследователи отмечают, что именно эти структуры находятся на переднем крае правоприменения, а издаваемые ими руководства и разъяснения выступают приоритетным ориентиром для субъектов бизнеса, нацеленных на выстраивание эффективной стратегии комплаенса [205, стр.177].

Особое значение придается функции уполномоченных органов по повышению осведомленности граждан о защите персональных данных, об утверждении и согласовании правил поведения объединений, правил трансграничной передачи персональных данных контролеров и операторов данных. Данное направление отвечает принципу человекоцентричности правового регулирования защиты персональных данных и имеет прямое воплощение. Об этом свидетельствуют в том числе специальные разделы сайта Европейского совета по защите данных (https://www.edpb.europa.eu/edpb_en), посвященные физическим лицам, контролерам и обработчикам, а также национальным регуляторам. В разделе для физических лиц содержатся руководства, подробно разъясняющие права субъекта данных (https://www.edpb.europa.eu/guidelines-your-rights-0_en), полные контакты национальных органов по защите данных (https://www.edpb.europa.eu/about-edpb/about-edpb/members_en), а также активная иконка «уведомить об утечке данных». Некоторые европейские надзорные органы по защите данных проводят специальные тренинги, включая тренинги для отдельных аудиторий или сфер, например, для исследователей [206, стр.5]. В международной научной литературе Зарубежные авторы считают «критической» роль органов по защите данных в повышении осведомленности и консультировании и характеризуют орган по защите данных как «аудитора, консультанта, преподавателя, политического советника и переговорщика» [207, стр.24]. Дополнительно европейское регулирование выделяет коммуникативную (связывающую) функцию уполномоченного органа по защите данных, обеспечивающую взаимодействие с другими национальными надзорными органами и с Европейским Советом по защите персональных данных (EDPB), а также с корпоративными офицерами по защите персональных данных. Последние выступают контактными лицами в организациях как для надзорного органа, так и для физических лиц.

Однако для того, чтобы просветительская и консультативная миссия подкреплялась реальными гарантиями, уполномоченные органы наделены широким спектром неисчерпывающих полномочий, выступающих необходимым средством выполнения его обязанностей [202, §43]. В рамках реализации указанных задач по охране основных прав человека данные органы обладают определенными следственными полномочиями, включая возможность собирать всю необходимую информацию для выполнения своих надзорных функций. Они также наделены правом эффективного вмешательства, к которому относятся полномочия по наложению временных или постоянных запретов на обработку

данных, а также право участвовать в судебных разбирательствах для защиты интересов субъектов и обеспечения законности.

Институциональная архитектура государственного регулирования в области защиты персональных данных в европейском правовом пространстве базируется на функциональной автономии надзорных органов. Сравнительный анализ моделей Эстонии и Германии позволяет выявить два различных, но комплементарных подхода к имплементации общеевропейских стандартов независимости регулятора.

В Эстонии имплементация норм GDPR реализована через Personal Data Protection Act 2019 (Isikuandmete kaitse seadus), который предусматривает основные понятия, базовые принципы, права и обязанности субъектов данных, контролеров, операторов и государственных органов, полномочия государственного органа по защите данных, меры реагирования на нарушения в сфере защиты персональных данных [185]. Данный закон закрепляет статус Инспекции по защите данных (Andmekaitse Inspektsioon) как централизованного и транспарентного органа надзора. Инспекция по защите данных выделена в отдельный, самостоятельный и независимый орган с ясными и конкретными полномочиями.

Внутренняя организация Инспекции по защите данных Эстонии ориентирована на пять ключевых векторов: технологический аудит, общее консультирование и юридическая экспертиза, международное сотрудничество, надзор (<https://www.aki.ee/en/contact>). Особенностью эстонской модели является высокая концентрация юридических компетенций в кадровом составе ведомства. Согласно сведениям веб-сайта эстонской инспекции при компактном штате ведомства (31 сотрудника) более 70% персонала (22 специалиста) составляют профессиональные правоведа. Подобная структура подчеркивает приоритет правовой интерпретации и защиты основных прав субъекта в условиях преобладающей цифровизации государственного управления (e-Estonia).

На уровне закона Personal Data Protection Act Эстонии предусматривает положения относительно первого руководителя Инспекции (Chapter 5). Процедура его назначения предполагает сложный механизм сдержек: кандидатура выдвигается Правительством после обязательного консультирования с Конституционным комитетом (Riigikogu). Императивный запрет Personal Data Protection Act Эстонии для первого руководителя относительно членства в какой-либо политической партии дополнительно обеспечивает статус Инспекции как независимого органа. Квалификационные требования к руководителю включают не только экспертные знания в области приватности, но и обязательный допуск к государственной тайне, что обусловлено глубокой интеграцией Инспекции в мониторинг государственных информационных систем.

Функциональный анализ деятельности надзорного органа Эстонии подтверждает, что Инспекция проявляет наибольшую активность в сфере издания разъяснений и практических рекомендаций по вопросам защиты персональных

данных [206, стр.4]. Оперативное информирование населения по вопросам безопасности персональных данных достигается за счет интеграции информационных ресурсов ведомства с общенациональным порталом Эстонии (<https://www.eesti.ee>). Данная государственная платформа имеет прямую связь с интернет-ресурсом Инспекции (<https://www.eesti.ee/en/security-and-defense/safety-and-security/protection-of-personal-data-and-privacy>), обеспечивая пользователя удобную навигацию. Вебсайт Инспекции структурирован таким образом, чтобы субъекты данных, контролеры и операторы могли не только детально ознакомиться со своими правами и обязанностями, но и эффективно их реализовать. Для субъектов данных доступно и последовательно изложен алгоритм действий: как, куда и в каких случаях следует обращаться за помощью и разъяснениями. Наличие на официальной странице эстонской Инспекции по защите данных готовых шаблонов обращений – ходатайство о вмешательстве, ходатайство о разъяснении, запрос об информации и другие (<https://www.aki.ee/ru/svyazhites-s-inspekciej>) – значительно снижает административные барьеры и упрощает процедуру нарушенных прав.

Важно отметить, что высокая эффективность правоприменения в Эстонии во многом обусловлена цифровизацией процесса назначения должностных лиц по защите данных (DPO). Обязанность контролеров и операторов по назначению такого должностного лица по защите данных реализуется через электронный портал *e-Business Register* (<https://www.rik.ee/en/e-business-register>). Подобная интеграция требования о защите данных в систему регистрации субъектов предпринимательства гарантирует прозрачность корпоративного управления и делает соблюдение режима приватности обязательным условием функционирования бизнеса на институциональном уровне.

Германская модель имплементации GDPR, закрепленная в Федеральном законе о защите данных (Bundesdatenschutzgesetz, BDSG 2018), характеризуется дуализмом и федеративной распределенностью полномочий [208]. На федеральном уровне непосредственные надзорные функции закреплены за Федеральным комиссаром по защите данных и свободе информации (BfDI), статус которого детально регламентирован разделом 11 BDSG. С учетом федеративного государственного устройства Германии надзорные функции в области персональных данных выполняют независимые органы земель (LfD). Функциональный профиль BfDI сфокусирован на надзоре за федеральными государственными органами, операторами связи, почтовых услуг, тогда как надзор за частным сектором и региональными властями делегирован независимым надзорным органам земель. Параллельно с BfDI и надзорными органами земель в Германии действует институт Конференция по защите данных (Datenschutzkonferenz, DSK) – координационный орган, состоящий из руководителей всех федеральных и земельных регуляторов. DSK не является самостоятельным органом, но осуществляет критически важную роль национального механизма обеспечения единства правоприменения. Публикуемые

Конференцией по защите данных документы в виде резолюций (Entschliefungen) и ориентирующих пособий (Orientierungshilfen) обеспечивают единообразие правоприменения и представляют собой документы, разъясняющие интерпретацию закона и служащие прикладным инструментарием для контролеров и операторов по комплаенсу. Таким образом, надзор в Германии осуществляется децентрализованно, но его методологическое единство обеспечивается через коллективные решения DSK.

В отличие от руководителя эстонской Инспекции, Федеральный комиссар Германии избирается Бундестагом (нижней палатой парламента) абсолютным большинством по предложению Федерального правительства, после чего назначается Федеральным президентом. Аналогично эстонскому закону BDSG устанавливает жесткие требования к квалификации Федерального комиссара: кандидат должен быть не моложе 35 лет и обладать компетенциями, соответствующими должности судьи или высшего административного чиновника, что гарантирует независимость и профессиональный авторитет органа. Таким образом, если эстонская модель ориентирована на технологическую интеграцию и оперативность в рамках цифрового пространства, то германская система делает акцент на демократическом легитимировании надзора через парламентские процедуры и децентрализованный контроль, что отражает различные подходы к обеспечению независимости регулятора в рамках единого европейского правового стандарта.

В обеих странах квалификационные требования и процедура назначения служат барьером для прямого политического влияния, однако германский акцент на парламентском избрании и эстонский механизм правительственного назначения с участием парламентского комитета представляют собой две различные, но одинаково эффективные формы реализации требований GDPR о полной независимости надзорного органа.

Аналогично эстонскому опыту официальный портал BfDI (<https://www.bfdi.bund.de>) структурирован по целевым аудиториям: для граждан, для организаций и для государственных структур. В разделе для частных лиц представлены детальные разъяснения о правах субъектов персональных данных и алгоритмах обжалования незаконных действий контролеров и операторов.

Правоприменительный эффект в Германии, как и в Эстонии, усиливается через институт корпоративных офицеров по защите данных (DPO), закрепленный Федеральным законом о защите данных императив, содержащий более строгие по сравнению с GDPR требования.

Таким образом, если эстонская модель акцентируется на оперативной сервисной поддержке через единый портал, то немецкий подход демонстрирует силу экспертно-аналитического надзора и многоуровневой координации. Обе системы, несмотря на различия в масштабах и структуре, реализуют ключевое требование GDPR: превращение надзорного органа из карательного института в активного консультанта и гаранта информационной автономии личности.

Проведенный анализ позволяет констатировать, что европейская архитектура обеспечения защиты персональных данных представляет собой многоуровневую систему, в которой наднациональные институты Европейского союза и национальные регуляторы государств-членов функционируют в рамках единого правового поля, детерминированного Договором о функционировании ЕС.

Наднациональный контур регулирования, базирующийся на нормотворческой деятельности Европарламента и Совета ЕС, закладывает правовой фундамент. В этой структуре ключевую связующую роль выполняет Европейский Совет по защите данных (EDPB). Объединяя руководителей национальных надзорных органов и Европейского инспектора (EDPS), EDPB трансформирует разрозненные национальные практики в согласованную систему «одного окна», обеспечивая обязательность и единообразие правоприменения.

Судебные гарантии и правовой контроль, характеризуется институциональным дуализмом, обеспечивающим всестороннюю защиту права на неприкосновенность частной жизни Судом Европейского Союза (ECJ) и ЕСПЧ. Если ECJ сфокусирован на обеспечении единообразия и законности в рамках GDPR, то ЕСПЧ реализует международный судебный надзор за соблюдением Европейской Конвенции по правам человека, в том числе статьи 8 о неприкосновенности частной жизни. ECJ позволяет разрешать споры между институтами ЕС и жалобы частных лиц по оспариванию актов органов ЕС. Юрисдикция ЕСПЧ позволяет рассматривать как межгосударственные споры, так и индивидуальные жалобы на действия государств-участников Конвенции. Таким образом, механизмы судебной защиты от любых организаций, институтов и государств трансформируют право на неприкосновенность личности в непосредственно действующее субъективное право, обладающее качеством безусловной принудительной реализуемости и судебной защиты вне зависимости от правового статуса нарушителя.

Национальный уровень имплементации, проанализированный на примере Эстонии и Германии, демонстрирует жизнеспособность принципа функциональной автономии. Несмотря на институциональные различия – цифровую централизацию Эстонии и федеративный демократический дуализм Германии – обе модели успешно реализуют императив GDPR о независимости регулятора и его консультативной функции, направленной на обеспечение комплаенса и правовой осведомленности физических лиц.

В совокупности государственное регулирование в рассматриваемой сфере эволюционировало в комплексную экосистему, где карательная функция уступила место превентивному партнерству.

3.2 Государственное регулирование защиты персональных данных в Республике Казахстан

Система государственных органов, обеспечивающая реализацию и исполнение норм Конституции и законодательных актов, выступает институциональным ядром государственно-правовой защиты персональных данных. Государственная функция охраны прав и свобод человека, или правоохранительная функция, реализуется «в целенаправленном, организующем и регулирующем воздействии со стороны государства» [209, стр. 112]. Практическая деятельность государства в этой сфере обладает организующей сущностью, выражающейся в формировании и функционировании системы государственных органов и институтов власти.

В Республике Казахстан архитектура защиты права на неприкосновенность частной жизни и защиту персональных данных выстроена в соответствии с принципом разделения властей и включает законодательный орган (Парламент РК), систему исполнительных органов, включающую Правительство РК, центральные и местные исполнительные органы, и судебную власть. Согласно профильному Закону «О персональных данных» Правительство ответственно за разработку государственной политики в области защиты персональных данных, а Министерство искусственного интеллекта и цифрового развития РК (МИИЦР) функционирует как центральный исполнительный орган, координирующий различные отрасли, включая электронную промышленность, «электронное правительство», связь, цифровые активы, инновации, цифровое и технологическое развитие, информационную безопасность и защиту персональных данных [210]. Параллельно с МИИЦР местные исполнительные органы (акиматы) наделены полномочиями по обеспечению соблюдения законодательства о защите персональных данных и осуществлению государственного контроля.

Важное место в государственной системе защиты персональных данных занимает институт Уполномоченного по правам человека (Омбудсмен), получивший конституционный статус после республиканского референдума в июне 2022 года (ст. 83-1 Конституции РК 1995 г.) [211]. Правозащитная деятельность Уполномоченного по правам человека реализуется посредством рассмотрения заявлений и обращений физических лиц, инициирования контрольно-проверочных мероприятий в соответствующих органах, передачи обращения физического лица в компетентные органы для их разрешения по существу. Функциональный профиль Омбудсмена также охватывает консультативно-разъяснительную деятельность, направленную на детерминацию способов и средств защиты прав человека, наряду с мероприятиями по повышению информированности и правовой грамотности населения.

Надзорную вертикаль в Казахстане замыкают органы прокуратуры, осуществляющие высший надзор за соблюдением законодательства о защите персональных данных (ст.28 Закона «О персональных данных») [212]. Реализация надзорных функций охватывает проверку соблюдения законодательства, анализ правового положения и верификацию состояния законности и вступивших в силу актов. При этом надзорная компетенция прокуратуры характеризуется строгой

детерминированностью по кругу инициаторов и целевой направленности. Проведение проверочных мероприятий допускается на основании поручений Президента либо уполномоченных должностных лиц органов прокуратуры. Целевой вектор проверочных процедур ориентирован на обеспечение правовых гарантий уязвимых категорий населения, а также на превенцию ущерба интересам общества и государства в ситуациях, сопряженных с угрозой жизни, здоровью и безопасности. Кроме того, к сфере полномочий прокуратуры относится контроль за соблюдением государственной правовой статистики, легитимностью информационных потоков в пользовательской среде. При констатации неправомерного получения сведений на прокурора возлагается профессиональная обязанность по принятию мер надзорного и правового реагирования.

Судебная защита персональных данных осуществляется в рамках гражданского, административного и уголовного судопроизводства, где Гражданский кодекс РК гарантирует возмещение убытков и компенсацию морального вреда за нарушение законодательства о неприкосновенности частной жизни и законодательства о персональных данных [213]. Противоправное посягательство на приватность квалифицируется как достаточное основание для требования денежной компенсации. Однако при определении размера компенсации судебные инстанции руководствуются критериями разумности и справедливости, оценивая жизненную важность нарушенных основных прав и степень испытываемых индивидом нравственных страданий.

Наряду с фундаментальным значением законодательного органа в формировании нормативно-правового базиса, а также весомым вкладом института Омбудсмана, органов прокуратуры и судебной системы в обеспечение защиты права на неприкосновенность частной жизни, роль исполнительного органа в общей архитектуре государственного регулирования представляется не менее значимым компонентом защиты персональных данных. Практическая деятельность исполнительной системы по реализации законодательных предписаний и обеспечению их соблюдения детерминирует состояние защищенности прав и интересов субъектов персональных данных, а также риски возникновения потенциального ущерба. Правоохранительная функция исполнительных государственных органов хотя и ограничена отраслевой сферой регулирования, охватывает важные аспекты имплементации норм, профилактики и предупреждение нарушений прав человека, что остается приоритетной государственной задачей в любой сфере регулирования [209, стр.115].

Функционирование исполнительного органа основано на законе, который конкретизирует предмет, сферу деятельности государственного органа и объем властных полномочий. В этой связи дальнейшее изложение материала сфокусировано на функциональном и проблемном исследовании казахстанских нормативных требований и правоприменительной практики в деятельности казахстанского регулятора. Деятельность уполномоченного органа анализируется

через призму европейских правовых стандартов к организации работы надзорных институтов в области защиты персональных данных.

Институциональное оформление специального регулятора по защите персональных данных в Казахстане состоялось в 2020 году. В соответствии с общемировыми правовыми тенденциями учреждение данного института было реализовано посредством законодательной детерминации действующего государственного органа, на который были возложены функции по защите персональных данных [214]. Практическое воплощение данного подхода выразилось в наделении действовавшего на тот момент Министерства Цифрового Развития и Аэрокосмической Промышленности (МЦРИАП) компетенциями уполномоченного органа по защите персональных данных, что получило законодательное закрепление в законе [215].

При этом МЦРИАП осуществляло руководство в нескольких отраслях, что исходя из полифункционального статуса и наименования органа не исключало дефицита ресурсов для обеспечения эффективного регулирования в сфере защиты персональных данных. В дальнейшем, в контексте реализации Послания Главы государства К.Токаева народу Казахстана «Казахстан в эпоху искусственного интеллекта: актуальные задачи и их решения через цифровую трансформацию» в стране была осуществлена реформа государственного управления [216]. В ходе преобразований, ориентированных на совершенствование системы государственного управления, МЦРИАП было преобразовано в Министерство искусственного интеллекта и цифрового развития (МИИЦР) [217, 210].

Набор функций, детерминированный Законом «О персональных данных», сводится преимущественно к трем ключевым блокам полномочий: регулирующему, инспекционному и корректирующему.

К регулятивной плоскости относится утверждение правил сбора и обработки персональных данных и мер по их безопасности, определение порядка интеграции с государственным сервисом контроля доступом персональных данных, а также разработка других правовых актов подзаконного уровня. Вместе с тем нормативный анализ свидетельствует о том, что в большинстве случаев, подзаконное регулирование характеризуется избыточным дублированием законодательных предписаний. Подобный подход регулятора препятствует содержательному раскрытию смысла норм законодательных актов и детальной регламентации механизмов практического применения.

Блок корректирующих и следственных полномочий МИИЦР включает в себя инструментарий по запросу информации, уведомлению о нарушениях и потенциальных угрозах для безопасности персональных данных, осуществлению государственного контроля за соблюдением законодательства о защите персональных данных, а также вынесению процессуальных документов по результатам проверок с требованиями об устранении выявленных нарушений и привлечению к административной ответственности.

В структуре МИИЦР функции уполномоченного органа в области защиты персональных данных реализуются Комитетом информационной безопасности (КИБ). Анализ регламентирующих документов КИБ показывает, что из общего числа 94 закрепленных функций непосредственно к защите персональных данных относятся только 20. Примечательно, что 11 из них ориентированы на разработку нормативных актов, создание правовой основы для которой на сегодняшний день уже фактически завершено [218, 219]. Хотя Положением на КИБ возложено рассмотрение индивидуальных обращений о целевой релевантности содержания и способов обработки персональных данных с принятием соответствующего решения, в компетенции КИБ по-прежнему отсутствуют консультативные полномочия, характерные для европейских надзорных органов. Практическая реализация функции по рассмотрению обращений физических лиц выявляет превалирование формального подхода: ответы зачастую содержат избыточное цитирование положений законодательства без предоставления комплексных и детальных пояснений по его интерпретации и применению. Подобное механическое дублирование норм законов («copy/paste») свидетельствует о недостаточной реализации принципов «слышащего» и профессионального государства [220, раздел 4]. Согласно Концепции развития государственного управления в Республике Казахстан до 2030 года, приоритет отдается оперативности предоставления информации, что нередко происходит в ущерб ее комплексной корректности и содержательной полноте [220, раздел 5]. В результате уполномоченный орган своевременно реагирует на запросы и обращения, но не всегда обеспечивает их качественное и исчерпывающее разрешение.

Данная ситуация подтверждает сохранение системных кадровых проблем, отмеченных в Концепции развития государственного управления в Республике Казахстан до 2030 года, в частности – недостаточную профессиональную компетентность государственных служащих, обусловленную дефицитом сотрудников с профильной специальностью, несовершенством системы отбора и оценки кадров, отсутствием эффективной системы актуализации знаний и повышения квалификации, способной восполнить пробелы в прикладных отраслевых навыках [220, раздел 2]. В противоположность отечественной практике, европейские исследователи акцентируют внимание на высокой степени экспертности разъяснений и консультаций надзорного органа в области защиты персональных данных [206, стр.1]. Если GDPR устанавливает императивные требования к профильной квалификации, практическому опыту и специальным навыкам сотрудников уполномоченного органа, то в Казахстане доминирует концепция сервисной государственной службы. В рамках данного подхода компетентностный профиль государственного служащего ориентирован на выполнение организационных, процедурных и административных функций внутри государственного аппарата. Это ведет к превалированию управленческих навыков над содержательным отраслевым опытом и препятствует формированию

комплексного, всестороннего знания специфики регулируемых общественных отношений в сфере обеспечения информационной приватности.

Указанный институциональный и кадровый дефицит закономерно обуславливает существенный разрыв в уровне фактической защищенности и информированности казахстанских субъектов персональных данных в сравнении с европейскими резидентами. Если в ранее рассмотренных моделях Эстонии и Германии надзорные органы выступают активными проводниками правовой грамотности, то в отечественной практике информационные ресурсы регулятора носят преимущественно декларативный характер. В частности, тематический раздел на официальном сайте МИИЦР РК ограничен лишь констатацией права граждан на обращение в случае выявления фактов незаконного сбора или обработки персональных данных (<https://www.gov.kz/memleket/entities/maidd/activities/9552?lang=ru&parentId=6>).

Подобный подход де-факто перекладывает бремя первичной прямой квалификации инцидента на само физическое лицо, предполагая наличие у него специальных знаний о критериях неправомерности таких действий. Более того, акцент уполномоченного органа на строго регламентированный законодательством порядок приема и рассмотрения обращений и необходимости предоставления убедительных данных и доказательств правонарушения создает дополнительные институциональные барьеры, что в отличие от европейской практики экспертного сопровождения препятствует эффективной реализации прав личностью и ограничивает возможности для повышения правовой грамотности населения.

Данная деструктивная тенденция экстраполируется и на уровень внутриорганизационного контроля, где по аналогии с европейским институтом корпоративного офицера по защите персональных данных (DPO) в 2020 году был внедрен императив о назначении лица, ответственного за организацию обработки персональных данных (ст.25 Закона «О персональных данных»). Однако, в то время как риск-ориентированный европейский подход устанавливает обязанность назначения офицера лишь при наличии определенных условий, таких как обширный мониторинг или обработка чувствительных сведений, казахстанская модель обязывает всех собственников и операторов баз, являющихся юридическими лицами, назначать ответственное за обработку данных лицо независимо от объема или характера обрабатываемых данных. Существенное расхождение прослеживается и в плоскости квалификационных требований: если GDPR детерминирует назначение DPO его профессиональными качествами и знаниями законодательства, то отечественные нормы не устанавливают требований к компетенциям и опыту. Полярные подходы демонстрируют также правовой статус и степень независимости специалиста, поскольку GDPR гарантирует DPO автономию и защиту от корпоративных санкций, в то время как Закон «О персональных данных» отсылает к общим нормам трудового или гражданско-правового законодательства, не обеспечивая специальных гарантий

[221]. Функциональный блок обязанностей в европейской практике носит экспертно-контрольный характер, включая консультирование и оценку рисков, тогда как в Казахстане постулируются ограниченные обязанности по внутреннему комплаенсу, информированию сотрудников о требованиях законодательства и обработке индивидуальных обращений субъектов данных. Таким образом, если европейские стандарты формируют фигуру независимого экспертного контролера, то казахстанская норма закрепляет роль административного исполнителя, что при отсутствии нормативных требований к квалификации и гарантиям автономии создает риски трансформации данной институциональной единицы в сугубо формальный инструмент, не способный обеспечить качественную защиту персональных данных в дополнение к существующим проблемам государственного надзора. Системные изъяны внутреннего корпоративного контроля закономерно дополняют несовершенство государственного надзора.

Наряду с реализацией регулятивных и контрольно-надзорных полномочий, институциональный базис деятельности МИИЦР РК включает формирование Консультативного совета по вопросам персональных данных и их защиты, порядок формирования и функционирования которого определяется самим министерством. Целью наделения министерства функцией по созданию консультативного совета являлось рассмотрение проблемных вопросов сферы, а также согласование интеграции информационных систем, обрабатывающих персональные данные [222, п.136 Сравнительной таблицы]. Созданный министерством Консультативный совет состоит из 57 участников, представляющих различные государственные органы, национальные компании, банковский сектор, телекоммуникационные компании, некоммерческие организации и других лиц [223]. Деятельность Консультативного совета носит выраженный межведомственный характер и ориентирована на предоставление предложений и консультаций по реализации государственной политики в области персональных данных и их защиты. Однако в функциональном перечне данного органа отсутствуют задачи по взаимодействию с населением, повышению правовой грамотности и непосредственному содействию гражданам в реализации своих прав.

В сопоставлении с практикой европейских надзорных институтов деятельность казахстанского регулятора в области защиты персональных данных на текущем этапе носит ограниченный характер, ориентированный на реактивно-санкционную модель вместо превентивного регулирования, направленного на недопущение нарушений. Именно дефицит консультативных механизмов уполномоченного органа по защите персональных данных существенно осложняет реализацию прав субъектами персональных данных и препятствует формированию качественной системы защиты персональных данных в стране.

Описанные проблемы казахстанского регулирования в области персональных данных усугубляются многофункциональностью и мультисекторным характером деятельности МИИЦР РК. Представляется

необходимым либо учреждение автономного ведомства, либо глубокая конкретизация полномочий и функционала существующего органа для обеспечения эффективности правоприменения. Это требует создания организационных и нормативных инструментов, позволяющих разъяснять положения законодательства, обеспечивать его единообразное исполнение контролерами и обработчиками данных, а также гарантировать полноту реализации прав субъектов данных.

Проведенный нормативный анализ свидетельствует о том, что европейские страны располагают комплексным и детальным регулированием в рассматриваемой сфере, закрепляя в законе конкретные и более широкие функции специализированных независимых уполномоченных органов по защите данных. Ключевое место в их деятельности занимает повышение осведомленности субъектов данных и других участников информационного обмена, издание руководств (guidelines) и заключений (opinions) по вопросам интерпретации и имплементации профильного законодательства.

В данном контексте важно подчеркнуть, что охранительная функция государства не должна исчерпываться исключительно мерами контроля, надзора и санкциями, которым в последнее время уделяется приоритетное внимание в рамках отечественного правотворческого процесса. Деятельность государства по защите прав и свобод предполагает также профилактику нарушений и проведения системной разъяснительной работы с обществом, бизнесом и органами публичной власти. Поскольку информационная грамотность общества является прямым продуктом такой деятельности, отсутствие в казахстанском законодательстве прямо установленных консультативных функций ограничивает возможности регулятора, который не может выходить за пределы предусмотренных законом полномочий. Соответственно, расширение охранительной функции профильного органа требует обязательного законодательного закрепления.

Европейские правовые стандарты диктуют необходимость обеспечения подлинной независимости и самостоятельности уполномоченного органа по защите персональных данных. Несмотря на то, что казахстанский уполномоченный орган по защите персональных данных в лице МИИЦР является отдельным государственным органом и обладает некоторой автономией, чрезмерно широкий спектр регулируемых им областей и функций (более 500) оказывают деструктивное влияние на эффективность его деятельности. органа в области защиты персональных данных [210, п.15]. Представляется, что уполномоченный орган должен обладать большей самостоятельностью, не входя в структуру многоотраслевого министерства и будучи свободным от избыточных функций. Как отмечают зарубежные исследователи, множественность задач государственного органа чаще всего приводит «к дополнительной работе без предоставления адекватных ресурсов» [207, стр.34]. При этом именно независимость надзорного органа позволяет ему сконцентрироваться «на

интерпретации и применении законодательства, обеспечить его хорошее понимание и повысить осведомленность в сообществе» [207, стр.38].

Наконец, эффективная работа регулятора невозможна без персонала, обладающего узкопрофильной квалификацией. Зарубежные исследования демонстрируют, что в штате профильного уполномоченного органа доля сотрудников со значительными знаниями или опытом в области информационно-коммуникационных технологий составляет не менее 50% [224, стр.205]. Именно качественная надежность и экспертный уровень персонала позволяют надзорному органу результативно осуществлять функции по защите персональных данных [224, стр.208]. Основываясь на европейском опыте, Казахстану необходимо пересмотреть подходы к кадровой политике, акцентируя внимание на содержательной и экспертной квалификации государственных служащих в сфере защиты персональных данных.

Следует констатировать, что планировавшиеся государством законодательные инициативы, в частности проект Цифрового Кодекса РК, не содержали новых положений в отношении уполномоченного органа по защите персональных данных [132]. Принятый Цифровой Кодекс РК также не привнес качественных изменений в правовой статус регулятора в области цифровизации и спектр его полномочий в области защиты персональных данных. Деятельность МИИЦР ориентирована на реализацию широких направлений социально-экономической политики государства, обороноспособности, безопасности и общественного порядка, однако прямая связь этих задач с защитой персональных данных выражена в Цифровом Кодексе РК неявно. Кроме того, Цифровой Кодекс РК также не закрепляет консультативные функции в рамках компетенции уполномоченного органа по цифровизации в целом или в отношении защиты персональных данных в частности [44, ст.14]. Подобный подход сохраняет институциональный пробел в системе защиты прав граждан, так как ни Цифровой Кодекс РК, ни Закон «О персональных данных» не наделяют уполномоченный орган консультативных функций в области защиты персональных данных. Это упущение вызывает вопросы о согласованности нормативно-правовых рамок, регулирующих цифровую среду и защиту персональных данных в государстве.

Помимо прочего системный анализ положений Цифрового Кодекса и Закона «О персональных данных» выявляет отсутствие норм об организационной форме регулятора, оставляя без ответа вопрос об организационной форме регулятора: сохранит ли он статус подразделения в структуре многоотраслевого министерства или будет преобразован в самостоятельный независимый орган по защите персональных данных. Ни Цифровой Кодекс, ни Закон «О персональных данных» не наделяют уполномоченный орган консультативными функциями, аналогичными европейским, не предъявляют требований к квалификации членов уполномоченного органа. Дефицит консультативных механизмов и требований к специальной квалификации персонала, сопоставимых с европейскими стандартами, служит индикатором периферийного статуса института защиты

персональных данных в правовой системе Казахстана, что объективно обуславливает состояние институциональной уязвимости субъектов данных.

Обеспечение прав и свобод граждан является фундаментальной функцией современного демократического развитого государства [95, стр.26], при этом права личности коррелируют с императивной обязанностью государства по их реализации и защите [196, стр.62]. Несмотря на то, что гарантии защиты персональных данных в Казахстане декларируются как комплексная система законодательных, имплементирующих и контрольных мер, практическая реализация этой охранительной функции сталкивается с рядом системных проблем.

Во-первых, профильные задачи уполномоченного органа по защите персональных данных фактически «растворены» в обширном перечне других задач и функций мультисекторного министерства, МИИЦР, что препятствует их качественному и автономному исполнению. Для преодоления этой диффузии функций необходимо институциональное обособление регулятора и наделение его консультативными функциями по примеру европейских стран. Во-вторых, наблюдается дефицит узкопрофильной компетентности государственных служащих, вынужденных совмещать регулирование вопросов приватности с другими задачами и функциями одного многоотраслевого министерства.

Глобальная тенденция к гармонизации национальных правовых систем с Европейским Регламентом GDPR обусловлена необходимостью обеспечения адекватного уровня защиты данных наличием специализированных независимых органов. Однако в Казахстане данный процесс характеризуется низкой динамикой. Учитывая полифункциональный характер МИИЦР, представляется необходимым учреждение самостоятельного государственного органа, полномочия которого будут четко конкретизированы для обеспечения эффективности правоприменения. Это позволит сформировать нормативные и организационные инструменты для разъяснения законодательства, обеспечения его единообразного исполнения участниками правоотношений в сфере защиты персональных данных и полноценной реализации прав субъектов.

Подобное реформирование и создание независимого профильного органа полностью соответствует установкам Концепции совершенствования государственного управления в РК до 2030 года, которая ставит задачу формирования оптимального и эффективного государственного аппарата через переосмысление роли и функций государства, а вместе с ним структуры и размера всего государственного аппарата [220, раздел 5].

Проведенный сравнительный анализ выявляет существенные расхождения казахстанского государственного регулирования с европейской, эстонской и германской моделями. Прежде всего в вопросе институциональной независимости наблюдается контраст между полной автономией органов Европейского союза и статусом казахстанского регулятора как структурного подразделения мультисекторного министерства, что закономерно детерминирует дефицит

ресурсов и потенциальный конфликт ведомственных интересов. В то время как германский Федеральный комиссар по защите данных (BfDI) избирается Бундестагом, а эстонская Инспекция по защите данных (AKI) функционирует в качестве самостоятельного субъекта с прозрачной организационной структурой, отечественная модель остается в рамках иерархической системы государственного аппарата. Существенные отличия прослеживаются в реализации консультативного потенциала: если деятельность МИИЦР характеризуется преимущественно реактивно-санкционной направленностью, то европейские институты ориентированы на превентивное регулирование через издание руководств (guideleines) и методических пособий (Orientierungshielfen), формирующих единообразный вектор правоприменения. Так при наличии более 60 детализированных документов на портале EDPB, казахстанский информационный ресурс ограничен лишь декларативными положениями о праве граждан на обращение и требованиями к доказательной базе правонарушений. Кадровая политика также демонстрирует разные подходы: штат эстонской Инспекции на 70% укомплектован специалистами с юридическим образованием, а общеевропейские стандарты предполагают наличие профильных ИКТ-компетенций как минимум у половины сотрудников, в то время как в Казахстане сохраняется системный дефицит специалистов с узкопрофильной квалификацией. Наконец, специфика инструментов взаимодействия проявляется в том, что в европейской модели институт корпоративных офицеров по защите данных превращает процесс соблюдения в органичный элемент взаимодействия «субъекты данных – контролер / обработчик – регулятор», в Казахстане же правовой статус ответственного за обработку данных лица и закрытый характер деятельности Консультативного совета смещают акцент на формальное администрирование процедур, что не позволяет сформировать транспарентную экосистему защиты персональных данных и обеспечить эффективное экспертное посредничество между государством, бизнесом и обществом.

В заключение следует отметить, что по аналогии с моделью GDPR ив. Целях минимизации рисков для интересов личности, нормы Цифрового Кодекса РК и Закона «О персональных данных» необходимо дополнить исчерпывающими положениями, регламентирующими консультативные и осведомительные функции отдельного уполномоченного органа по защите персональных данных, а также устанавливающими стандарты профессиональной квалификации его сотрудников.

3.3 Пути совершенствования государственно-правового регулирования защиты персональных данных в РК

Современные юридическая теория и практика расширили интерпретацию частная жизнь под влиянием технологического развития и инноваций, проникших во все сферы жизни общества, включая государственное управление и

администрирование потоков информации как между государственными органами, так и между государством и бизнесом, государством и населением, а также между субъектами частной сферы. Повсеместное использование электронных информационных ресурсов, программ и приложений, социальных сетей позволяют размещать и вносить множество различной информации о человеке, что делает его уязвимым и угрожает его частной жизни. Если ранее, исторически, наблюдение и слежка воспринимались как вмешательство со стороны государства, то сегодня наблюдение и отслеживание в онлайн-пространстве стало важной составляющей экономической деятельности частных организаций. Крупные частные корпорации (Google, Meta (Facebook), iHerb, TikTok, Amazon, OLX, Yandex и др.), а также финансовые институты, приобретают власть, сопоставимую с государственной, а зачастую и превосходящую её технологически.

Со стремительным развитием «экономики данных», Gov-tech, edtech, fintech и прочих областей цифровизации, использованием платформ, интернет-ресурсов, социальных сетей, мессенджеров, выявились и другие существенные проблемы законодательства о защите персональных данных. Государственные и коммерческие участники общественных отношений перевели физическое взаимоотношение в виртуальное, оцифровав практически все процессы, которые не могут быть осуществлены без информации и персональных данных.

Интеграция информационной системы «электронного правительства» с информационными системами банков второго уровня позволила последним получить доступ к персональным данным «электронного правительства».

Функционирование интеграционной платформы *Smart bridge*, инициированной МЦРИАП РК и АО «НИТ», выступает как мост, обеспечивающий оперативную синергию государственных баз данных и информационных систем частного сектора, благодаря которому вывод государственных услуг стал значительно проще [225]. Практическая реализация данной модели, в частности в рамках проекта онлайн-регистрации индивидуального предпринимателя, объединила информационные системы МЦРИАП, Kaspi.kz, Комитета государственных доходов и государственной базы данных «Е-лицензирование» [226]. Согласно позиции представителей финансового сектора, стратегической задачей в сфере GovTech является полная цифровизация бизнес-процессов, предполагающая переход к формату «невидимого правительства» (*Invisible Government*) [225]. Данная модель предусматривает делегирование функций взаимодействия с государством банковским структурам, что нивелирует необходимость прямого обращения граждан в центр обслуживания населения (ЦОН) или к государственному portalу *Egov*. Статистические данные подтверждают эффективность этой децентрализации: через приложения Halyk, Kaspi, Freedom оказано более 11 млн. государственных услуг [227]. Трансформация роли *Egov* из монопольного поставщика в один из каналов получения государственных услуг подтверждает возможность получения 48 государственных услуг в приложении банка [225].

Интеграция государственных сервисов в банковские экосистемы позволяет финансовым организациям аккумулировать сведения, выходящие за рамки их основной деятельности, и связать финансовые аспекты с различными жизненными ситуациями граждан. В приложениях банков сохраняются цифровые копии медицинских справок, сведения о пенсионных и социальных отчислениях, о недвижимости, истории владения автотранспортом [225]. Это ведет к созданию избыточных массивов данных в электронных хранилищах банков, предоставляя сотрудникам организаций косвенный доступ к информации, содержащейся в личном кабинете физического лица на веб-портале «электронного правительства»: от сведений о состоянии здоровья и семейном статусе до данных о налогах и статусе опекуна. Через банковские приложения организации аккумулируют сведения, выходящие за рамки банковской тайны, тем самым осуществляется непрозрачный сбор избыточных сведений.

Казахстанские банки заинтересованы в доступе к огромному количеству личной информации электронного правительства, что дает банкам возможность в своих интересах улучшить свои сервисы, расширить возможности банковских приложений для еще большего сбора и обработки персональных данных, исключить бумажную волокиту и предоставить государству информацию от финансовых институтов взамен на полученные персональные данные.[226] Иными словами, для банков персональные данные служат неким сырьем для коммерциализации своих продуктов и увеличения прибыльности, а для государства – «платежным средством» за информацию о финансовой деятельности и финансовом статусе физических лиц.

Населению такое взаимодействие платформ коммерческих банков и электронного правительства представлено как технологический прорыв в услугах и удобство. Однако, очевидно нарушение конституционного права на неприкосновенность личности и уважение частной жизни, которое подразумевает информационную составляющую, наличие данных, информации о человеке. Удобство и технологический прорыв не учитывают фундаментальное право на приватность и защиту персональных данных, а наоборот, дополняют существующую проблему «слежки» в коммерческом секторе. Несмотря на широкую и нечеткую (ill-identified) концепцию неприкосновенности частной жизни, она остается хорошо понимаемой [228, стр.9].

Проблема законодательного регулирования интеграции государственной платформы и базы данных «электронного правительства» с платформами коммерческих банков не решает вопросы защиты персональных данных, не раскрывает пределы использования персональных данных, сбора и обработки персональных данных, не является прозрачной и понятной для физического лица, нарушает автономию в принятии решений и право контроля за использованием персональных данных. Именно данные вопросы должны быть урегулированы и изложены в законах ясно, без двусмысленностей, содержать ясные права и обязательства, содержать меньше отсылочных положений как к правовым актам,

так и к гражданско-правовым договорам и корпоративным документам, исключая произвол коммерческого сектора по отношению к физическим лицам [134, стр.52].

Цифровизация в государственном и коммерческом секторе не ставят во главу угла фундаментальные права и интересы человека, защищать которые призвано государство. Внедрение функционала «государственные услуги» в приложения банков второго уровня через интеграцию платформ коммерческих банков и «электронного правительства» выявляет ряд системных противоречий, позволяя банкам собирать, обрабатывать и хранить практически весь массив информации о личности. По своей правовой природе государственная услуга является осуществлением функции государства и не может исключать элемент государственного присутствия. Однако несмотря на то, что действующее законодательство допускает участие банков в качестве «партнерских организаций» [229, 230, 231], ограничивая их роль приемом заявлений и выдачей результатов, фактическая технологическая интеграция банковских платформ с платформой «электронного правительства» превращает их в полноценных посредников, обладающих доступом к государственной базе данных.

В условиях глобальной цифровизации общества, когда вопрос о защите персональных данных ставится еще более остро, важнейшая роль отводится праву как средству социального управления, инструменту осуществления функций государства по обеспечению конституционного права на неприкосновенность частной жизни и защиты персональных данных. Через усовершенствование положений Закона «О персональных данных» государство создаст условия для надлежащего правоприменения и обеспечит защиту права человека на неприкосновенность частной жизни.

Системные противоречия, выявленные при анализе интеграции банковских платформ с платформой «электронного правительства», имеют общую природу с проблемами всех иных субъектов цифрового рынка Казахстана: их первопричина заложена в отсутствии в национальном законодательстве императивных специальных принципов и четко детерминированных обязанностей собственников и операторов баз персональных данных. Данный правовой вакуум подтверждается при изучении деятельности популярных онлайн-платформ в Казахстане, «Каспи», «Тенгриный» и «Крыша», продемонстрировав общие для Казахстана проблемы в отношении обработки персональных данных [232, стр.38-39]. Общий уровень защиты персональных данных на этих платформах не соответствует стандартам ЕС, установленным GDPR, с заметными проблемами, включая отсутствие прозрачности и ограниченный контроль пользователей над данными. В политиках конфиденциальности отсутствует подробная информация о сборе согласия и возможностях управления данными пользователей.

В таких условиях центральное значение приобретает институт информированного согласия физического лица. Во-первых, оно обеспечивает

прозрачность в отношении того, какие данные собираются, как и для чего обрабатываются. Обладание этой информацией при сборе персональных данных с одной стороны, может создать уверенность физическому лицу о справедливости и разумности их сбора и обработки, а с другой стороны, означает принятие контролёром и оператором персональных данных обязательств по законному и справедливому использованию данных. Возможно наличие информированного согласия может только создавать иллюзию понимания физическим лицом происходящих действий и не гарантирует добросовестной обработки персональных данных. Тем не менее, наличие соответствующих положений в Законе «О персональных данных» обеспечивает исполнение закона, является более значимой и авторитетной гарантией для физического лица о неизбежности ответственности контролера и оператора данных в случае нарушения закона. Большинство ученых согласны с необходимостью информированного согласия, которое является ключевым условием для принципа законности. Но некоторые ученые считают информированное согласие чрезмерным требованием и малоэффективным инструментом ввиду субъективных особенностей физического лица, которое либо не имеет достаточной цифровой грамотности, либо автоматически соглашается со сбором и обработкой данных, не читая политику конфиденциальности. Солове отмечает, что большинство согласий на конфиденциальность расплывчаты, и предлагает признать новый тип согласия, называемый «смутным согласием» (*murkey consent*), которое существует между полным согласием и несогласием. [233, стр.42-43] Он считает, что полное согласие, предписанное GDPR, часто недостижимо, а несогласие неуловимо, поскольку всегда есть способы заявить о формальном согласии — например, с помощью «галочки», принятия файлов cookie или просто неспособности прочитать или понять политику конфиденциальности. Соответственно, концепция «смутное согласие» уже нашла свое отражение в цифровой реальности на практике, что ставит вопрос о необходимости формализовать ее в законах. Однако закрепление «смутного согласия» в законе сопряжено с критическими рисками и негативными последствиями в результате действий, совершенных без должного внимания или ознакомления с условиями сбора и обработки, что в итоге возлагает на субъектов данных вину за возможный ущерб. В то же время законодатель оказывается в ситуации регулятивного тупика: юридическая формализация отказа от требований об информированности и осознанности невозможна, так как это подрывает фундаментальные основы прав личности, но и сохранение этих стандартов в качестве декларативных норм закрепляет разрыв между требованиями закона и реальной практикой, не обеспечивая защиту персональных данных.

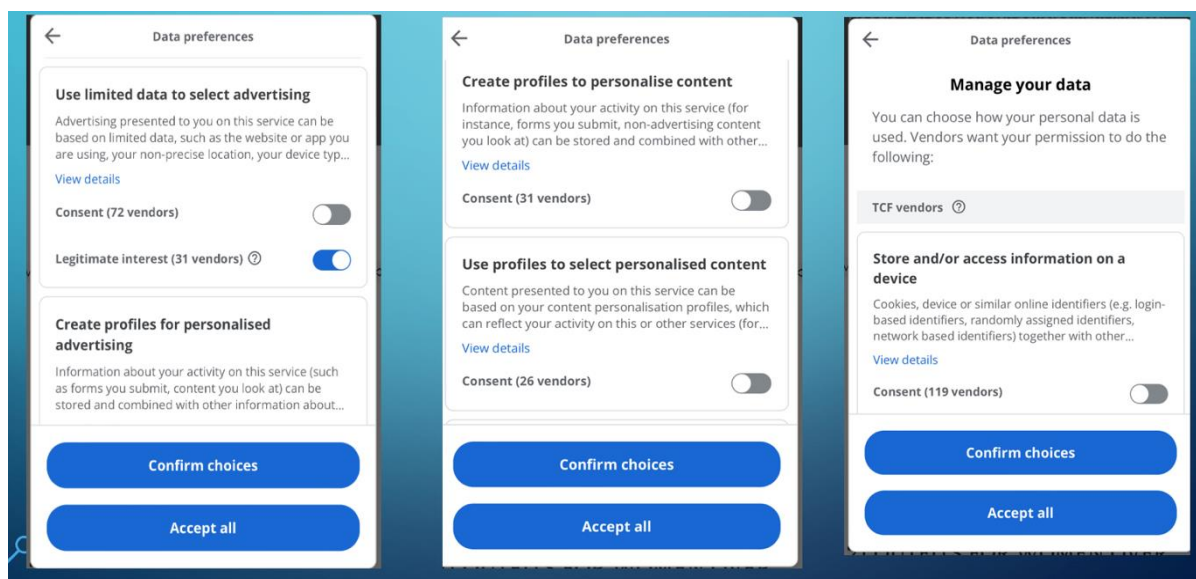
В качестве эффективного инструмента преодоления указанных пробелов в защите персональных данных выступают технические средства защиты, такие как принципы и обязательства «конфиденциальности по замыслу» (*Privacy by*

Design) и «конфиденциальности по умолчанию» (Privacy by Default). Автоматизация процессов связана со сбором и обработкой информации, при этом алгоритмы «прописывают» и программируют сбор данных для любых операций. Следовательно, тип и пределы данных технически, алгоритмически, можно ограничить при их сборе и использовании как по типу и количеству (объему) информации, так и по цели использования. Иными словами, технология может служить инструментом регулирования, быть «встроенной» в алгоритмы. Однако, сама по себе технология может добиться цели и эффективно работать, если она подкреплена и дополнена нормами закона, как это реализовано в GDPR.

GDPR впервые на нормативном уровне включил понятие «защита данных по замыслу» и «конфиденциальность по умолчанию» - *Data Protection by Design, Data Protection by Default*. Статья 25 предусматривает, что контролеры должны осуществить организационные меры для «встраивания» защиты конфиденциальности на протяжении всей разработки, а также в процессы сбора данных. Контролеры должны также обеспечить, чтобы персональные данные обрабатывались «по умолчанию» с учетом принципов минимизации данных, ограничения цели, ограничения хранения и «по умолчанию» не будут доступны без вмешательства лица неопределенному числу физических лиц.

Нормативное закрепление Европейским Союзом самих технологий как средства защиты персональных данных продемонстрировало, что европейское законодательство о защите данных и его правоприменительная практика подталкивают технологические компании к внедрению требуемых практик. Для пользователей не осталось незамеченным требование об уведомлении в отношении куки-файлов, практика *opt-in* («подпишись») вместо *opt-out* («отпишись»), внедрение *privacy-by-design* и *privacy-by-default*. Например, при изменении местонахождения (локации) из Казахстана в Европу, Эстонию, можно увидеть, что любые приложения, поисковые системы Google и Safari по-разному работают в Эстонии и в Казахстане. Для использования онлайн-сервисов и приложений в Эстонии необходимо выбрать вид и способ использования персональных данных (см. рисунок).

Рисунок №2: Пример технического внедрения «privacy-by-design» и «privacy-by-default» в мобильных приложениях по GDPR.



Технологии конфиденциальности по замыслу и по умолчанию изображены на рисунке как «переключатели» настройки сервиса приложения. Таким образом, онлайн-сервисы, приложения и IT продукты спроектированы так, что технологии конфиденциальности уже «вшиты» и «встроены» поскольку это обязательство разработчиков и требование закона, GDPR. Цель этих требований – защита персональных данных, контроль физического лица за доступом к персональным данным, прозрачность сбора и обработки, информированность о лицах, использующих данные и целях использования. Ибраева А.С. отмечает, что закрепленные в законах технологии «конфиденциальности по замыслу» и «конфиденциальности по умолчанию», предоставляя людям контроль над своими персональными данными, одновременно гарантируют технологическую защиту [125]. В дискуссиях о сложности регулирования и соблюдения GDPR, член Европарламента Маркета Грегорова (Markéta Gregorová) отметила, что соблюдение GDPR может быть простым, если будут реализованы принципы «по замыслу» и «по умолчанию» [234]. Данные технологические меры устойчивы к изменениям, просты среди сложности и последовательны в различных инновациях [235, стр.14].

Действующий Закон «О персональных данных» и Закон «Об информатизации» содержит общее требование для субъектов регулирования по обеспечению защиты персональных данных и самих объектов информатизации. Единые требования в области информационно-коммуникационных технологий и информационной безопасности устанавливают требования к антивирусным, криптографическим средствам защиты информации, соблюдению сертификации и иные требования [236]. Область применения Единых требований ограничена государственными юридическими лицами, субъектами квазигосударственного сектора, собственниками и владельцами негосударственных информационных систем, интегрированных с информационными системами государственных

органов или предназначенных для формирования государственных электронных информационных ресурсов, собственниками и владельцами критически важных объектов информационно-коммуникационной инфраструктуры. Единые требования не содержат обязательств к «конфиденциальности по замыслу» и «конфиденциальности по умолчанию». Закон «О персональных данных» не содержит обязательств по проектированию систем обработки персональных данных, в том числе обязательств по обеспечению конфиденциальности по замыслу или по умолчанию (*Privacy by Design, Privacy by Default*). Кроме того, обсужденный Мажилисом текст законопроекта об ИИ и изменения в законодательство о защите персональных данных не предусматривал такого обязательства [237]. Принятые в стране Закон РК «Об искусственном интеллекте» и Цифровой Кодекс также не внесли требования о конфиденциальности по замыслу и по умолчанию для собственников и владельцев цифровых объектов и систем искусственного интеллекта. Такой подход в законодательстве означает, что по умолчанию в настройках систем ИИ и цифровых объектов может быть заложен неконтролируемый человеком и возможно неограниченный сбор и обработка персональных данных.

Отсутствие законодательно закрепленных стандартов защиты персональных данных *Privacy by Design, Privacy by Default* в сочетании с дефицитом цифровой и правовой грамотности населения формирует потенциальные риски для сохранения приватности. В числе основных проблем законодательства о защите персональных данных можно выделить ограниченную осведомленность об угрозах конфиденциальности, отсутствие понимания пользователями рисков, связанных с использованием их персональных данных, низкий уровень цифровой грамотности среди интернет-пользователей, отсутствие необходимого минимального уровня правовых знаний, незнание гражданами своих базовых прав [232, стр.34]. Усовершенствование законодательства, в особенности нормативное закрепление принципов защиты персональных данных, массовое просвещение и правовое воспитание помогут преодолеть возникший в стране пробел правовых знаний в сфере защиты персональных данных. Повышению осведомленности в сфере защиты персональных данных на уровне закона может послужить несколько способов. Во-первых, форма и содержание изложения прав субъектов персональных данных в Законе «О персональных данных» значительно отличается от GDPR. Казахстанский закон дает перечень прав физических лиц в одной статье, в то время как GDPR содержит десять отдельных статей, каждая из которых подробно излагает положения по реализации каждого отдельного права субъектом персональных данных и соответствующие требования для контролеров и операторов данных. Во-вторых, должна быть ясная и прямая обязанность организаций по предоставлению более полной и понятной информации о собираемых ими персональных данных, их использовании и о том, как физические лица могут реализовать свои права и контролировать свои данные. Аналогичные

положения предусмотрены статьями 13 и 14 GDPR. В-третьих, GDPR как специальный нормативный акт в области защиты персональных данных в пункте 132 Преамбулы и статье 57.1. закрепляет функцию соответствующего государственного органа по повышению осведомленности и правовой грамотности о защите персональных данных как среди контролёров и операторов данных, так и среди физических лиц. Положения закона должны обеспечить качественную осведомленность как граждан, так и предприятий, что будет способствовать развитию правовой культуры и эффективному исполнению законов [232, стр.38].

Резюмируя вышеизложенное, можно констатировать, что текущий этап развития цифровой экосистемы Казахстана характеризуется диссонансом между темпами технологической экспансии и уровнем правовой защищенности личности, поскольку интеграция коммерческих сервисов с государственными платформами, а также совершенствование частных платформ, включая банковские, порождает расширение масштабов «цифровой слежки» и неконтролируемую коммерциализацию персональных данных. Решение выявленных проблем требует совершенствования законодательства путем закрепления обязанностей о повышении правовой грамотности пользователей систем, внедрению технологий *Privacy by Design*, *Privacy by Default*, а также детальную регламентацию механизмов реализации прав субъекта персональных данных.

ЗАКЛЮЧЕНИЕ

Диссертационное исследование государственно-правового регулирования защиты персональных данных в Республике Казахстан и в Европе позволило выявить ключевые проблемы и тенденции развития данной сферы. Современные реалии высокотехнологичного развития и глобализации требуют от государства более тщательного регулирования и обеспечения неприкосновенности частной жизни, создания четкой и последовательной законодательной базы, правоприменительной практики, компетентного государственного регулирования, реализующего и обеспечивающего защиту права человека на неприкосновенность частной жизни.

Частная жизнь имеет широкую и многоаспектную интерпретацию, включающую несколько сторон проявления частной жизни человека – телесную (физиологическую), пространственную, коммуникационную, имущественную, интеллектуальную, ассоциативную, поведенческую, конфиденциальность принятия решений, информационную. Информационная сторона частной жизни имеет особенное значение, поскольку связана с каждым из других аспектов и проявляется в них, «ее следует рассматривать как другую сторону медали» [8, стр.554]. Информационный аспект частной жизни включает персональные данные, личную информацию о частной жизни, в мировой и казахстанской практике является отдельным объектом защиты и регулирования.

Неприкосновенность частной жизни служит для защиты человека, его автономии, свободы, идентичности, самоопределения и самосозидания, контроля своей частной жизни, определении границ и степени доступа, контроля за коммуникациями. Право на неприкосновенность частной жизни является фундаментальным правом человека, тесно взаимосвязанным с другими основными правами и свободами. Неисчерпывающее понятие частной жизни и ее предназначение для существования человека определяют содержание норм Конституции и основанных на ней правовых актах.

Стремительное развитие информационных технологий требует соответствующего и актуального нормативного закрепления защиты персональных данных, как информационного аспекта частной жизни, обладающего всеми функциями права на неприкосновенность частной жизни, обеспечивающего реализацию физическим лицом автономии, свободы принятия решений, установления пределов вмешательства и контроля за доступом.

В ходе исследования был осуществлен комплексный анализ правовых механизмов реализации права на неприкосновенность частной жизни и защиту персональных данных в Казахстане, выявлены положительные аспекты и недостатки, проведен сравнительный анализ с европейским правом, правовыми актами, деятельностью государственных органов и правоприменительной

практикой. Самостоятельным предметом исследования стали проблемы юридической интерпретации базовых дефиниций, функциональный статус уполномоченного органа, технологические и процедурные барьеры на пути реализации права на защиту персональных данных.

Результаты проведенной научной работы позволили обосновать комплекс рекомендаций, направленных на системную модернизацию отечественного законодательства, его синхронизацию с международными правовыми стандартами и оптимизацию институциональной модели государственного регулирования в сфере защиты персональных данных. Сформулированные выводы подтверждают назревшую потребность в глубоком реформировании нормативного массива и профильного государственного органа. Данные преобразования необходимы для создания действенных механизмов реализации гражданами права на неприкосновенность личных сведений, легитимации специальных отраслевых принципов, а также введения юридических обязанностей для государственных институтов, собственников и операторов баз данных по просвещению населения и повышению его правовой грамотности в цифровой среде.

Основные выводы проведенного исследования состоят в следующем:

1. Терминология и типология «персональных данных» требует четкого, ясного, последовательного и согласованного закрепления в законодательстве. В системе правовых актов специальный Закон «О персональных данных» призван выполнять функцию базового концептуального регулятора и системообразующей нормативной основы, обеспечивающей унификацию толкования и применения положений как специального, так и смежного законодательства. Понятие «персональные данные» и «частная жизнь» имплицитно взаимосвязаны и не могут иметь исчерпывающего значения для целей правоприменения. Специальный закон должен дать четкие и ясные критерии для отнесения определенной информации или элементов, факторов частной жизни и личной информации к категории «персональные данные». Понятие персональные данные должно характеризоваться содержательной широтой, одновременно оставаясь юридически ясным и адаптивным к конкретным ситуациям. Критерии дефиниции «персональные данные» должны обладать ясностью для всех участников общественных отношений – от физических лиц (субъектов персональных данных) до представителей коммерческих и государственных структур – что является необходимым условием для единообразного толкования и правоприменения.

В зависимости от степени «ценности», «существенности» конкретного элемента или идентификатора персональной информации, его взаимосвязи с социально-экономическими правами и последствиями для прав и свобод личности, закон должен закрепить типологию персональных данных, установить ясные критерии, способы и требования к сбору, защите и обработке персональных данных. При этом следует учитывать, что отдельные элементы или

идентификаторы (такие как ИИН) не должны быть взаимоисключающими. Закон должен содержать императивные правила и запреты на определенные действия с персональными данными, совокупное совершение каких-либо действий в отношении одного элемента (идентификатора) личной информации во взаимосвязи и соединении с другим элементом (идентификатором) в то числе из разрозненных источников. Именно связанное использование различных персональных сведений в современных цифровых экосистемах влечет наиболее значимые риски и неблагоприятные последствия для физического лица.

В связи с этим рекомендуется имплементировать термин «персональные данные», максимально приближенное к стандартам GDPR, поскольку данное понятие включает в себя аспекты проявления частной жизни, а также признание персональными данными сведений, которые допускают возможность идентифицировать личность косвенным способом, как например ИИН. Такой подход позволит учесть темпы развития технологий и появление новых идентификаторов физического лица и предупредить риски нарушения прав и законных интересов личности. Детальные предложения по совершенствованию понятийного аппарата Закона «О персональных данных» представлены в Приложении А.

Особого пересмотра требует классификация персональных данных по типу доступа (общедоступные персональные данные и персональные данные ограниченного доступа). Закон должен пересмотреть условия сбора и обработки общедоступности личных сведений с учетом степени их воздействия на права человека. Распространение ФИО, ИИН и некоторых других сведений в общедоступных государственных базах, а также самим физическим лицом, не должно лишать человека права на неприкосновенность личности или ущемлять его защиту. Факт установления или идентификации личности не лишает человека права на уважение частной жизни от какого-либо вмешательства. Правовые рамки сбора и обработки общедоступных персональных данных не должны быть слишком размытыми и выражаться в общих формулировках «запрещается сбор и обработка персональных данных в целях причинения вреда правам и свободам человека». Закон должен конкретизировать и четко определить целевое назначение сбора и обработки общедоступных персональных данных, а также границы допустимого вмешательства.

В качестве универсального принципа предлагается закрепить презумпцию конфиденциальности любых персональных данных «по умолчанию», независимо от установленного режима доступа. Данное требование является универсальным и адаптивным ответом на вызовы, связанные с внедрением новых технологий и неравномерным уровнем цифровой и информационной грамотности различных социальных и возрастных групп населения.

2. Необходимость конкретной, последовательной и ясной формулировки основных терминов и видов операций с персональными данными в национальном законодательстве продиктована требованиями глобальной цифровизации в

обществе. Дефиниции операций по обработке персональных данных, участников правоотношений, связанных со сбором и обработкой персональных данных, должны быть максимально приближены к общепринятым международным терминам, что существенно упростит правоприменительную практику как для отечественных, так и для зарубежных участников правоотношений.

В этой связи понятие «обработка персональных данных» в Законе «О персональных данных» не должно носить ограниченного или исчерпывающего характера. Требуется расширение данного понятия на законодательном уровне путем включения любых операций и действий с персональными данными, совершаемых для любых целей, в том числе действия и операции по профилированию (профайлингу) и псевдонимизации. Кроме того, все виды операций с персональными данными должны получить ясные, конкретные и недвусмысленные юридические описания в законе.

Особого внимания требует детальная регламентация профилирования и таргетированного контента. Данные методы сбора и обработки должны быть законодательно признаны специфическими видами обработки персональных данных, поскольку являются особенно интрузивными, вторгающимися в частную жизнь, нарушают автономию личности, лишают контроля за использованием личной информации, имеют дискриминирующий характер и чреваты манипулированием личностью. В этой связи предлагается не только закрепить профилирование как вид обработки в Законе «О персональных данных», но и синхронизировать понятийный аппарат с Законом «Об онлайн-рекламе».

Концептуальным шагом в сторону гармонизации с международными нормами должна стать трансформация субъектной архитектуры правоотношений. В казахстанском Законе «О персональных данных» предлагается заменить понятия «собственник базы персональных данных» и «оператор базы персональных данных», на понятия «контролер» и «обработчик» соответственно, по примеру Европейского Регламента. Принципиально важно, чтобы описание указанных дефиниций базировалось не вещно-правовых титулах собственности на базу персональных данных, а на фактических функциях и роли участников, вовлеченных в процесс сбора и обработки персональных данных, степени их контроля над целями обработки и обязательствах по отношению к физическому лицу. Данный функциональный подход является прагматически обоснованным: субъективный интерес индивида заключается в сохранности персональных данных и их законном без ущерба использовании, а не в реализации имущественного права в отношении базы данных. Реализация указанных предложений, детально изложенных в Приложении А, позволит создать сбалансированную и современную нормативную базу, отвечающую вызовам цифровой среды и обеспечивающую высокий уровень защиты прав и свобод личности.

3. Специальные принципы защиты персональных данных следует ясно и подробно сформулировать и закрепить в специальном законе в качестве

основополагающих руководящих начал для всех отраслей правового регулирования. На современном этапе социально-экономического и, прежде всего, технологического развития личная информация приобретает особую значимость и форму существования. Процессы сбора, обработки, хранения и распространения личной информации в условиях тотальной цифровизации несут в себе угрозы и создают риски ущерба, которые требуется максимально детально урегулировать положениями закона. Поскольку законодательные органы зачастую не успевают за стремительной эволюцией информационно-коммуникационных технологий, именно правовые принципы выступают в роли адаптивного инструментария - правил «на вырост», позволяющих эффективно устранять конфликты или пробелы в законодательстве и обеспечивать единообразное толкование закона.

Правовые принципы представляют собой «несущую конструкцию» в регулировании общественных отношений. Действующий Закон «О персональных данных» базируется на пяти положениях: (1) соблюдения конституционных прав и свобод человека и гражданина, (2) законности, (3) конфиденциальности персональных данных ограниченного доступа, (4) равенства субъектов персональных данных, собственников, операторов, (5) обеспечения безопасности личности, общества и государства. Однако данные принципы носят преимущественно декларативный характер и не раскрываются в тексте закона. Являясь абстрактными идеями, они не имеют прямой направленности на специфику процессов обработки данных, что делает их малоэффективными и зачастую позволяют правоприменителю игнорировать их без каких-либо последствий и санкций.

В противовес отечественному подходу, европейская модель, основанная на GDPR, характеризуется значительно большей конкретикой. Европейский Регламент устанавливает семь императивных принципов: (1) законности, справедливости и прозрачности, (2) минимизации данных, (3) ограничения хранения, (4) ограничения цели, (5) точности персональных данных, (6) целостности и конфиденциальности, (7) подотчетности. Важной особенностью GDPR является детальное раскрытие содержания принципов в тексте начальных статей, что придает им силу норм прямого действия и делает их самодостаточными для понимания и исполнения всеми участниками общественных отношений по сбору и обработке персональных данных.

Подробное и ясное закрепление принципов в тексте специального закона будет способствовать повышению уровня комплаенса (соблюдения) и правовой осведомленности операторов, контролеров, субъектов персональных данных и государственных органов. Принципы должны быть сформулированы таким образом, чтобы из них эксплицитно следовало, как именно они обеспечивают защиту автономии личности и реализацию права на неприкосновенность частной жизни. В связи с этим рекомендуется изложить статью 5 Закона «О персональных данных» в новой редакции, путем рецепции системы принципов GDPR, как это предложено в Приложении А.

4. Следуя конституционному приоритету прав и свобод человека, с учетом повышенного внимания статьи 21 Конституции РК 2026 года к защите персональных данных, необходимо конкретизировать в специальном законе права физического лица, субъекта персональных данных, и закрепить подробные корреспондирующие обязанности лиц, которые вовлечены в сбор и обработку персональных данных. Действующий Закон «О персональных данных» ограничивается перечислением перечня прав субъекта персональных данных в виде списка, что не обеспечивает их эффективной реализации. В противовес этому, GDPR посвящает каждому праву отдельную статью, раскрывающую его содержание и устанавливающую соответствующие обязанности контролёра и оператора данных.

Важным элементом реформы должно стать закрепление подробных корреспондирующих обязанностей для всех лиц, вовлеченных в процессы сбора и обработки информации. Данные обязанности должны возлагаться на любого участника правоотношений, получающего или использующего персональные данные. В частности, нормативный комплекс должен обязывать участников информационного оборота разъяснять необходимость манипуляций с личной информацией, предупреждать о потенциальных последствиях, а также раскрывать контактные данные лица по защите данных (офицера) и профильного государственного органа для направления обращений и претензий. Напротив, дефицит четко структурированных взаимных обязательств в действующем законодательстве дестимулирует участников рынка, порождает регуляторный произвол лиц, оперирующих массивами информации, и казуирует утечки сведений, существенно ущемляющие конституционные права личности.

Следует отметить, что принятый Цифровой Кодекс РК, имплементируя новые права субъекта данных (право на анонимизацию и право на ограничение обработки персональных данных), не раскрывает содержание новых прав субъекта, механизмы их реализации и не определяет связанные с ними обязанности собственников и операторов баз, что оставляет данные нормы декларативными.

Для обеспечения технологической защиты персональных данных в национальный закон необходимо включить специальные технологические меры защиты и обязанности для собственников и операторов баз персональных данных, которые отвечают международной практике и правилам: *Privacy by Default* («конфиденциальность по умолчанию») и *Privacy by Design* («конфиденциальность по замыслу», спроектированная или встроенная конфиденциальность). Закрепление данных обязанностей обеспечит технологическую защиту персональных данных, встроенную в архитектуру информационных систем, тем самым придав более надежную защиту и упростив соблюдение законодательства.

Комплексное дополнение прав субъектов и детализация обязанностей всех лиц, вовлеченных в сбор и обработку персональных данных, предлагаемые в

Приложении А, позволят минимизировать риски произвола и обеспечить безопасность личности в цифровой среде.

5. Для обеспечения эффективной защиты персональных данных необходимо реформирование уполномоченного органа в области защиты персональных данных, предусматривающее его выделение в самостоятельную структуру и наделение его дополнительными полномочиями. По аналогии со специальным Законом «О персональных данных», уполномоченный орган должен функционировать как специализированный институт с ясно определенной компетенцией. Данный институт должен координировать и проводить «генеральную линию» защиты персональных данных в тесном взаимодействии с иными государственными органами.

В процессе институциональной трансформации особое внимание следует уделить квалификационным критериям государственных служащих уполномоченного органа по защите персональных данных, включая строгие требования к их профессиональной компетенции, опыту и специализированным навыкам в области защиты персональных данных. Существенное значение имеет законодательное закрепление за уполномоченным органом дополнительных функций, в первую очередь – консультативной деятельности и функции по повышению правовой осведомленности среди физических и юридических лиц по вопросам законодательства о защите персональных данных.

Реализация данных функций способствуют соблюдению закона, носят предупредительный характер в отличие от закреплённого в законодательстве неэффективного реактивного и карательного подхода. На основании результатов проведенного исследования сформулированы предложения по дополнению компетенции уполномоченного органа по защите персональных данных в Законе «О персональных данных», представленные в Приложении А.

Выводы диссертационного исследования соответствуют его цели и задачам, направлены на комплексный анализ государственно-правового регулирования защиты персональных данных, на выявление теоретических и практических пробелов, изучение международного опыта и разработку предложений по совершенствованию законодательства Республики Казахстан.

Исследование обосновывает необходимость совершенствования национального законодательства в области защиты персональных данных с учетом международных стандартов и современных вызовов цифровой экономики. Приоритетное внимание уделено вопросам унификации правовой терминологии, уточнению дефиниции «персональные данные» и операций с персональными данными, закреплению специальных принципов и пересмотру компетенции уполномоченного органа по защите персональных данных.

Для повышения эффективности правоприменительной практики предложены меры по устранению регуляторных пробелов, реформированию уполномоченного органа по защите персональных данных и расширению его

компетенций. Имплементация предложенных изменений в законодательство по защите персональных данных позволит существенно укрепить правовые гарантии неприкосновенности частной жизни и защиту персональных данных, обеспечить соблюдение законодательства и эффективную реализацию защиты персональных данных, повысит уровень доверия граждан к деятельности собственников и операторов баз данных.

Таким образом, результаты проведенного исследования представляют собой научно обоснованные и практически значимые рекомендации, ориентированные на качественное развитие системы государственно-правового регулирования защиты персональных данных в Казахстане и ее гармонизацию с признанными международными стандартами.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Конституция Республики Казахстан : принята на респ. референдуме 30 авг. 1995 г. (с изм. и доп. по состоянию на 19.09.2022 г.) // Информационно-правовая система «Әділет» (Офиц. текст).
- 2 Конституция Республики Казахстан : принята на респ. референдуме 15 марта 2026 года // Информационно-правовая система «Әділет» (Офиц. текст).
- 3 Послание Главы государства Касым-Жомарта Токаева народу Казахстана «Справедливый Казахстан: закон и порядок, экономический рост, общественный оптимизм» от 02 сентября 2024 г.
https://adilet.zan.kz/rus/docs/K24002024_1/info 17.10.2025
- 4 Концепция по продвижению в обществе идеологии закона и порядка на 2025 – 2030 годы. Утверждена постановлением Правительства Республики Казахстан от 1 апреля 2025 года № 200 // <https://adilet.zan.kz/rus/docs/P2500000200> 17.10.2025
- 5 Warren S.D, Brandies L.D., The right to privacy // Harv Law Rev, - 1890. – Vol. 4, № 5. -P. 193-220.
- 6 Westin Alan F. Privacy and freedom. - New York: Atheneum, 1967. – 487 p.
- 7 Ego Sarah I. The known citizen: a history of privacy in modern America. - Cambridge, Massachusetts: Harvard University Press, 2018. - 592 p.
- 8 Koops B.J., Newell B. C., Timan T., Škorvánek I., Chokrevski T., Galič M. A typology of privacy. // Univ. Pa. J. Int. Law, 2017. - Vol.38, № 2. - P. 483-575.
- 9 Koops B.J. On legal boundaries, technologies, and collapsing dimensions of privacy // Politica e Societ, 2014. - Vol.3, №2. - P. 247-264.
- 10 Véliz C. Privacy is power: why and how you should take back control of your data. – UK: Penguin Random House, 2021. - 224 p.
- 11 Solove D.J. Conceptualizing privacy. // Cal Law Rev, 2002. - Vol. 90, № 4. - P. 1087-1156.
- 12 Solove D.J. Understanding privacy. - Cambridge: Harvard University Press, 2009. - 265 p.
- 13 Solove D. J. A taxonomy of privacy. // Penn Law Rev, 2006. - Vol. 154, № 3. - P. 477-564.
- 14 Citron D. K., Solove D. J. Privacy harms // BU Law Rev, 2022. - Vol.102, № 3. - P. 793-864.
- 15 Solove D. J. Privacy and power: computer databases and metaphors for information privacy. // Stanford Law Rev, 2001. - Vol. 53, № 6. - P. 1393-1462.
- 16 Solove D. J., Introduction: privacy self-management and the consent dilemma. // Harv L Rev, 2013. - Vol.126, № 7. - P. 1880-1903.

- 17 Solove D. J. Artificial Intelligence and Privacy. // Florida Law Rev, 2025. - Vol.77, № 1. - P. 1-73.
- 18 Borgesius F. Z., Helberger N., Reyna A. The perfect match? A closer look at the relationship between EU Consumer law and Data protection law // Common Mark. Law Rev., 2017. - Vol. 54, № 5. - P. 1427-1465.
- 19 Borgesius F. Z., Poort J. Online price discrimination and EU data privacy law // J Consum Policy, 2017. - Vol.40, № 3 - P.347-366.
- 20 Borgesius F. Z. Singling out people without knowing their names: Behavioural targeting, pseudonymous data, and the new data protection regulation // Comp. Law Sec. Rev., 2016. - Vol. 32, № 2 - P. 256-271.
- 21 Borgesius F. Z. Personal data processing for behavioural targeting: which legal basis? // Int. Data Priv. Law, 2015. - Vol. 5, № 3. – P.163-176.
- 22 Purtova N. The law of everything. Broad concept of personal data and future of EU Data protection law // Law, Innovation and Technology, 2018. - Vol.10, № 1. - P. 40-81.
- 23 Purtova N. From knowing by name to targeting: the meaning of identification under the GDPR // Int. Data Priv. Law, 2022. - Vol.12, № 3. - P. 163–183.
- 24 Mantelero A. AI and big data: A blueprint for a human rights, social and ethical impact assessment // Comp. Law Sec. Rev., 2018. - Vol.34, № 4 - P.754–772.
- 25 Mantelero A., Esposito M. An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems //Comp. Law Sec. Rev., 2021. – Vol. 41 – P.1-35.
- 26 Mantelero, A. The future of data protection: gold standard vs. global standard // Comp. Law Sec. Rev., (2021). – Vol. 40. – P.1-5.
- 27 Greenleaf G. Renewing convention 108: the CoE's 'GDPR Lite' initiatives // UNSW Law Research, 2017. -Vol.3. – P. 1-8.
- 28 Greenleaf G. Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. // UNSW Law Research, 2017. – Vol. 45. – P.1-9.
- 29 Greenleaf G. The Brussels effect // <https://ssrn.com/abstract=5125412> 23.01.2025
- 30 Закон РК от 21 мая 2013 г. № 94-V «О персональных данных и их защите» (с изм. и доп. по состоянию на 02.03.2026 г.) // Информационно-правовая система «Әділет» (Офиц. текст).
- 31 Омурчиева Э.М., Саудабаева Д.Е. Проблемы применения законодательства Республики Казахстан о персональных данных: риски для работодателя //Вест. Инст. зак. и прав. инф. РК. – 2024. – Т. 77, № 2. – С. 111-121.
- 32 Сырлыбаева Ф. М. Некоторые вопросы защиты информационных прав работника // Вест. ЕНУ. Сер. Право., 2022. – Т. 140, № 3. - С.72-80.
- 33 Гельманова З.С., Саульский Ю.Н., Иванова А.В., Петровская А.С. Цифровая эпоха и управление персоналом: этика и конфиденциальность как

стратегический приоритет // In The World Of Science and Education, - 2025. - Экономические Науки, №15 – С. 38-42.

34 Амиров А.М. О некоторых подходах зарубежных государств к вопросу защиты персональных данных // Вест. Акад. правоохр. органов. - 2024, -Т. 32, № 2.- С. 253-263.

35 Амиров А.М., Шаяхметов Ш.Ш. Проблемы и перспективы правового регулирования обработки биометрических данных // Вест. Акад. правоохр. органов. - 2024. - Т. 34, №4. - С. 8-17.

36 Мухамеджанова, Д. У. Биометрическая аутентификация в Казахстане и риски, связанные с практикой ее применения // Цифровые технологии и право: Сборник научных трудов I Междун. научно-практич. конф. - Казань, 2022.- Том 1. - 560 с.– С. 298-303.

37 Утеген Д., Рахметов Б. Ж. Технология распознавания лиц и обеспечение безопасности биометрических данных: компаративный анализ моделей правового регулирования // Journal of Digital Technologies and Law, - 2023. - Vol.1, № 3. – P.825-844.

38 Toqmati M., Zakharchenko N. I agree to terms and conditions: Negotiating privacy online in Central Asia // JeDEM-EJournal of EDemocracy and Open Government, - 2021. - Vol. 13, № 1. - P.71-100.

39 Iskakova Zh. T., Kadyrzhanova T.S. Analysis of problems and challenges in the legislation of the Republic of Kazakhstan on personal data protection and international legal regulation // Bulletin of L.N Gumilyov Eurasian National University, Law Series, - 2022. - Vol.141, № 4. - P. 48-60.

40 Лозовая О. В. Законодательство Республики Казахстан в сфере защиты персональных данных: сравнительный анализ с правом Европейского Союза // Вест. Инст. законодат. и прав. инф. РК. - 2015. – Т. 37, № 1. - С. 128-133.

41 Максutow Б. М. Правовой механизм защиты персональных данных в Казахстане на основе Общего Регламента по защите персональных данных (GDPR) // Тезисы докл. XI International Correspondence Scientific specialized conference. - Boston, 2019. - года / Editor: Emma Morgan. – Boston: Problems of Science, 2019.-105 с.

42 Аубакирова И.У., Тoleубек А.А. О защите персональных данных в Европейском Союзе и Казахстане в сравнительной перспективе // Вест. Инст. законод. и прав. инф. РК. - 2025. - Т.80, № 1. - С.174-185

43 Закон Республики Казахстан от 17 ноября 2025 года № 230-VIII «Об искусственном интеллекте» // Информационно-правовая система «Әділет» (Офиц. текст)

44 Цифровой кодекс Республики Казахстан: Кодекс РК от 9 января 2026 года № 255-VIII // Информационно-правовая система «Әділет» (Офиц. текст).

45 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of

personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] (OJ) L 119/1, 4.5.2016.

46 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37)

47 В КазНУ прошли академические слушания по проекту закона «Об искусственном интеллекте». <https://farabi.university/news/98191?lang=ru> 19.10.2025

48 Gavison R. Privacy and the limits of law // Yale Law Journal, - 1980. - Vol. 89, № 3. - P. 421-471.

49 Nissenbaum H. Privacy in context. – Stanford: Stanford University Press, 2009. – 304 p.

50 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), (OJ) L 277/1, 27.10.2022.

51 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), (OJ) L 2024/1689, 12.7.2024

52 Закон Республики Казахстан от 10 июля 2023 года № 18-VIII «Об онлайн-платформах и онлайн-рекламе» (с изменениями и дополнениями по состоянию на 02.03.2026 г.) // Информационно-правовая система «Әділет» (Офиц. текст).

53 Ерболатов Е.Е., Жетписов С.К. Баланс цифровизации и защиты персональных данных: казахстанский кейс // Вест. Акад. правоохр. Органов. - 2024. - Т. 34, № 4. - С. 26-35.

54 Каирбаева Л.К. Защита персональных данных в международном и европейском праве // Вест. Инст. законод. и прав. инф. РК. - 2020. - Т. 63, № 5. - С. 168-174.

55 Всеобщей декларации прав человека, принятой резолюцией 217 А(III) Генеральной Ассамблеи ООН от 10 декабря 1948 года

56 Закон Республики Казахстан от 28 ноября 2005 года N 91 «О ратификации Международного пакта о гражданских и политических правах» // Информационно-правовая система «Әділет» (Офиц. текст).

57 Regan P.M. Legislating privacy. Technology, social values, and public policy. - Univ of North Carolina Press, 1995. - 310 p.

58 Ибраева А.С. Теория государства и права. Учебное пособие. 2-е изд. - Алматы: Жеті Жарғы, 2006. - 105 с.

59 Толковый словарь Ушакова <https://www.dicsonline.ru/slovary/tolkovyy-slovar-ushakova/l/lichnost> 16.06.2025

- 60 Толковый словарь С.И.Ожегова
<https://www.dicsonline.ru/slovary/slovar-ozhegova/l/lichnost> 16.06.2025
- 61 Экономический словарь
<https://www.dicsonline.ru/slovary/ekonomicheskij/l/lichnost> 16.06.2025
- 62 Энциклопедия Брокгауза и Ефрона
<https://www.dicsonline.ru/slovary/enciklopediya-brokgauza-i-efrona/l/lichnost> 16.06.2025
- 63 Мещеряков Б.Г., Зинченко В.П. Большой психологический словарь. 4-е изд. - Москва, Санкт-Петербург: АСТ; Прайм-Евроник, 2009. — 811 с.
- 64 Социологический словарь,
<https://www.dicsonline.ru/slovary/sociologicheskij-slovar/l/lichnost> 16.06.2025
- 65 Политический словарь См.
<https://www.dicsonline.ru/slovary/politicheskij-slovar/l/lichnost> 16.06.2025
- 66 Аристотель. Сочинения в четырех томах // АН СССР, Институт Философии. - Москва: Мысль, 1983. - Т. 4. - 828 с.
- 67 Costello R. Á. Privacy Law in Ireland. - Dublin: Bloomsbury Professional, 2023. - 438 p.
- 68 Кляшторный С.Г., Султанов Т.И. Казахстан: летопись трех тысячелетий. – Алматы: Рауан, 1992. – 375 с.
- 69 Сарсембаев М.А. Казахское ханство как суверенное государство средневековой эпохи. - Астана: ГУ «Институт законодательства Республики Казахстан», 2015. - 342 с.
- 70 Конституция Германской империи (Веймарская) 11 августа 1919 г.,
https://togudv.ru/ru/faculties_old/full_time/isptic/iogip/study/studentsbooks/histsources2/igpzio64/ 04.06.2025
- 71 Конституция (Основной Закон) СССР, Утверждена Чрезвычайным VIII съездом Советов Союза ССР, 5 декабря 1936 года,
<https://www.hist.msu.ru/ER/Etext/cnst1936.htm> 04.06.2025
- 72 *Verordnung des Reichspräsidenten zum Schutz von Volk und Staat*, Vom 28. Februar 1933, <http://www.documentarchiv.de/ns/rtbrand.html> 04.06.2025
- 73 Европейской конвенции о защите прав человека и основных свобод, совершена 4 ноября 1950г
- 74 Конституция СССР 1977 года
- 75 Смольяков А. А. Формирование и развитие права на неприкосновенность частной жизни в России в период XX века // Закон. Право. Государство. - 2019. - Т.21, № 1(21). - С. 75-84.
- 76 Баранов В.М., Головкин Р.Б. Государственно-правовое воздействие на частную жизнь граждан в современной России: философско-правовой анализ // Философия права. - 2000. - №2. - С. 33-37.
- 77 Конституция Республики Казахстан от 28 января 1993 года

78 Татаринова Л.Ф. Проблемные аспекты осуществления права человека на неприкосновенность частной жизни в РК // Вестник КазНУ. Серия юридическая. - 2009. - Т.51, №3. - С. 64 – 66.

79 Конституционный Совет РК, «Конституция РК. Научно-практический комментарий», 2018, https://online.zakon.kz/Document/?doc_id=38623503&pos=1562;25#pos=1562;25 8.06.2025

80 Гражданский Кодекс Республики Казахстан (Общая часть) от 27 декабря 1994 г. (с изм. и доп. по состоянию на 19.03.2026 г.) // Информационно-правовая система «Әділет» (Офиц. текст).

81 Уголовный кодекс Республики Казахстан : Кодекс РК от 3 июля 2014 г. № 226-V (с изм. и доп. по состоянию на 08.03.2026 г.) // Информационно-правовая система «Әділет» (Офиц. текст).

82 Кодекс Республики Казахстан об административных правонарушениях : Кодекс РК от 5 июля 2014 г. № 235-V (с изм. и доп. по состоянию на 12.03.2026 г.) // Информационно-правовая система «Әділет» (Офиц. текст).

83 Комментарий к Гражданскому кодексу Республики Казахстан (Общая часть) (Ответственные редакторы: Сулейменов М.К., Басин Ю.Г.), https://online.zakon.kz/Document/?doc_id=1019750&pos=1893;-37#pos=1893;-37 8.06.2025

84 Неприкосновенность частной жизни: Сборник материалов круглого стола. / Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан. - Астана, 2018. - 333 с.

85 Борчасвили И.Ш. Комментарий к Уголовному кодексу Республики Казахстан: общая и особенная части. - 2-е изд. - Алматы: Жеті жарғы, 2007. - 989 с.

86 Челмакина М.А. Понятие частной жизни в конституционном праве // Наука. Общество. Государство. - 2021. - Т. 33, № 1(33). – С.139-148.

87 Право на неприкосновенность частной жизни в Республике Казахстан, Сборник материалов экспертной встречи / Центр исследования правовой политики. - Астана, 2009. – 116 с. - <https://lprc.kz/wp-content/uploads/2020/05/Pravona-neprikosnovennost-chastnoj-zhizni-v-Respublike-Kazahstan.pdf> 25.11.2022

88 ECHR Judgement Case of *Lopez Ribalda and others v. Spain* [GC], nos. 1874/13 and 8567/13, 17 October 2019

89 ECHR Judgement Case of *M.L. and W.W. v. Germany*, nos. 60798/10 and 65599/10, 28 June 2018

90 ECHR Judgement Case of *L.B. v. Hungary* [GC], no. 36345/16, 9 March 2023

91 ECHR Judgement Case of *Niemetz v. Germany*, no. 13710/88, 16 December 1992

- 92 ECHR Judgement Case of *Bărbulescu v. Romania* [GC], no. 61496/08, 5 September 2017
- 93 ECHR Judgement Case of *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], no. 931/13, 27 June 2017
- 94 Рассказов Л.П. Теория государства и права: углубленный курс: Учебник. - Москва.: РИОР, ИНФРА-М, 2015. - 559 с.
- 95 Ибраева А.С., Сартаев С.А., Ибраев Н.С., Есетова С.К., Сейфуллина А.Б. Теория государства и права». Учебное пособие. - Алматы: Жеті жарғы, 2017. - 344с.
- 96 Pollicino O., Bassini M., De Gregorio G. Internet Law and Protection of Fundamental Rights. - Milano: Bocconi University Press, 2022. - 351 p.
- 97 Charter of Fundamental Rights of the European Union (OJ) C 303/01, 14.12.2007
- 98 Naef T. Data Protection without Data Protectionism. - Berlin: Springer, 2022. - 431 p.
- 99 Нормативное постановление Конституционного Суда РК от 21 апреля 2023 года № 11 О рассмотрении на соответствие Конституции РК подпункта 3) пункта 1-1 статьи 14 Закона РК от 23 июля 1999 года «О средствах массовой информации» // Информационно-правовая система «Әділет» (Офиц. текст).
- 100 Баймаханова Д.М. Конституционные проблемы развития непосредственной демократии (на материалах Республики Казахстан): Дис. на соиск. учен. степ. канд. юрид. Наук. - Алматы: КазГНУ им. аль-Фараби, 1998. - 186 с.
- 101 Gurtwirth S., De Hert P. Privacy, data protection and law enforcement. Opacity of the individual and transparency of power // RDP, Brasília, - 2021. – Vol. 18, № 100. – P. 500-549.
- 102 Vrabec H. U. Data subject rights under the GDPR. - Oxford University Press, 2021. - 288 p.
- 103 German Constitutional Court Judgment of the First Senate of 15 December 1983
https://bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html доступ 23 апреля 2026г.
- 104 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50
- 105 US Supreme Court Judgement Case of *Katz v. United States*, 389 U.S. 347 (1967)
// [https://supreme.justia.com/cases/federal/us/389/347/#:~:text=United%20States%2C%20389%20U.S.%20347%20\(1967\)&text=It%20is%20unconstitutional%20under%20the,privacy%2C%20unless%20certain%20exceptions%20apply](https://supreme.justia.com/cases/federal/us/389/347/#:~:text=United%20States%2C%20389%20U.S.%20347%20(1967)&text=It%20is%20unconstitutional%20under%20the,privacy%2C%20unless%20certain%20exceptions%20apply) 19.11.2022

- 106 Жижис С.А. К вопросу о доктринальном определении понятия неприкосновенность частной жизни // Вест. Акад. правоохр. орг. - 2019. - Т. 14, №4. - С.10-15.
- 107 Knijnenburg B. P., Page X., Wisniewski P., Lipford H. R., Proferes N., Romano J. Modern socio-technical perspectives on privacy. - Springer, 2022. - 462 p.
- 108 Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера, принятая в Страсбурге 28 января 1981 года (Конвенция 108), <https://rm.coe.int/1680078c46> 19.10.2022
- 109 Akhmetova S. B., Ibrayeva A. S. The European data protection model as a global privacy standard // Farabi Journal of Social Sciences, - 2023. - Vol. 9 № 1. - P. 78-85.
- 110 Opinion 4/2007 on the concept of personal data // https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf 23.10.2023
- 111 CJEU Judgement case of *Breyer* (C-582/14, EU:C:2016:779), 19 October 2016.
- 112 CJEU Judgement (Grand Chamber) case of *Planet49* (C-673/17, EU:C:2019:801), 1 October 2019.
- 113 CJEU Judgement (Grand Chamber) Case of *Digital Rights Ireland and Seitlinger and Others* (Joined Cases C-293/12 and C-594/12, EU:C:2014:238), 8 April 2014.
- 114 CJEU Judgement case of *Nowak* (C-434/16, EU:C:2017:994), 20 December 2017.
- 115 Открытый диалог eGov // <https://dialog.egov.kz/blogs/all-questions/724888> 15.07.2022.
- 116 Открытый диалог eGov // <https://dialog.egov.kz/blogs/all-questions/724882> 15.07.2022.
- 117 Открытый диалог eGov // <https://dialog.egov.kz/blogs/all-questions/691916> 15.07.2022.
- 118 Решение Павлодарского городского суда от 12 апреля 2018г. по делу № 5510-18-00-2/2734
- 119 Решение районного суда № 2 Алмалинского района города Алматы от 14 января 2019 года № 7514-18-00-2/21215
- 120 Ахметова С. Некоторые аспекты законодательства о защите данных // <https://kazlawreview.kz/nekotorye-aspekty-zakonodatelstva-o-zashhite-personalnyh-dannyh/> 19.06.2025.
- 121 Ахметова С. Б., Нусипова Л.Б. Некоторые аспекты законодательства о защите персональных данных: зарубежный и национальный опыт // Междун. Науч.-практич. конф. «Становление правового государства и гражданского общества в новом Казахстане: теория, практика и перспективы развития». - Алматы: Қазақ университеті, 2023. – 494 с.

- 122 Постановление 2 апреля 2019 года Дело № 212 Суд специализированного межрайонного административного суда г.Алматы
- 123 Постановление 26 апреля 2023 года №7199-23-00-3а/ 322, Суд города Астана (апелляционная инстанция)
- 124 Решение Бостандыкский районный суд города Алматы 19 сентября 2025 года дело № 7514-25-00-2/25461
- 125 Akhmetova S., Kassymzhanova A., Ibrayeva A. Modern development of artificial intelligence technologies and problems of legal regulation of profiling and targeted advertising in Kazakhstan // Вестник ЕНУ, - 2025. - Т.1, №150. - С.77–97
- 126 Gellert R. Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies // Int. Data Priv. Law, - 2021. – Vol.11, № 2. – P. 196–208.
- 127 Kuner C. Face-to-data—another developing privacy threat? // Int. Data Priv. Law, - 2013. - Vol. 3, № 1. - P. 1-2.
- 128 Estrada-Jiménez J., Parra-Arnau J., Rodríguez-Hoyos A., Forné J. Online advertising: analysis of privacy threats and protection approaches // Comp. Communications, - 2017. - Vol.100. - P. 32-51.
- 129 Закон Республики Казахстан от 16 ноября 2015 года № 401-V «О доступе к информации» (с изм. и доп. по состоянию на 16.03.2025 г.) // Информационно-правовая система «Әділет» (Офиц. текст).
- 130 Кодекс Республики Казахстан от 29 июня 2020 года № 350-VI «Административный процедурно-процессуальный кодекс Республики Казахстан» (с изм. и доп. по состоянию на 19.03.2026 г.) // Информационно-правовая система «Әділет» (Офиц. текст).
- 131 Закон Республики Казахстан от 9 января 2026 года № 256-VIII «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам цифровизации, транспорта и предпринимательства» // Информационно-правовая система «Әділет» (Офиц. текст).
- 132 Досье на проект Цифрового Кодекса РК (апрель 2024) // https://online.zakon.kz/Document/?doc_id=38933548 17.05.2024.
- 133 Saglam R. B., Nurse J. R.C., Hodges D. Personal information: perceptions, types and evolution // Journal of Inf. Sec. and Applications, - 2022. – Vol. 66. – P.1-31.
- 134 Ахметова С.Б., Ибраева А.С. Государственные услуги на платформах коммерческих банков. Защищены ли персональные данные? // Тезисы докл Респуб. Конф. «Возрождение Казахской государственности: историко-правовой анализ». - Алматы, 2024. – 132с.
- 135 Закон РК от 24 ноября 2015 г. № 418-V «Об информатизации» (с изм. и доп. по состоянию на 18.01.2026 г.) // Информационно-правовая система «Әділет» (Офиц. текст).
- 136 Закон РК от 19 марта 2010 г. № 257-IV «О государственной статистике» (с изм. и доп. по состоянию на 17.07.2024 г.) // Информационно-правовая система «Әділет» (Офиц. текст).

137 Кодекс Республики Казахстан от 29 октября 2015 года № 375-V «Предпринимательский кодекс Республики Казахстан» (с изм. и доп. по состоянию на 19.03.2026 г.) // Информационно-правовая система «Әділет» (Офиц. текст).

138 Письмо Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 20 февраля 2024 года № ЖТ-2023-03079866 // https://prg.kz/document/?doc_id=34497565 27.05.2024

139 Открытый диалог eGov // <https://dialog.egov.kz/blogs/all-questions/758957> 15.07.2022.

140 Открытый диалог eGov // <https://dialog.egov.kz/blogs/all-questions/582584> 15.07.2022

141 Открытый диалог eGov // <https://dialog.egov.kz/blogs/all-questions/702238> 15.07.2022

142 Законом РК от 22 декабря 2003 г. № 510-II «О государственной правовой статистике и специальных учетах» (с изм. и доп. по состоянию на 15.04.2026 г.) // Информационно-правовая система «Әділет» (Офиц. текст).

143 Письмо заместителя Председателя Комитета по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 2 мая 2025 года № ЖТ-2025-01361495 // https://prg.kz/document/?doc_id=33364061 27.06.2025

144 Закон Республики Казахстан от 30 декабря 2016 года № 40-VI «О дактилоскопической и геномной регистрации» (с изм. и доп. по состоянию на 12.07.2025 г.) // Информационно-правовая система «Әділет» (Офиц. текст)

145 Кодекс Республики Казахстан «О здоровье народа и системе здравоохранения» : Кодекс РК от 7 июля 2020 г. № 360-VI (с изм. и доп. по состоянию на 01.02.2026 г.) // Информационно-правовая система «Әділет» (Офиц. текст).

146 Закон Республики Казахстан от 16 января 2026 года № 258-VIII «О банках и банковской деятельности в Республике Казахстан» // Информационно-правовая система «Әділет» (Офиц. текст).

147 Постановление Правления Агентства РК по регулированию и развитию финансового рынка от 3 апреля 2026 года № 54. «Об утверждении Правил проведения биометрической аутентификации банками, организациями, осуществляющими отдельные виды банковских операций, и микрофинансовыми организациями»

148 Письмо Комитета по информационной безопасности МЦРИАП РК от 6 мая 2024 года № ЖТ-2023-03797512 // https://prg.kz/document/?doc_id=34375785 27.05.2024

149 Закон Республики Казахстан от 23 июля 1999 года № 451-I «О средствах массовой информации» (с изм. и доп. по состоянию на 19.06.2024 г.) // Информационно-правовая система «Әділет» (Офиц. текст).

150 ПОСТАНОВЛЕНИЕ 28 октября 2024 года 7528-24-00-3ж/1007
Специализированный межрайонный суд по административным правонарушениям
города Алматы

151 CJEU Judgement Case of *Lindqvist*, (Case C-101/01, ECLI:EU:C:2003:596), 6 November 2003

152 CJEU Judgement (Grand Chamber) Case of *Google Spain* (Case C-131/12, ECLI:EU:C:2014:317), 13 May 2014.

153 Tene O. Privacy: The new generations // Int. Data Priv. Law, - 2011. - Vol. 1, № 1. - P. 15–27

154 Casagran C. B., Vermeulen M. Reflections on the murky legal practices of political micro-targeting from a GDPR perspective // Int. Data Priv. Law, - 2021. – Vol. 11, № 4. – P.348–359

155 Fourberg N., Taş S., Wiewiorra L., Godlovitch I., De Streel A., Jacquemin H., Hill J., Nunu M., Bourguignon C., Jacques F., Ledger M., Lognoul M. Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice. The committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament. - Luxembourg, 2021. – 157p.

156 Skiera B., Miller K., Jin Y., Kraft L., Laub R., Schmitt J. The impact of the General Data Protection Regulation (GDPR) on the online advertising market. – Frankfurt: Bernd Skiera, 2022. - 158 p.

157 Ullah I., Boreli R., Kanhere S.S. Privacy in targeted advertising on mobile devices: a survey // Int. J. Inf. Secur., - 2023. - Vol. 22. - P. 647-678. <https://doi.org/10.1007/s10207-022-00655-x>, accessed 11 September 2023

158 Goldenfein J. Monitoring Laws. Profiling and identity in the World State. - New York: Cambridge University Press, 2019. - 250 p.

159 Tan Zhai Yun The battle between targeted advertising & data privacy // <https://theedgemalaysia.com/article/battle-between-targeted-advertising-data-privacy%C2%A0> 11.09.2023.

160 King N., Jessen P. Profiling the mobile customer – privacy concerns when behavioural advertisers target mobile phones – Part I // Comp. Law & Sec. Rev.,- 2010. - Vol.26, № 5. - P.455-478.

161 Trepte S., Reinecke L. Privacy online: perspectives on privacy and self-disclosure in the social web. - Berlin, Heidelberg: Springer-Verlag, 2011. - 282 p.

162 Shah H. Beneath the Bonnet of Online Privacy // EU Research,- 2023. - Vol. 35. - P. 78-81.

163 Pariser E. The filter bubble. What the Internet is Hiding from You. - New York: Penguin books, 2011. – 304 p.

164 A29WP Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 // https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_en 21.09.2023.

- 165 A29WP Opinion 2/2010 on online behavioural advertising // https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf 21.09.2023.
- 166 European Union Agency for Fundamental Rights // <https://fra.europa.eu/en/themes/unlawful-profiling> 22.09.2023.
- 167 Galanis K., Syed I., Williams K. Privacy versus products in targeted digital advertising // <https://mediaengagement.org/research/privacy-versus-products-in-targeted-digital-advertising/> 11.09.2023.
- 168 Sætra H. S. Generative AI: here to stay, but for good? // Technology in Society,- 2023. - Vol. 75. - P.1-5.
- 169 ECHR Judgement Case of *Basu v Germany* App no 215/19, 18 October 2022.
- 170 ECHR Judgement Case of *Mukhammad v Spain* App no 34085/17, 18 October 2022.
- 171 ECHR Judgement Case of *N.F. and Others v Russia* App nos 3537/15 and 8 others, 12 September 2023.
- 172 ECHR Judgement Case of *I. v Finland* App no 20511/03, 17 July 2008.
- 173 ECHR Judgement Case of *Catt v the United Kingdom* App no 43514/15, 24 January 2019.
- 174 Мамышев Ж. Казахстанцы стали чаще удалять персональные данные из открытого доступа // <https://kz.kursiv.media/2021-10-29/kazakhstancy-stali-chasche-trebovat-udalit-personalnye-dannye-iz-otkrytogo/> 15.07.2022.
- 175 Открытый диалог eGov // <https://dialog.egov.kz/blogs/all-questions/755230> 15.07.2022.
- 176 Открытый диалог eGov // <https://dialog.egov.kz/blogs/all-questions/751245> 15.07.2022.
- 177 Открытый диалог eGov // <https://dialog.egov.kz/blogs/all-questions/750232> 15.07.2022
- 178 Открытый диалог eGov // <https://dialog.egov.kz/blogs/all-questions/750162> 15.07.2022.
- 179 С.Ахметова. Некоторые аспекты законодательства о защите персональных данных // <https://kazlawreview.kz/nekotorye-aspekty-zakonodatelstva-o-zashhite-personalnyh-dannyh/> 23.04.2023.
- 180 Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 21 октября 2020 года №395/НҚ «Об утверждении Правил сбора, обработки персональных данных».
- 181 Приказ Председателя Агентства по стратегическому планированию и реформам Республики Казахстан от 20 июня 2023 года № 3 «Об утверждении Правил и сроков проведения национальных переписей».
- 182 Закон РК от 6 апреля 2016 г. № 480-V «О правовых актах» (с изм. и доп. по состоянию на 01.01.2026 г.) // Информационно-правовая система «Әділет» (Офиц. текст)

- 183 Вопленко Н.Н., Рудковский В.А. Понятие и классификация принципов права // Ленинградский юридич. Жур.,- 2014. – Т. 38, № 4. – С. 35-48.
- 184 Ахметова С.Б., Ибраева А.С., Баймаханова Д.М., Байкенжеев А.С., Турсынкулова Д.А. Принципы защиты персональных данных: сравнительный анализ национального и зарубежного законодательства // Вестник КазНУ. Серия Юридическая. - 2023. – Т. 106, № 2. – С. 33-46.
- 185 Personal Data Protection Act of the Republic of Estonia 2007 // <https://www.riigiteataja.ee/en/eli/523012019001/consolide> 03.04.2023.
- 186 Data Protection Act 2018 // <https://www.legislation.gov.uk/ukpga/2018/12/contents> 03.04.2023.
- 187 Открытый диалог eGov, // <https://dialog.egov.kz/blogs/all-questions/700318> 15.07.2022.
- 188 Постановление Специализированного межрайонного суда по административным правонарушениям города Астана от 19 февраля 2024 года № 3 ж-93/2024.
- 189 Постановление Специализированного межрайонного суда по административным правонарушениям города Астаны от 22 февраля 2023 года 7120-23-00-3/1385
- 190 Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 21 июня 2023 года № 199/НК "Об утверждении Правил определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач".
- 191 Закона Республики Казахстан от 29 января 2013 года № 73-V «О документах, удостоверяющих личность
- 192 Открытый диалог eGov // <https://dialog.egov.kz/blogs/all-questions/727791> 15.07.2022.
- 193 Гусарова А., Джаксылыков С. Защита персональных данных в Казахстане 2.0: цифровой след Covid-19 // https://www.soros.kz/wp-content/uploads/2021/03/Personal-Data_Covid-Implications.pdf 15.07.2022.
- 194 Демичев А. А. Позитивистская классификация принципов современного российского права // Государство и право,- 2014. - № 5. - С. 5-13.
- 195 Романовский Г.Б. Право на неприкосновенность частной жизни. - Москва: МЗ-Пресс, 2001. - 312 с.
- 196 Бергем К. В., Карлсен Г. М., Слюдал Б. Введение в права человека. - Осло: Норвежский Хелтсинский Комитет по правам человека, 2003. – 117 с.
- 197 Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+)
- 198 Капицын В.М. История, теория и защита прав человека. Учебник. - Москва: Московский университет потребительской кооперации, 2003. - 206 с.
- 199 Договора о функционировании Европейского союза (Рим, 25 марта 1957 г., в редакции Лиссабонского договора 2007 г.)

200 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L 119*, 4.5.2016, p. 89–131.

201 Greenleaf G. Independence of data privacy authorities (Part I): International standards // *Comp. Law & Sec. Rev.*, - 2012. - Vol.28, № 1. - P.3-13

202 CJEU Judgement (Grand Chamber) Case of *Maximillian Schrems v Data Protection Commissioner, Digital Rights Ireland Ltd* (Case C-362/14, ECLI:EU:C:2015:650) 6 October 2015.

203 CJEU Judgement (Grand Chamber) Case of *Commission v Germany* (Case C-518/07, ECLI:EU:C:2010:125) 9 March 2010.

204 Vicente D.M., de Vasconcelos Casimiro S. Data protection in the Internet. - Springer, 2020. – 543 p.

205 Bryan C., Farhangi A., Vogl R. Rethinking explainable machines: The GDPR's "Right to Explanation" debate and the rise of algorithmic audits in enterprise // *Berkeley Technology Law Journal*, - 2019. - Vol.34, № 1 - P. 143-188.

206 Puljak L., Mladinić A., Koporc Z. Workload and procedures used by European data protection authorities related to personal data protection: a cross-sectional study // *BMC Research Notes*, - 2023. - Vol.16, №1. - Article 41. - 7p.

207 Neta Y., Agsel A., Melisa M. The urgency of independent supervisory authority towards Indonesia's personal data protection // *Constitutionale*, - 2022. - Vol. 3, № 1. - P. 19-38.

208 Federal Data Protection Act (BDCG) of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 10 of the Act of 23 June 2021 (Federal Law Gazette I, p. 1858; 2022 I p.1045).

209 Уваров В.Н. Правоохранительная функция государства и механизм ее реализации // *Право и государство*, - 2018. – Т.80-81, № 3-4. - С.111-120.

210 Постановление Правительства Республики Казахстан от 9 октября 2025 года № 846 «О мерах по реализации Указа Президента Республики Казахстан от 18 сентября 2025 года № 997 «О мерах по дальнейшему совершенствованию системы государственного управления»».

211 Конституционный закон Республики Казахстан от 5 нояб. 2022 г. № 154-VII «Об Уполномоченном по правам человека в Республике Казахстан» // Информационно-правовая система «Әділет» (Офиц. текст).

212 Конституционный закон Республики Казахстан от 5 нояб. 2022 г. № 155-VII «О прокуратуре» (с изм. от 01.07.2023 г.) // Информационно-правовая система «Әділет» (Офиц. текст).

213 Нормативное постановление Верховного суда Республики Казахстан от 27 ноября 2015 года № 7 "О применении судами законодательства о возмещении морального вреда"

214 Языкова Т. Как усилят защиту персональных данных казахстанцев // https://online.zakon.kz/Document/?doc_id=37190300 10.05.2024.

215 Закон РК от 25 июня 2020 г. № 347-VI «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий» (с изм. от 31.12.2022 г.) // Информационно-правовая система «Әділет» (Офиц. текст).

216 Послание Главы государства Касым-Жомарта Токаева народу Казахстана «Казахстан в эпоху искусственного интеллекта: актуальные задачи и их решения через цифровую трансформацию» от 8 сентября 2025 г. // <https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-kazahstan-v-epohu-iskusstvennogo-intellekta-aktualnye-zadachi-i-ih-resheniya-cherez-cifrovuyu-transformaciyu-885145> 09.10.2025.

217 Указ Президента Республики Казахстан от 18 сентября 2025 года № 997 «О мерах по дальнейшему совершенствованию системы государственного управления».

218 Приказ и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 22 июля 2019 года № 169/НК Об утверждении Положения о республиканском государственном учреждении "Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан".

219 Приказ Заместителя Премьер-Министра - Министра искусственного интеллекта и цифрового развития Республики Казахстан от 21 октября 2025 года № 527/НК «Об утверждении Положения о республиканском государственном учреждении «Комитет по информационной безопасности Министерства искусственного интеллекта и цифрового развития Республики Казахстан».

220 Указ Президента Республики Казахстан от 26 февраля 2021 года № 522 "Об утверждении Концепции развития государственного управления в Республике Казахстан до 2030 года".

221 Открытый диалог eGov // <https://dialog.egov.kz/blogs/all-questions/636689> / 15.07.2022

222 Досье на проект Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам торговой деятельности, развития биржевой торговли и защиты персональных данных» (декабрь 2021 года) // https://prg.kz/lawyer/document/?doc_id=35488373&billingResult=success&sessionId=LvTGU1wXUUVeQF4UVUJYXEJEXIFCFFJAXRJKQIVfXEcDUEIBWEBLEwBUDRFQXIIIVwQNUQ9bQAFBEFcFDVEJRVNDFEcJXlcQFw==&pos=4;154 15.03.2025.

223 Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 12 апреля 2022 года № 118/НК «О

некоторых вопросах консультативного совета по вопросам персональных данных и их защиты».

224 Bezerra Sales Sarlet G., Piñeiro Rodriguez D. Alternatives for an adequate structuring of the national data protection authority (ANPD) in its independent profile: Proposals to overcome the technological challenges in the age of digital governance // *Int. Cybersec. Law Rev.*, - 2023. - Vol.4, №2. - P. 197-211.

225 Тургумбаева Ж. Нариман Мукушев: Halyk GovTech стремится оказывать госуслуги в ноль кликов // https://forbes.kz/economy/finance/nariman_mukushev_halyk_govtech_ctremitsya_okaz_yivat_gosuslugi_v_nol_klikov/ 29.04.2024.

226 Масанов Ю. Казахстанские банки активно внедряют госуслуги и сервисы // <https://kz.kursiv.media/2021-06-18/kazakhstanskije-banki-aktivno-vnedryayut-gosuslugi-i-servisy/> 24.04.2024.

227 Как Govtech помогает гражданам получать услуги за пару минут // <https://bluescreen.kz/kak-govtech-pomoghalet-ghrazhdanam-poluchat-uslughi-za-paru-minut/> /24.04. 2024

228 Reedijk M. Privacy in E-government 2.0. The Case of Utrecht // *Sociology*, - 2017. // <http://hdl.handle.net/2105/41952> 10.05.2024.

229 Закон Республики Казахстан от 15 апреля 2013 года № 88-V «О государственных и социально ответственных услугах» (с изм. и доп. по состоянию на 12.03.2026 г.) // Информационно-правовая система «Әділет» (Офиц. текст).

230 Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 10 апреля 2024 года № 219/НК «Об утверждении Типового партнерского соглашения»

231 Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 9 апреля 2024 года № 214/НК «Об утверждении требований к субъекту предпринимательства для заключения партнерского соглашения»

232 Akhmetova S., Ibrayeva A., Baimakhanova D., Tursynkulova D., Hoffmann T. Legal regulation of profiling and targeted advertising in Kazakhstan through the lens of European experience // *Social and Legal Studios*, - 2025. - Vol. 8, №1. - P. 33-45.

233 Solove D. J. Murky consent: an approach to the fictions of consent in privacy law // *Boston University Law Rev.*, - 2024. - Vol. 104, № 2. – P. 593-639.

234 14-я конференция по защите данных и конфиденциальности // <https://dataprotection-conference.com> 26.03.2025.

235 Raab C. Information privacy, impact assessment, and the place of ethics // *Comp. Law & Sec. Review*, - 2020. - Vol.37. – P. 1-16.

236 Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 "Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности".

237 Досье на проект Закона Республики Казахстан «Об искусственном
интеллекте» (январь 2025 года) //

https://online.zakon.kz/Document/?doc_id=34868071 15.03.2025.

ПРИЛОЖЕНИЕ А

Проект сравнительной таблицы

О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам защиты персональных данных.

№ п/п	Пункт НПА	Действующая редакция	Предлагаемая редакция	Обоснование вносимых изменений
«О персональных данных и их защите» Закон Республики Казахстан от 21 мая 2013 года № 94-V				
1	Статья 1 подпункт 2)	2) персональные данные - данные, в том числе биометрические, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе; Редакция с 11 июля 2026г.:	2) персональные данные - сведения или совокупность сведений, относящихся к определенному или определяемому с их помощью субъекту персональных данных, дополненные одним или несколькими идентификаторами персональных данных, таких как индивидуальный идентификационный номер, данные удостоверяющих личность	С принятием Цифрового Кодекса РК от 9 января 2026г. с 11 июля 2026 года вносятся существенные изменения в Закон РК «О персональных данных и их защите» в определение «персональные данные». Согласно изменениям, «персональные данные» будут включать в себя «сведения или совокупность сведений о субъекте персональных данных, дополненные одним или несколькими идентификаторами персональных данных». Во-первых, в Законе РК «О персональных данных и их защите» необходимо закрепить, что сведения должны относиться к субъекту. Это

		2) персональные данные - сведения или совокупность сведений о субъекте персональных данных, дополненные одним или несколькими идентификаторами персональных данных;	документов, номер абонента оператора связи, адрес электронной почты и иные идентификаторы персональных данных;	положение будет согласовываться с пп.16) ст.1 Закона РК «О персональных данных и их защите» и п.2 ст.37 Цифрового Кодекса РК, в которых под субъектами персональных данных понимаются физические лица, к которым относится соответствующая информация. Во-вторых, необходимо дать понятие «идентификатор персональных данных» или уточнить, какая информация признается идентификатором персональных данных. Цифровой Кодекс РК не содержит понятия «идентификатор» в контексте персональных данных. Однако в п.2 ст. 45 Цифровой Кодекс РК устанавливает, что индивидуальный идентификационный номер (ИИН) является уникальным идентификатором для физических лиц. В то же время Закон «О персональных данных и их защите» также не дает точного определения «идентификатор персональных данных».
2	Статья 1 подпункт 7)	7) обезличивание персональных данных - действия, в результате совершения которых	7) обезличивание (анонимизация) персональных данных - действия, в результате	Привести терминологию в соответствие с положениями Цифрового Кодекса РК от 9 января 2026г.

		определение принадлежности персональных данных субъекту персональных данных невозможно;	совершения которых определение принадлежности персональных данных субъекту персональных данных невозможно;	Статья 41 Цифрового Кодекса РК «Право на удаление, анонимизацию и ограничение обработки персональных данных» дает определение анонимизации персональных данных, которое полностью совпадает с понятием «обезличивание персональных данных». Под анонимизацией персональных данных понимаются действия, в результате совершения которых определение принадлежности персональных данных субъекту персональных данных становится невозможным. Закон РК «О персональных данных и их защите» дает аналогичное содержание понятию «обезличивание».
3	Статья 1 подпункт 12)	12) обработка персональных данных - действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных;	12) обработка персональных данных – любые действия с персональными данными, включая накопление, хранение, изменение, дополнение, использование, распространение, удаление, профайлинг, обезличивание	Операции по обработке персональных данных должны иметь формулировку, близкую к общепринятым международным терминам. Понятие «обработка персональных данных» в Законе РК «О персональных данных и их защите» необходимо расширить, включив любые операции и действия с персональными данными для любых целей, в том числе действия и операции по профилированию

			(анонимизацию), блокирование и уничтожение персональных данных;	(профайлингу). Профайлинг следует установить в Законе РК «О персональных данных и их защите» в качестве вида операции по обработке, поскольку такой метод сбора и обработки персональных данных является особенно интрузивным, вторгающимся в частную жизнь, нарушает автономию личности, лишает контроля за использованием личной информации, чаще всего носит дискриминирующий характер и чреват манипулированием личностью. Гармонизированный с международным законодательством понятийный аппарат об операциях с персональными данными упрощает правоприменение в условиях глобальной цифровой экономики как для национальных компаний, так и зарубежных компаний в сфере информационных технологий. Далее, Закон РК «О персональных данных и их защите» содержит операцию по уничтожению персональных данных - действиям, совершение которых приводит к невозможности восстановить персональные данные. Цифровой Кодекс РК предоставляет новое право
--	--	--	--	--

				субъекту данных - «право на удаление персональных данных», таким образом вводит новый вид операции по обработке «удаление персональных данных» (ст.41, п.4 ст.37). Однако, содержание данного вида обработки персональных данных не раскрывается в Цифровом Кодексе РК и не указано в Законе РК «О персональных данных и их защите».
4	Статья 1 подпункт 9)	9) собственник базы, содержащей персональные данные (далее - собственник) - государственный орган, физическое и (или) юридическое лицо, реализующие в соответствии с законами Республики Казахстан право владения, пользования и распоряжения базой, содержащей персональные данные	9) Контролер - государственный орган, физическое и (или) юридическое лицо, которое самостоятельно или совместно с другими определяет цели и средства сбора и обработки персональных данных; По всему тексту Закона слово «собственник» заменить на «контролер».	В казахстанском законодательстве о персональных данных требуется конкретизировать и заменить понятия «собственник базы персональных данных» и «оператор базы персональных данных», на понятия «контролер» и «обработчик» соответственно, по примеру Европейского Регламента GDPR. При этом, по примеру GDPR, описание указанных понятий должно базироваться не на вещном праве на базу персональных данных, а на конкретных функциях и роли лиц, вовлеченных в процесс сбора и обработки персональных данных, на их обязательствах по отношению к физическому лицу и его персональным данным. Такой подход является более

				прагматичным, поскольку субъективный интерес физического лица, субъекта персональных данных, состоит в сохранности персональных данных и их законном без ущерба использовании, а использование – это совершение конкретных действий с персональными данными, а не осуществление вещного права в отношении базы данных. Операции по обработке персональных данных, субъекты правоотношений, связанных со сбором и обработкой персональных данных, должны иметь ясную и простую формулировку в законе, более близкую к общепринятым международным терминам.
5	Статья 1 подпункт 10)	10) оператор базы, содержащей персональные данные (далее - оператор) - государственный орган, физическое и (или) юридическое лицо, осуществляющие сбор, обработку и защиту персональных данных;	10) обработчик - физическое или юридическое лицо, государственный орган, агентство или иной орган, который обрабатывает персональные данные от имени контролера; По всему тексту Закона слово «оператор»	Операции по обработке персональных данных, субъекты правоотношений, связанных со сбором и обработкой персональных данных, должны иметь ясную и простую формулировку в законе, более близкую к общепринятым международным терминам.

			заменить на «обработчик».	
6	Статья 1 подпункт 14-1)	отсутствует	14-1) профайлинг – форма автоматизированной обработки персональных данных, заключающаяся в использовании персональных данных для оценки определенных личных характеристик физического лица, в частности для анализа или предугадывания поведения физического лица, его экономического или социального положения, здоровья, личных предпочтений, интересов;	Согласно международным нормам, профайлинг представляет собой запрограммированный, сбор, обработку и анализ персональной информации пользователей, их признаков и характеристик, паттернов поведения или причин осуществления какого-то выбора. Анализ пользователя осуществляется с целью определить и предугадать наиболее возможные действия пользователя и его поведение, и создать условия, воздействующие на его поведение и выбор. Тем самым машина (программа) собирает и анализирует личную информацию физического лица, обрабатывает их по заданным алгоритмам, то есть происходит вмешательство в частную жизнь Профайлинг следует установить как вид операции именно в Законе РК «О персональных данных и их защите», поскольку такой метод сбора и обработки персональных данных является особенно интрузивным, вторгающимся в частную жизнь, нарушает автономию личности, лишает

				контроля за использованием личной информации, чаще всего носит дискриминирующий характер и чреват манипулированием личностью. Предлагаемая формулировка близка к международным стандартам.
7	Статья 1 подпункт 14-2)	отсутствует	В статью 1 ввести подпункт 14-2) «удаление персональных данных»	Закон РК «О персональных данных и их защите» содержит операцию «уничтожение персональных данных» - действия, совершение которых приводит к невозможности восстановить персональные данные. Цифровой Кодекс РК предоставляет новое право субъекту данных - «право на удаление персональных данных», таким образом вводит вид операции по обработке «удаление персональных данных» (ст.41, п.4 ст.37). Однако, Цифровой Кодекс РК и Закон «О персональных данных и их защите» не раскрывают и не указывают содержание данного вида обработки персональных данных, его отличие от уничтожения персональных данных.
8	Статья 5	Статья 5. Принципы сбора, обработки и защиты персональных данных	Статья 5. Принципы сбора, обработки и защиты персональных данных	Согласно Закону РК от 6 апреля 2016г. «О правовых актах» закон должен содержать принципы правового регулирования с раскрытием содержания и механизмов реализации.

		Сбор, обработка и защита персональных данных осуществляются в соответствии с принципами: 1) соблюдения конституционных прав и свобод человека и гражданина; 2) законности; 3) конфиденциальности персональных данных ограниченного доступа; 4) равенства прав субъектов, собственников и операторов; 5) обеспечения безопасности личности, общества и государства.	В целях соблюдения конституционных прав и свобод отдельных лиц и граждан, а также обеспечения безопасности личности, общества и государства, сбор, обработка и защита персональных данных должны осуществляться в соответствии со следующими принципами: 1) «законность, справедливость и прозрачность», означающие, что персональные данные должны обрабатываться законным, справедливым и прозрачным образом по отношению к субъекту данных; 2) «ограничение цели», означающие, что персональные данные должны собираться для определенных, явных и законных целей и не	Принципы необходимы для применения аналогии закона, разъяснения смысла правовых норм и устранения противоречия между правовыми нормами (статьи 14-3 и ст.59). Закрепленные действующим Законом РК «О персональных данных и их защите» принципы сбора, обработки и защиты персональных данных: 1) не отвечают свойствам права на уважение частной жизни 2) не раскрывают содержание и механизмы реализации закона и права на уважение частной жизни 3) не работают на практике и не могут служить для определения смысла правовых норм и устранения противоречий. Защита персональных данных охватывается конституционным правом на уважение частной жизни (Статья 18 Конституции РК 1995г. и ст.21 Конституции РК 2026г.). Данное основное право человека имеет свойства (функции) автономии, самоопределения, установления границ (социальных, физических, информационных и др.), контроля за
--	--	---	---	---

			должны далее обрабатываться способом, несовместимым с этими целями; за исключением дальнейшей обработки для статистических целей или в целях научных или исторических исследований; 3) «минимизация данных», означающие, что персональные данные должны быть адекватными, релевантными и ограниченными тем, что необходимо в отношении целей, для которых они обрабатываются; 4) «точность» означает, что персональные данные должны быть точными и, при необходимости, обновляться; должны быть предприняты все разумные шаги для обеспечения того, чтобы неточные персональные данные, с учетом целей их	доступом к данным границам, ограничению вторжения. Действующие принципы закона не отвечают указанным свойствам конституционного права. Принцип конфиденциальности персональных данных ограниченного доступа имеет узкое применение только к конкретному виду персональных данных. Узкий характер данного принципа не согласуется с целями защиты персональных данных, закрепленных статьей 21 Закона РК «О персональных данных и их защите». В частности, одной из целей защиты персональных данных является соблюдение конфиденциальности любых персональных данных. Принцип равенства субъектов, собственников и операторов не обеспечивает адекватной защиты конституционного права на неприкосновенность частной жизни и защиту персональных данных, не отражает объективную реальность. В реальном мире технологическое, цифровое и экономическое равенство значительно различается между
--	--	--	---	---

			обработки, были незамедлительно удалены или исправлены; 5) «ограничение срока хранения» означает, что персональные данные должны храниться в форме, позволяющей идентифицировать субъектов данных, не дольше, чем это необходимо для целей, для которых обрабатываются персональные данные; персональные данные могут храниться в течение более длительных периодов, если они будут обрабатываться исключительно в целях научных или исторических исследований или статистических целей при условии внедрения необходимых мер по защите персональных данных в соответствии с законодательством	физическим лицом-субъектом и собственником (контролером) и (или) оператором базы данных (обработчиком), как и уровень цифровой грамотности. Это неравенство оказывает заметное влияние на юридическое равенство, поскольку владельцы и операторы, контролирующие технологии и обладающие большими ресурсами, могут влиять на то, как люди реализуют свои права. Следовательно, баланс юридического равенства искажен в пользу этих собственников и операторов. Приоритет конституционных прав и свобод человека не предполагает равенства прав человека и интересов коммерческих организаций. Кроме того, целью регулирования Закона о ПД являются право на неприкосновенность частной жизни и интересы личности, а не права и интересы других лиц или организаций. Специальные принципы защиты персональных данных следует ясно и подробно сформулировать и закрепить на уровне законодательства, в специальном законе и определить их
--	--	--	--	--

			Республики Казахстан; 6) «целостность и конфиденциальность» означает, что персональные данные должны обрабатываться таким образом, чтобы обеспечить надлежащую безопасность персональных данных, включая защиту от несанкционированных или незаконных доступа, сбора, обработки и от случайной потери, уничтожения или повреждения, с использованием соответствующих технических или организационных мер; 7) «подотчетность» означает, что собственник, оператор, третье лицо несут ответственность за соблюдение принципов сбора, обработки и защиты персональных данных и должны быть в	как руководящие для любой отрасли правового регулирования и применения иного специального законодательства. В условиях повсеместной цифровизации и имеющихся угроз и рисков ущерба необходимо максимально детально урегулировать сбор, обработку, хранение и распространение личной информации основными руководящими положениями закона - принципами. С учетом продолжающегося развития информационных технологий, законодательно закрепленные принципы сбора и обработки персональных данных способствуют урегулированию возможных будущих общественных отношений, недостатков, конфликтов или пробелов в законодательстве, единообразному пониманию, согласованной и эффективной реализации Закона РК «О персональных данных и их защите». Рекомендуются заимствовать специальные принципы европейского GDPR: (1) законности, справедливости и прозрачности, (2) минимизации данных, (3) ограничения хранения, (4)
--	--	--	--	--

			состоянии продемонстрировать это соблюдение.	ограничения цели, (5) точности персональных данных, (6) целостности и конфиденциальности, (7) подотчетности. Также рекомендуется раскрыть их содержание в тексте начальных статей Закона, чтобы принципы имели прямое действие, были самодостаточными для понимания и применения в том числе вне цифровой среды.
9	Статья 24 Пункт 1 Подпункт 7-1)	1) знать о наличии у собственника и (или) оператора, а также третьего лица своих персональных данных, а также получать информацию, содержащую: • подтверждение факта, цели, источников, способов сбора и обработки персональных данных; • перечень персональных данных; • сроки обработки персональных данных, в том числе сроки их хранения;	1) знать о наличии у собственника и (или) оператора, а также третьего лица своих персональных данных, а также получать информацию, содержащую: • подтверждение факта, цели, источников, способов сбора и обработки персональных данных; • перечень персональных данных; • сроки обработки персональных данных, в том числе сроки их хранения или критерии,	Пункт 2 статьи 25 Закона «О персональных данных и их защите» перечисляет обязанности собственника и (или) оператора, лица, ответственного за организацию обработки персональных данных. К таким обязанностям в том числе относится требование по обращению субъекта сообщать информацию, относящуюся к нему, в сроки, предусмотренные законодательством Республики Казахстан (подпункт 6 пункта 2 статьи 25). Подпункт 1) пункта 1 статьи 24 Закона РК «О персональных данных и их защите» устанавливает право субъекта получать информацию, содержащую: • подтверждение факта, цели, источников, способов сбора и

			определяющие срок хранения; • лица или их категории, которым персональные данные были или будут раскрыты; • наличие права требовать исправления или удаления персональных данных или ограничения обработки персональных данных или возражать против такой обработки; • право обратиться за защитой своих прав и интересов, связанных с защитой персональных данных, в уполномоченный орган по защите персональных данных; • наличие автоматизированной обработки персональных данных, включая разъяснение о порядке	обработки персональных данных; • перечень персональных данных; • сроки обработки персональных данных, в том числе сроки их хранения. В то же время подпункт 6) пункта 2 статьи 25 Закона РК «О персональных данных и их защите» ограничивает корреспондирующую обязанность собственников (контролеров) и операторов баз персональных данных (обработчиков) в отношении физических лиц исключительно перечнем информации, указанным в подпункте 1) пункте 1 статьи 24 Закона. Таким образом, Закон устанавливает ограниченный перечень информации, которую вправе получить физическое лицо о своих персональных данных и действиях с ними. Тем самым ограничиваются права субъекта персональных данных. Более того, Цифровой Кодекс РК закрепляет условия прозрачности использования цифровых технологий (статьи 9, 13). С целью обеспечить эффективную реализацию конституционного права на защиту персональных данных
--	--	--	---	--

			автоматизированной обработки, возможных последствий и праве заявить возражение против автоматизированной обработки его персональных данных.	рекомендуется расширить права физического лица и закрепить обязанности контролеров и обработчиков обеспечить реализацию права субъекта получать информацию о действиях, совершаемых с персональными данными, наличие и реализации иных прав физического лица-субъекта персональных данных. Предлагаемое изменение согласовывается со статьей 21 Конституции РК 2026г., в которой защита персональных данных указана как элемент неприкосновенности частной жизни, а также с положениями Цифрового Кодекса РК о прозрачности применения цифровых технологий. Кроме того, предлагаемые изменения позволят гармонизировать национальное законодательство с зарубежным регулированием и практикой.
10	Статья 24 Пункт 1 Подпункт 7-1)	Отсутствует	7-1) требовать от контролера и (или) обработчика удаления персональных данных в случаях, установленных законодательством Республики Казахстан.	Статья 24 Закона РК «О персональных данных и их защите» устанавливает права субъекта персональных данных, в том числе требовать уничтожения своих персональных данных, сбор и обработка которых произведены с нарушением законодательства

			Если контролер и (или) обработчик сделал персональные данные общедоступными и обязан в соответствии с частью 1 настоящего подпункта удалить персональные данные, контролер и (или) обработчик, принимая во внимание доступные технологии и стоимость внедрения, должен предпринять разумные шаги, включая технические меры, чтобы уведомить контролеров и обработчиков, о том, что субъект данных запросил удаление любых ссылок на эти персональные данные, их копий или репликаций.	Республики Казахстан и в иных случаях, установленных нормативными правовыми актами Республики Казахстан (подпункт 4) п.1 ст.24). Цифровым Кодексом РК от 9 января 2026г. субъекту персональных данных предоставлено новое право на удаление персональных данных (ст.41, п.4 ст.37). Необходимо раскрыть право на удаление персональных данных с тем, чтобы из закона следовало его содержание и отличие от права на уничтожение персональных данных. Кроме того, предложение включает «право на забвение», которое заключается в удалении персональных данных, ставших общедоступными, как самим контролером или обработчиком, так и в последующих цепочках распространения таких персональных данных по обращению субъекта персональных данных с учетом доступных технологий. Содержание прав субъекта персональных данных необходимо раскрыть в законе, а не в подзаконном правовом акте, поскольку законы принимаются законодательным органом, который в то же время
--	--	--	--	--

				является представительным органом, избранным народом. Подзаконный акт принимается органом исполнительной власти, который обладает возможностью собственного усмотрения при принятии правовых актов. Раскрытие содержания прав субъектов в законе исключает произвол власти.
11	Статья 24 Пункт 1 Подпункт 7-2)	Отсутствует	7-2) требовать от контролера и (или) обработчика ограничения обработки персональных данных в случаях: • оспаривания точности персональных данных на период, позволяющий контролеру проверить точность персональных данных; • незаконной обработки, если субъект данных вместо удаления персональных данных запрашивает ограничение их использования; • достижения	Статья 24 Закона РК «О персональных данных и их защите» устанавливает права субъекта персональных данных. В данной статье отсутствует новое право субъекта персональных данных на ограничение обработки персональных данных, которое предоставлено Цифровым Кодексом РК от 9 января 2026г. (ст.41, п.4 ст.37). Необходимо раскрыть данное право субъекта персональных данных с тем, чтобы из закона следовало его содержание, что способствует правовой грамотности и обеспечивает реализацию конституционного права. Предлагаемое изменение согласуется с положениями и ограничениями статьи 41 Цифрового Кодекса РК, однако, Цифровой Кодекс РК ограничен областью применения – цифровой

			контролером целей обработки персональных данных, если субъект данных вместо уничтожения персональных данных запрашивает ограничение их обработки в связи с необходимостью защиты субъектом данных своих прав и интересов в будущем; • субъект оспаривает законность сбора и обработки персональных данных контролером и требует ограничить обработку до разрешения такого спора; • если законодательством Республики Казахстан установлены обязательные сроки хранения цифровых данных, контролер и (или) обработчик,	средой, в то время как Закон «О персональных данных и их защите» применяется и вне ее. Содержание права субъекта персональных данных необходимо раскрыть в законе, а не в подзаконном правовом акте, поскольку законы принимаются законодательным органом, который в то же время является представительным органом, избранным народом. Подзаконный акт принимается органом исполнительной власти, который обладает возможностью собственного усмотрения при принятии правовых актов. Раскрытие содержания прав субъектов в законе исключает произвол власти.
--	--	--	---	--

			обязаны ограничить доступ к таким данным и приостановить их обработку по требованию субъекта персональных данных с учетом иных требований законодательства Республики Казахстан. Контролер и (или) обработчик обязаны проинформировать субъекта данных об ограничении обработки и о снятии ограничения обработки в письменной форме или электронным способом.	
12	Статья 25 Пункт 2 подпункт 6)	6) по обращению субъекта сообщать информацию, относящуюся к нему, в сроки, предусмотренные законодательством Республики Казахстан;	6) по обращению субъекта обязаны принять надлежащие меры для предоставления субъекту данных любой информации, относящейся к нему, а также касающихся обработки персональных данных, в краткой, прозрачной,	Пункт 2 статьи 25 Закон РК «О персональных данных и их защите» перечисляет обязанности собственника и (или) оператора, лица, ответственного за организацию обработки персональных данных. Подпункт 1) пункта 1 статьи 24 Закона устанавливает право субъекта получать информацию, содержащую: • подтверждение факта, цели,

			понятной и легкодоступной форме. Информация должна предоставляться в письменной форме или иными способами, включая, при необходимости, электронные средства.	источников, способов сбора и обработки персональных данных; • перечень персональных данных; • сроки обработки персональных данных, в том числе сроки их хранения. Таким образом, закон устанавливает ограниченный перечень информации, которую может получить физическое лицо, тем самым ограничивая его права. В то же время подпункт 6) пункта 2 статьи 25 Закона ограничивает корреспондирующую обязанность собственников (контролеров) и операторов баз персональных данных (обработчиков). С целью обеспечить эффективную реализацию конституционного права на защиту персональных данных и гармонизировать национальное законодательство с зарубежным регулированием и практикой рекомендуется расширить права физического лица и закрепить обязанности контролеров и обработчиков обеспечить реализацию права субъекта получать информацию о действиях, совершаемых с
--	--	--	---	---

				персональными данными, наличие и реализации иных прав физического лица-субъекта персональных данных.
13	Статья 25 пункт 2 подпункт 11)	Отсутствует	11) внедрять технические и организационные меры на этапе проектирования и в течение всего жизненного цикла цифрового объекта и цикла обработки персональных данных (встраиваемая защита), обеспечивая эффективное применение и соблюдение принципов законности, минимизации данных, ограничения цели, ограничения хранения, целостности и конфиденциальности. Внедряемые меры должны обеспечивать, что по умолчанию обрабатываются только персональные данные, необходимые для достижения каждой конкретной цели обработки, а также, что	Подпункт 2) пункта 2 статьи 25 Закона РК «О персональных данных и их защите» содержит обязанность собственника и оператора принимать и соблюдать необходимые меры, в том числе правовые, организационные и технические, для защиты персональных данных в соответствии с законодательством Республики Казахстан. Указанная обязанность принимать организационные и технические меры является неопределенной и расплывчатой, отсылающей к другим правовым актам. Основными правовыми актами являются законодательство об информатизации и специальный Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 12 июня 2023 года № 179/НК «Об утверждении Правил осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных». Указанный Приказ № 179/НК дает

			персональные данные не будут доступны без вмешательства субъекта персональных данных неопределенному числу лиц (защита по умолчанию);	исчерпывающий перечень обязательных технических мер защиты персональных данных: • обеспечивать установку средств защиты информации, обновлений программного обеспечения на технических средствах, осуществляющих обработку персональных данных ограниченного доступа; • применять средства контроля целостности персональных данных ограниченного доступа; • обеспечивать передачу персональных данных ограниченного доступа иным лицам по защищенным каналам связи и (или) с применением шифрования и при наличии согласия субъекта персональных данных, если иное не предусмотрено законодательством Республики Казахстан; • обеспечивать применение средств криптографической защиты информации для надежного хранения персональных данных ограниченного доступа. Законодательство об информатизации регулирует главным образом
--	--	--	--	---

				техническую защиту от нарушения безопасности. Однако техническая защита должна касаться также и защиты от излишнего сбора, чрезмерной обработки, в том числе в коммерческом секторе. Неконтролируемый и нерегулируемый сбор, доступ и передача неопределенного спектра персональных данных между различными коммерческими организациями создают риски нарушения права на защиту персональных данных. Таким образом, действующее законодательство Казахстана возлагает ограниченные обязательства по применению технических мер защиты персональных данных, направленных главным образом на защиту от утечки, нарушения целостности и уничтожения персональных данных. В европейском регулировании и практике контролеры и обработчики обязаны применять технические меры защиты персональных данных <i>Privacy by design</i> (встроенная конфиденциальность) и <i>Privacy by default</i> (конфиденциальность по
--	--	--	--	--

				умолчанию). Встроенная конфиденциальность и конфиденциальность по умолчанию требуется, начиная с этапа проектирования программ, приложений и других цифровых объектов и в течение всего периода их использования, сбора и обработки персональных данных. Данные технические меры способствуют защите персональных данных и эффективному соблюдению прав и обязанностей всех лиц, задействованных в процессе сбора и обработки персональных данных. Более того, конфиденциальность по замыслу и по умолчанию благоприятствуют соблюдению права на защиту персональных данных даже несмотря на значительный разрыв между как минимум тремя показателями - темпом развития информационных технологий, нормативного регулирования и цифровой грамотности населения и общества в целом.
14			Реорганизация Министерства искусственного	Европейские уполномоченные органы являются отдельными государственными органами, не

			интеллекта и цифрового развития РК, создание отдельного уполномоченного органа по защите персональных данных.	включенными в состав какого-либо министерства или агентства. Государственные служащие в этих органах власти должны обладать необходимой квалификацией и опытом в области защиты персональных данных. Рекомендуется реформировать казахстанский уполномоченный орган в области персональных данных. Выделить его из структуры многоотраслевого Министерства искусственного интеллекта и цифрового развития РК в отдельный независимый орган.
15	Статья 27-1 пункт 1 подпункт 7-5)	отсутствует	7-5) издавать руководства и рекомендации для обеспечения единообразного применения законодательства о защите персональных данных, адаптации правовых норм к новым технологиям и оказания практической помощи контролерам, обработчикам и третьим лицам в соблюдении требований	В целях защиты основных прав и свобод физических лиц Европейские надзорные органы по защите данных осуществляют мониторинг применения законодательства и способствуют последовательному применению законодательства. Для этой цели надзорные органы наделены консультативными функциями, что носит проактивный, предупредительный характер. Напротив, деятельность казахстанского уполномоченного органа в области персональных данных является либо

			законодательства о защите персональных данных;	бездействующей, либо реактивной и карательной. В рамках своей деятельности Европейские надзорные органы издают руководства (guidelines), чтобы обеспечить единообразное применение правил GDPR и помочь контролерам и операторам соблюдать законодательство. Издаваемые руководства служат мостом между сложными формулировками закона и реальными процессами в обществе. В частности, руководства европейских надзорных органов помогают: • Устранить неопределенность в интерпретации абстрактных терминов или положений (например, «персональные данные», «разумные меры», «высокий риск») и применении законодательства. Руководства расшифровывают, что именно регулятор ожидает увидеть на практике. • Адаптироваться к технологиям, минимизируя регуляторный разрыв. Законы меняются медленно, а технологии (ИИ, биометрия, облачные вычисления) — быстро. Руководства позволяют оперативно
--	--	--	---	---

				разъяснить, как применять основные положения и действующие нормы к новым цифровым угрозам. • Снизить регуляторный риск. Для бизнеса это руководство к правоприменению, «дорожная карта», где регулятор поясняет, как следовать законодательству, чтобы минимизировать риски нарушения и ответственности. • Защитить права субъектов персональных данных. Руководства разъясняют как должны осуществляться обязанности контролеров и обработчиков, как именно должны реализовываться права пользователей. Рекомендуется заимствовать европейский опыт по изданию руководств надзорным органом по защите персональных данных в казахстанское регулирование и практику правоприменения.
16	Статья 27-1 пункт 1 подпункт 7-6)	отсутствует	7-6) осуществлять консультативную поддержку о применении законодательства о защите персональных данных, осуществлять	В целях защиты основных прав и свобод физических лиц Европейские надзорные органы по защите данных осуществляют мониторинг применения законодательства и способствуют последовательному применению

			предварительную оценку рисков, этических кодексов поведения, внедрять рекомендации унифицированных стандартов для договорных обязательств и корпоративных правил.	законодательства. Для этой цели надзорные органы наделены консультативными функциями, что носит проактивный, предупредительный характер. Напротив, деятельность казахстанского уполномоченного органа в области персональных данных является либо бездействующей, либо реактивной и карательной. Консультативные полномочия европейского надзорного органа включают: • Предоставление предварительных консультаций по оценке воздействия на защиту данных. • Вынесение заключений и утверждение кодексов поведения для обеспечения надлежащих гарантий. • Принятие обязательных стандартных договорных положений для обработки данных. • Установление обязательных корпоративных правил для организаций, работающих в разных юрисдикциях. В связи с этим, рекомендуется наделить казахстанский
--	--	--	--	---

				уполномоченный орган в области персональных данных консультативными функциями по опыту Европы.
«Об онлайн-платформах и онлайн-рекламе» Закон Республики Казахстан от 10 июля 2023 года № 18-VIII				
17	Статья 1 п. 15)	15) профайлинг – совокупность алгоритмов, направленных на определение предпочтений и (или) интересов пользователей.	15) профайлинг – любая форма автоматической обработки персональных данных, заключающаяся в использовании персональных данных для оценки определенных личных характеристик физического лица, в частности для анализа или предугадывания поведения физического лица, его экономического или социального положения, здоровья, личных предпочтений, интересов.	В содержащемся в действующем законодательстве понятие не передает суть операции по профайлингу и не отражает международную практику. Профайлинг не является просто совокупностью алгоритмов и автоматической обработкой, как это определено в Законе РК «Об онлайн-платформах и онлайн-рекламе». Такая обработка запрограммирована, осуществляет сбор и анализ персональной информации пользователей, их признаков и характеристик, паттернов поведения или причин осуществления какого-то выбора. Анализ пользователя осуществляется с целью определить и предугадать наиболее возможные действия пользователя и его поведение, и создать условия, воздействующие на его поведение и выбор. Тем самым машина (программа) собирает и

				анализирует личную информацию физического лица, обрабатывает их по заданным алгоритмам, то есть происходит вмешательство в частную жизнь.
«О масс-медиа» Закон Республики Казахстан от 19 июня 2024 года № 93-VIII				
18	Статья 4 пункт 2 подпункт 5)	5) неприкосновенность частной жизни;	5) неприкосновенность частной жизни и персональных данных, чести, достоинства человека и гражданина;	Пункт 2 статьи 4 Закона РК «О масс-медиа» закрепляет основные принципы деятельности масс-медиа, одним из которых является неприкосновенность частной жизни. Неприкосновенность частной жизни взаимосвязана с честью и достоинством человека и гражданина, что следует из статьи 18 Конституции РК 1995г. Практика показывает, что публикации в масс-медиа практически всегда связаны с честью и достоинством, и уважение и соблюдение этих конституционных прав является особенной обязанностью сферы деятельности масс-медиа. Честь и достоинство являются самостоятельными конституционными правами, защищаемыми статьями 17 и 18 Конституции РК 1995г. и статьей 20 Конституции РК 2026г.

				Кроме того, пункт 4 статьи 23 Конституции РК 2026г. закрепляет, что свобода слова и свобода распространения информации не должны посягать на честь и достоинство других лиц.
19	Статья 14 Пункт 5	5. Запрещается распространение в масс-медиа персональных и биометрических данных лица, включая информацию о его родителях и иных законных представителях, иной информации, позволяющей установить личность, о: 1) несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия); 2) несовершеннолетних, подозреваемых и (или) обвиняемых в совершении административных и (или) уголовных	В пункте 5 статьи 14 после слов «признанных судом виновными в совершении тяжких и (или) особо тяжких преступлений» исключить слова «включая информацию об их родителях и иных законных представителях».	Пункт 5 статьи 14 и пункт 5 статьи 67 Закона РК «О масс-медиа» разрешают распространение персональных данных родителей несовершеннолетних, признанных виновными в тяжких и особо тяжких преступлениях. Но Закон РК «О масс-медиа» не учитывает личные <u>права родителей</u> таких несовершеннолетних на неприкосновенность личности, личную и семейную тайну, защиту чести и достоинства. Защита персональных данных охватывается правом на неприкосновенность личности, охраняемым статьей 18 Конституции РК 1995 г. и статьей 21 новой Конституции РК. Более того, статья 21 Конституции РК 2026г. отдельно включает персональные данные в объект охраны. Основные права принадлежат каждому человеку с рождения. Статья 34 Конституции РК

		правонарушений. Действие подпункта 2) части первой настоящего пункта не распространяется на несовершеннолетних, признанных судом виновными в совершении тяжких и (или) особо тяжких преступлений, <u>включая информацию об их родителях и иных законных представителей.</u> Ограничения, установленные настоящим пунктом, не распространяются на случаи, предусмотренные частью второй пункта 5 статьи 67 настоящего Закона		1995 г. и статья 36 Конституции РК 2026 закрепляют обязанность каждого уважать права, свободы, честь и достоинство других лиц, в том числе родителей несовершеннолетних, признанных виновными в уголовных правонарушениях. Пункт 5 статьи 12 Конституции РК 1995г, а также пункт 5 статьи 15 Конституции РК 2026г. закрепляют, что осуществление прав и свобод человека и гражданина не должно нарушать прав и свобод других лиц. Соответственно, права потерпевших, право на свободу слова и доступ к информации, не должны нарушать прав и свобод родителей и законных представителей несовершеннолетних, признанных виновными в преступлении. Статья 39 действующей Конституции РК 1995г требует, чтобы ограничение прав было адекватным законно обоснованным целям и отвечало требованиям справедливости, пропорциональности и соразмерности. Новая Конституция РК 2026г. в статье 41 устанавливает, что закон может ограничить права и свободы человека в
--	--	--	--	---

				той мере, в какой это необходимо в целях защиты основ конституционного строя, прав и свобод человека и гражданина, обеспечения национальной безопасности, охраны общественного порядка, здоровья граждан и нравственности общества. Разрешение законом распространять персональные данные родителей несовершеннолетних, признанных виновными в тяжких и особо тяжких преступлениях, не является адекватным цели защиты прав потерпевших, общественному интересу, соразмерным или пропорциональным, поскольку вред, причиненный ограничением права на неприкосновенность частной жизни родителей или законных представителей, больше, чем полученное благо. Действующее уголовное и гражданское законодательство предусматривает достаточные меры защиты и восстановления баланса в нарушенных правах путем привлечения к уголовной ответственности конкретного лица, удовлетворения гражданского иска в рамках уголовного судопроизводства.
--	--	--	--	--

				Кроме того, Закон РК «О масс-медиа» позволяет публиковать персональные данные и информацию о признанном виновном несовершеннолетнем без его согласия или согласия его родителей и законных представителей. Таким образом, разрешенное Законом РК «О масс-медиа» вмешательство в частную жизнь самого правонарушителя является адекватным, соразмерным и пропорциональным по отношению к потерпевшим и обществу в целом, достаточным для восстановления баланса нарушенных прав потерпевших и общества. Процесс уголовного судопроизводства с самого начала и до вынесения приговора несовершеннолетнему, в любом случае влекут общественное порицание не только в отношении несовершеннолетнего, но и в отношении его родителей и законных представителей. Вынесенный несовершеннолетнему приговор порождает эмоционально-волевые переживания у его родителей и законных представителей, чувства унижения, подавленности, стыда, отчаяния и могут привести к изоляции
--	--	--	--	---

				их от общества и другим последствиям. Указанные моральные последствия совершенного уголовного деяния сами по себе могут быть достаточными для родителей и законных представителей несовершеннолетнего преступника. Закон РК «О масс-медиа» не учитывает данных последствий для родителей и законных представителей несовершеннолетних преступников. Соответственно, публичное распространение персональных данных родителей и законных представителей несовершеннолетнего преступника без их согласия представляет собой чрезмерное вмешательство общества в частную жизнь указанных родителей и законных представителей, является неадекватным, непропорциональным по отношению к потерпевшим и обществу в целом, смещающим баланс в пользу прав потерпевших и общества.
20	подпункт 5) пункта 4 статьи 26	5) получать согласие от физического и (или) юридического лица либо их представителей на распространение в средстве массовой информации личной,	5) получать согласие от физического и (или) юридического лица либо их представителей на сбор и обработку распространение в средстве массовой	Пункт 4 статьи 26 Закон РК «О масс-медиа» закрепляет обязанности журналиста. Рекомендуемое изменение будет согласовываться со статьей 21 Конституции РК 2026г., которая отдельно включает персональные

		семейной, врачебной, банковской, коммерческой и иных охраняемых законом тайн, за исключением случаев, если сведения указаны в официальных сообщениях и (или) распространены самим физическим и (или) юридическим лицом либо их представителями в источниках, доступ к которым не ограничен;	информации персональных данных, личной, семейной, врачебной, банковской, коммерческой и иных охраняемых законом тайн, за исключением случаев, если сведения указаны в официальных сообщениях и (или) распространены самим физическим и (или) юридическим лицом либо их представителями в источниках, доступ к которым не ограничен. Журналист обязан осуществлять сбор и обработку персональных данных в соответствии с принципами и другими требованиями законодательства РК о персональных данных и их защите;	данные в объект охраны. Несмотря на то, что тайны и информация, указанная в подпункте 5) пункта 4 статьи 26 Закона «О масс-медиа» могут содержать персональные данные согласие не является достаточным механизмом, обеспечивающим право на неприкосновенность личности. Масс-медиа имеют широкую аудиторию и с учетом интернет-технологий предоставляют ей неограниченный доступ и возможность последующего распространения. Законодательство не устанавливает ясно допустимый объем информации и степень его распространения. Закон РК «О масс-медиа» также не конкретизирует, в отношении какого объема и какой информации, журналист получает согласие физического лица. С учетом принятия новой редакции статьи 5 Закона РК «О персональных данных и их защите», законодательство будет ясно требовать согласия на сбор и обработку персональных данных с учетом принципов минимизации, ограничения цели обработки и
--	--	--	---	---

				ограничения хранения. В связи с этим, в Законе РК «О масс-медиа» появится ясность для журналистов не просто о получении согласия, а также о допустимом объеме и степени распространения персональных данных в масс-медиа. Данная поправка не противоречит основным положениями Закона РК «О масс-медиа», ограничениям, предоставленным для реализации свободы слова и доступа к информации.
21	Пункт 5 статьи 67	5. Масс-медиа не вправе разглашать в распространяемых сообщениях и материалах информацию, указанную в пункте 5 статьи 14 настоящего Закона, за исключением случаев, если распространение такой информации осуществляется в целях защиты прав и законных интересов несовершеннолетнего, пострадавшего в результате	В части первой пункта 5 статьи 67 Закона «О масс-медиа» после слов «за исключением несовершеннолетних, признанных судом виновными в совершении тяжких и (или) особо тяжких преступлений» исключить слова «включая информацию об их родителях и иных законных представителях».	Статья 67 устанавливает ответственность за нарушение законодательства Республики Казахстан о масс-медиа. Пункт 5 статьи 14 и пункт 5 статьи 67 Закона РК «О масс-медиа» разрешают распространение персональных данных родителей несовершеннолетних, признанных виновными в тяжких и особо тяжких преступлениях. Но Закон РК «О масс-медиа» не учитывает личные <u>права родителей</u> таких несовершеннолетних на неприкосновенность личности, личную и семейную тайну, защиту чести и достоинства.

		противоправных действий (бездействия), и несовершеннолетних, подозреваемых и (или) обвиняемых в совершении административных и (или) уголовных правонарушений, за исключением несовершеннолетних, признанных судом виновными в совершении тяжких и (или) особо тяжких преступлений, включая информацию об их родителях и иных законных представителях. Информация, указанная в части первой настоящего пункта, может распространяться в масс-медиа с согласия: 1) несовершеннолетнего, достигшего четырнадцатилетнего возраста, пострадавшего в результате		Защита персональных данных охватывается правом на неприкосновенность личности, охраняемым статьей 18 Конституции РК 1995 г. и статьей 21 новой Конституции РК. Более того, статья 21 Конституции РК 2026г. отдельно включает персональные данные в объект охраны. Основные права принадлежат каждому человеку с рождения. Статья 34 Конституции РК 1995 г. и статья 36 Конституции РК 2026 закрепляют обязанность каждого уважать права, свободы, честь и достоинство других лиц, в том числе родителей несовершеннолетних, признанных виновными в уголовных правонарушениях. Пункт 5 статьи 12 Конституции РК 1995г, а также пункт 5 статьи 15 Конституции РК 2026г. закрепляют, что осуществление прав и свобод человека и гражданина не должно нарушать прав и свобод других лиц. Соответственно, права потерпевших, право на свободу слова и доступ к информации, не должны нарушать прав и свобод родителей и законных представителей несовершеннолетних,
--	--	---	--	--

		противоправных действий (бездействия), и его законных представителей; 2) законных представителей несовершеннолетнего, не достигшего четырнадцатилетнего возраста, пострадавшего в результате противоправных действий (бездействия); 3) несовершеннолетнего, достигшего шестнадцатилетнего возраста, совершившего административные и (или) уголовные правонарушения, и его законных представителей. В случае, если одно из лиц, указанных в части второй настоящего пункта, не дает своего согласия на распространение информации в масс-		признанных виновными в преступлении. Статья 39 действующей Конституции РК 1995г требует, чтобы ограничение прав было адекватным законно обоснованным целям и отвечало требованиям справедливости, пропорциональности и соразмерности. Новая Конституция РК 2026г. в статье 41 устанавливает, что закон может ограничить права и свободы человека в той мере, в какой это необходимо в целях защиты основ конституционного строя, прав и свобод человека и гражданина, обеспечения национальной безопасности, охраны общественного порядка, здоровья граждан и нравственности общества. Разрешение законом распространять персональные данные родителей несовершеннолетних, признанных виновными в тяжких и особо тяжких преступлениях, не является адекватным цели защиты прав потерпевших, общественному интересу, соразмерным или пропорциональным, поскольку вред, причиненный ограничением права на неприкосновенность частной жизни
--	--	--	--	--

		медиа, распространение данной информации запрещено, за исключением следующих случаев: 1) без согласия несовершеннолетнего, достигшего четырнадцатилетнего возраста и пострадавшего в результате противоправных действий (бездействия), или его законных представителей, если законный представитель является подозреваемым или обвиняемым в совершении данных противоправных действий (бездействия); 2) с согласия одного законного представителя пострадавшего несовершеннолетнего в случае, если второй законный представитель находится за пределами Республики Казахстан и		родителей или законных представителей, больше, чем полученное благо. Действующее уголовное и гражданское законодательство предусматривает достаточные меры защиты и восстановления баланса в нарушенных правах путем привлечения к уголовной ответственности конкретного лица, удовлетворения гражданского иска в рамках уголовного судопроизводства. Кроме того, закон о масс-медиа позволяет публиковать персональные данные и информацию о признанном виновном несовершеннолетнем без его согласия или согласия его родителей и законных представителей. Таким образом, разрешенное Законом РК «О масс-медиа» вмешательство в частную жизнь самого правонарушителя является адекватным, соразмерным и пропорциональным по отношению к потерпевшим и обществу в целом, достаточным для восстановления баланса нарушенных прав потерпевших и общества. Процесс уголовного судопроизводства с самого начала и до вынесения приговора несовершеннолетнему, в
--	--	---	--	--

	его согласие получить не представляется возможным. 6. Масс-медиа вправе в целях содействия расследованию преступления, установлению лиц, причастных к совершению преступления, розыску пропавших несовершеннолетних в объеме, необходимом для достижения указанных целей, и с соблюдением требований, установленных Уголовно-процессуальным кодексом Республики Казахстан, на основании процессуальных документов, полученных от органов, ведущих уголовный процесс, распространять сведения, относящиеся к несовершеннолетнему,		любом случае влекут общественное порицание не только в отношении несовершеннолетнего, но и в отношении его родителей и законных представителей. Вынесенный несовершеннолетнему приговор порождает эмоционально-волевые переживания у его родителей и законных представителей, чувства унижения, подавленности, стыда, отчаяния и могут привести к изоляции их от общества и другим последствиям. Указанные моральные последствия совершенного уголовного деяния сами по себе могут быть достаточными для родителей и законных представителей несовершеннолетнего преступника. Закон РК «О масс-медиа» не учитывает данных последствий для родителей и законных представителей несовершеннолетних преступников. Соответственно, публичное распространение персональных данных родителей и законных представителей несовершеннолетнего преступника без их согласия представляет собой чрезмерное вмешательство общества в частную жизнь указанных родителей и законных представителей, является
--	--	--	--

		без получения согласия лиц, установленных частью второй пункта 5 настоящей статьи.		неадекватным, непропорциональным по отношению к потерпевшим и обществу в целом, смещающим баланс в пользу прав потерпевших и общества.
--	--	--	--	--