

МРНТИ 10.19.25

<https://doi.org/10.26577/JAPJ.2023.v106.i2.04>

С.Б. Ахметова^{1*}, А.С. Ибраева¹, Д.М. Баймаханова¹,
А.С. Байкенжеев², Д.А. Турсынкулова¹

¹Казахский национальный университет имени аль-Фараби, Казахстан, г. Алматы

²Академия КНБ РК, Казахстан, г. Алматы

*e-mail: akhmetova.saule@gmail.com

ПРИНЦИПЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ НАЦИОНАЛЬНОГО И ЗАРУБЕЖНОГО ЗАКОНОДАТЕЛЬСТВА

Информационно-коммуникационные технологии стали неотъемлемым элементом современной жизни, обеспечивающим доступ к информации, товарам и услугам. Республика Казахстан занимает одно из ведущих мест в мире по внедрению и использованию цифровых технологий в общественной-политической жизни страны. Современные технологии позволяют собирать широкий спектр сведений и информации о человеке, привязывая все его документы и данные к его персональному аккаунту и/или профилю, отслеживать его действия, получать представление о привычках и предпочтениях человека, использовать полученные сведения в различных целях.

В настоящей статье рассмотрены принципы защиты персональных данных. Объектом исследования являются общественные отношения, связанные с неприкосновенностью частной жизни, в частности защиты персональных данных в Республике Казахстан. Предметом исследования являются законодательство о защите персональных данных, а также некоторые вопросы правовой практики.

Цель исследования выявить проблемные аспекты института защиты персональных данных в Республике Казахстан и на этой основе аргументировать предложения и рекомендации для действующего законодательства. При подготовке исследования были использованы общенаучные, общие и частные методы исследования. Проведен сравнительный анализ национального и зарубежного законодательства по защите персональных данных. Сделан вывод о необходимости нормативного закрепления принципов защиты персональных данных в соответствии с международно-признанными стандартами. Выявлены возможные риски использования персональной информации недобросовестными лицами во вред личности, ее интересам и имуществу. Обоснован вывод о законодательном закреплении принципов о защите персональных данных в соответствии с международными стандартами и на уровне нормативных принципов.

Ключевые слова: права и свободы человека, неприкосновенность частной жизни, защита персональных данных, принципы права, конфиденциальность.

S.B. Akhmetova^{1*}, A.S. Ibrayeva¹, D.M. Baimakhanova¹,
A.S. Baikenzheyev², D.A. Tursynkulova¹

¹Al-Farabi Kazakh National University, Kazakhstan, Almaty

²Academy of the National Security Committee of the Republic of Kazakhstan, Kazakhstan, Almaty

*e-mail: akhmetova.saule@gmail.com

Principles of protection of personal data: comparative analysis of national and foreign legislation

Information and communication technologies have become integral to modern life, providing access to information, goods, and services. Modern technologies make it possible to collect a wide range of data and information about a person, linking all his documents and data to his account and profile, tracking his actions, getting an idea of a person's habits and preferences, and using the information received for various purposes. The Republic of Kazakhstan occupies one of the top places in the world in the implementation and use of digital technologies in the public and political life of the country.

This article discusses the principles of personal data protection enshrined in the national law. The object of the study is public relations related to privacy, in particular, the protection of personal data in the Republic of Kazakhstan. The research subject is the legislation on protecting personal data, as well as some issues of law implementation practice.

The purpose of the study is to identify the problematic aspects of the institution of personal data protection in the Republic of Kazakhstan and, on this basis, to argue proposals and recommendations for the current legislation. The authors used general scientific and private research methods to prepare the study. A comparative analysis, mainly external and regulatory comparisons, has been conducted. The authors analyzed legal norms, articles of normative legal acts of some states, and normative definitions of the compared laws to identify differences. Legislative consolidation of provisions like the principles in the Kazakh law was found at the level of obligations of owners and operators of databases rather than at a more significant level of regulatory principles. Possible risks of using personal information by unscrupulous persons to the detriment of a person, his interests and property are identified. The conclusion is made about the need for regulatory consolidation of the principles of personal data protection following internationally recognized standards at a level of normative principles.

Key words: human rights and freedoms, privacy, protection of personal data, principles of law, confidentiality.

С.Б. Ахметова^{1*}, А.С. Ибраева¹, Д.М. Баймаханова¹,
А.С. Байкенжеев², Д.А. Турсынкулова¹

¹Әл-Фараби атындағы ҚазҰУ, Қазақстан, Алматы қ.

²ҚР ҰҚК Академиясы, Қазақстан, Алматы қ.

*e-mail: akhmetova.saule@gmail.com

Жеке деректерді қорғау қағидаттары: ұлттық және шетелдік заңнаманы салыстырмалы талдау

Ақпараттық-коммуникациялық технологиялар ақпаратқа, тауарлар мен қызметтерге қол жеткізуді қамтамасыз ететін қазіргі өмірдің ажырамас бөлігіне айналғаны белгілі. Қазақстан Республикасы елдің қоғамдық-саяси өміріне цифрлық технологияларды енгізу және пайдалану жағынан әлемдегі жетекші орындардың бірінде тұр. Заманауи технологиялар адам туралы көптеген мәлімет пен ақпарат жинауға, сол тұлғаның барлық құжаттары мен деректерін оның жеке шотымен және/немесе дербес аккаунтымен байланыстыруға, оның әрекеттерін қадағалауға, әдеттері мен қызығушылықтарын білуге, алынған мәліметтерді әр түрлі мақсаттарда пайдалануға мүмкіндік береді.

Осы мақалада жеке деректерді қорғау қағидаттары қарастырылған. Зерттеу объектісі: адамның жеке өміріне қол сұқпау, атап айтқанда, Қазақстан Республикасында жеке деректерді қорғау саласындағы қоғамдық қатынастар. Зерттеу мәні жеке деректерді қорғау туралы заңнама, сондай-ақ құқықтық тәжірибенің кейбір мәселелері болып табылады.

Зерттеудің мақсаты: Қазақстан Республикасындағы жеке деректерді қорғау институтының проблемалық аспектілерін анықтау және солардың негізінде қолданыстағы заңнамаға енгізуге ұсыныстар дайындау, оларды дәйектеу. Зерттеуді дайындау кезінде жалпы ғылыми, жалпы және жекелеген зерттеу әдістері қолданылды. Жеке деректерді қорғау жөніндегі ұлттық және шетелдік заңнамаларға салыстырмалы талдау жүргізілді. Халықаралық дәрежеде танылған стандарттарға сәйкес жеке деректерді қорғау қағидаттарын нормативтік түрде бекіту қажеттілігі туралы қорытынды жасалды. Адамдардың жеке басына, меншігіне және мүлкіне зиян келтіруде жеке ақпаратты жөнсіз пайдалану тәуекелдері қандай болатыны анықталды. Жеке деректерді қорғау қағидаттарын халықаралық стандарттарға сәйкес және нормативтік қағидаттар деңгейінде заңнамалық бекіту туралы жасау жөнінде тұжырым негізделді.

Түйін сөздер: адамның құқықтары мен бостандығы, жеке өмірге қол сұқпау, жеке деректерді қорғау, құқық қағидаттары, құпиялылық.

Введение

Стремление Республики Казахстан утвердить себя в качестве правового государства должно быть основано на конституционном регулировании основных прав и свобод человека и гражданина. Основным Законом страны закреплено, что права и свободы человека являются естественными, абсолютными, принадлежат ему от рождения и не могут быть отчуждены. Статья 18 Конституции Республики Казахстан закреп-

ляет неприкосновенность частной жизни, личной и семейной тайны, тайны личных вкладов и сбережений, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. По оценкам экспертов указанная норма Конституции Республики Казахстан полностью соответствует международно-правовым стандартам.

Обратимся к Всеобщей декларации прав и свобод человека и гражданина. В статье 3 закреплено, что каждый человек имеет право на личную неприкосновенность. В статье 12 рас-

крывается понятие личной неприкосновенности и утверждается, что никто не может подвергаться произвольному вмешательству в его личную 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.

Неприкосновенность частной жизни в нашей стране регулируется нормами конституционного, уголовного, административного, гражданского законодательства, а также специальными законодательными актами. Укажем следующие законы: Закон Республики Казахстан от 21 мая 2013 года «О персональных данных и их защите», Закон Республики Казахстан от 24 ноября 2015 года «Об информатизации», Закон Республики Казахстан от 16 ноября 2015 года «О доступе к информации», Закон РК от 30 декабря 2016 года «О дактилоскопической и геномной регистрации», Закон Республики Казахстан от 5 июля 2004 года «О связи», Закон Республики Казахстан от 15 сентября 1994 года «Об оперативно-розыскной деятельности», Закон Республики Казахстан от 31 августа 1995 года «О банках и банковской деятельности в Республике Казахстан» и другие. Необходимость в специальном законодательстве обусловлена появлением новых социально-экономических отношений, новых информационно-коммуникационных технологий, глобализацией, повсеместным внедрением интернета и цифровых инструментов во все сферы жизни общества.

Современную действительность невозможно представить без цифровых и интернет-технологий. Телекоммуникации и сети электронной связи стали неотъемлемым элементом современной жизни, обеспечивающим доступ к информации и услугам, включая Интернет, через который многочисленные поставщики продуктов и услуг предоставляют клиентам и конечным пользователям доступ к товарам, информации или контенту.

Казахстан не может находиться в стороне от процессов глобализации политических, экономических и социальных отношений. Наше государство «шаг за шагом приближается к самым высоким стандартам в области демократизации и прав человека» (Стратегия Казахстан 2050 : раздел I). Следуя мировым тенденциям, государство вносит изменения в национальное законодательство о защите персональных. Так, недавние изменения в Закон РК «О персональных данных и их защите» (далее – Закон) наделили граждан правом на забвение в интернете, право

на отзыв согласия на использование персональных данных. Кроме того, предусмотрены санкции за нарушения законодательства о защите персональных данных (Министерство юстиции РК 2022: 40).

Тем не менее, новые поправки предписывают, как обращаться с персональными данными, какие действия и как необходимо совершать. Хотя последние формулировки закона отвечают общему смыслу и имеют сходство с международными стандартами, они в большей части касаются прав и обязанностей, допустимых действий с персональными данными.

Государство обеспечивает реализацию права на защиту персональных данных через законодательство. А на уровне закона главная роль отводится принципам. Именно принципы определяют, как будут реализовываться права и выполняться обязательства. Принципы имеют первостепенное значение, так как являются исходными началами, выражают основополагающие, «сквозные и генеральные» идеи, в которых выражается общий «дух» и направленность правового регулирования (Вопленко 2013: 5). Они либо выводятся из общего смысла законов, либо прямо сформулированы в законе и призваны регулировать пробелы в правоотношениях. Учитывая темпы технологического развития и цифровизации, нельзя предвидеть, насколько быстро закон будет устаревать, насколько полно и достаточно он будет предусматривать и регулировать новые элементы персональных данных, новые общественные отношения и действия с персональными данными, новые угрозы безопасности персональных данных. В связи с этим, возникает вопрос, сформулированы ли принципы защиты персональных данных в казахстанском законодательстве таким образом, чтобы обеспечить их надлежащую защиту, урегулировать возможные пробелы в правоотношениях по использованию и безопасности персональных данных.

Поскольку принципы того или иного закона определяют имплементацию нормативного акта на практике в данной статье будут изучены принципы защиты персональных данных, закрепленные в Законе Республики Казахстан от 21 мая 2013 года «О персональных данных и их защите». Цель исследования выявить проблемные аспекты нормативного закрепления принципов защиты персональных данных в Республике Казахстан и на этой основе аргументировать предложения и рекомендации для действующего законодательства.

Практическая ценность статьи состоит в уяснении первостепенной роли специальных принципов законодательства, важности законодательного закрепления их содержания, общего характера их соблюдения любым субъектом правоотношения в сфере защиты персональных данных независимо от того, насколько полно и детально закон описывает права и обязанности сторон правоотношения. Научная актуальность заключается в том, что специальные принципы законодательства о защите персональных данных мало изучены в казахстанской юридической науке.

Материалы и методы

При подготовке исследования были использованы общенаучные, общие и частные методы исследования. Проведен сравнительный анализ национального закона о защите персональных данных и европейского законодательства по защите персональных данных. Были изучены, сопоставлены и проанализированы виды и содержание казахстанских и европейских принципов защиты персональных данных, способы их нормативного закрепления, проведен функциональный анализ национального и европейского законодательства. Нормативное сравнение показывает различия в казахстанском и европейском подходе к обозначению и содержанию принципов защиты персональных данных. Обнаруженное отличие национального законодательства усугубляет возможные риски использования персональной информации недобросовестными лицами во вред личности, ее интересам и имуществу.

Результаты и обсуждения

Современные технологии позволяют собирать сведения и информацию о каждом гражданине, привязывая все его документы и данные к его персональному аккаунту и/или профилю, отслеживать его действия, получать представление о привычках и предпочтениях человека, использовать полученные сведения в различных целях. Республика Казахстан занимает одно из ведущих мест в мире по внедрению и использованию цифровых технологий в общественной-политической жизни страны. По уровню электронного участия граждан Казахстан занимает 15-е место в мире, по развитию e-Government – 28-е место (Спутник-Казахстан 2022а). По заявлению Президента К.Токаева, Казахстан входит в трид-

цатку самых оцифрованных государств-членов ООН (Спутник-Казахстан 2022б). В нашу жизнь прочно вошли такие явления как электронное правительство, центры обслуживания населения (ЦОНЫ), электронные услуги в государственном и частном секторе, дистанционная работа, дистанционное обучение, цифровое взаимодействие государства с населением, интернет-магазины и т.д.

Вместе с тем возникает определенный риск того, что персональная информация о человеке может быть использована недобросовестными лицами во вред личности, ее интересам и имуществу.

Интернет и информационно-коммуникационные технологии сделали широкой и многогранной жизнь и взаимодействие с внешним миром каждого отдельно взятого человека. В современных условиях систематизация и классификация персональных данных может иметь несколько вариантов. К примеру, государственные органы собирают и обрабатывают следующую личную информацию: демографическую, личную идентификационную информацию, медицинскую, финансовую, судебные данные и данные правоохранительных органов (Saglam 2022: 8). Если рассмотреть сферу здравоохранения, личная информация может касаться физиологических параметров (рост, вес и тп), режима и типа питания, физических и спортивных нагрузок, сведений о репродуктивном здоровье, медицинских записей, мониторинга сердечбиения, частоты дыхания и прочей информации (Saglam 2022: 10). Что касается финансового сектора, круг собираемой и используемой личной информации помимо личных идентификационных и биометрических 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, экономический статус.

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 (Saglam 2022: 10).

Отношение казахстанцев к конфиденциальности персональных данных противоречиво. Некоторые чрезмерно скрытны и ограниченно предоставляют информацию о себе, не имеют аккаунта в социальных сетях либо не дают свои данные в социальных сетях, отказываются от интернет-подписок, не проводят интернет-платежи, опасаясь утечки данных, особенно банковских сведений. Другие же, напротив, активно ведут онлайн-каналы, ведут персональные страницы в социальных сетях, различные блоги, участвуют в общественных групповых аккаунтах, отслеживают и используют различные промо-акции, охотно размещают свои фото и видео, принимают различные онлайн приглашения от любых лиц и не задумываются о том, кто и как может воспользоваться личными сведениями, об утечке данных или неправомерном использовании.

Если сравнить то, как относятся люди к сохранности и доступу к сведениям о своей частной жизни вне интернета, в оффлайн среде, обнаруживается соблюдение определенных социальных норм. К примеру, считается неэтичным вскрывать конверт и читать чужие письма, войти в дом без приглашения, услышать чей-то разговор, раскрыть чей-то секрет и так далее. Эти правила нежелательного поведения сформировывались в обществе на протяжении многих десятилетий и даже столетий. Поскольку социальная этика в онлайн режиме все еще не сформировалась, необходимо законодательное закрепление соблюдения неприкосновенности частной жизни и правил поведения в интернет-среде, обеспеченных государственным принуждением и санкциями.

В этих условиях необходимы четкое правовое регулирование со стороны государства как основного института защиты прав человека, ясно и точно закрепленные в законодательстве правовые действия, а также необходимы меры ограничения для государства и государственных служащих, для организаций всех форм собственности, субъектов предпринимательства и частных лиц, чтобы персональные данные не стали объектом правонарушений.

Право на неприкосновенность частной жизни охраняется Конституцией Казахстана наравне с другими фундаментальными правами и свободами человека. Реализация конституционного права на неприкосновенность частной жизни включает защиту персональных данных и обеспечивается специальным законом. С принятием Закона РК от 21 мая 2013 года «О персональных данных и их защите» в казахстанском законода-

тельстве внедрена правовая основа для защиты прав человека при обработке его персональных данных, в том числе с целью защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Статья 18 Конституции РК запрещает вмешательство в частную жизнь, толкование которой содержит незавершенную, открытую для интерпретации (неисчерпывающую) формулировку (Конституционный Совет 2018: 149). Конституция позволяет законодательным актам раскрыть содержание права на неприкосновенность частной жизни. Специальный Закон Республики Казахстан «О персональных данных и их защите» также дает широкое определение термина «персональные данные» как «сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе».

Конституция и Закон содержат насколько это возможно всеобъемлющую формулировку персональных данных, как любые сведения, относящиеся к конкретному человеку. Аналогичное неисчерпывающее определение понятия персональных данных содержится и в зарубежном законодательстве.

Несмотря на то, что Закон претерпевает изменения, следуя мировым тенденциям, вопросы правового регулирования в нашей стране все еще существуют и требуют решения с учетом зарубежной практики и стандартов. Одной из проблем является правовое закрепление принципов сбора и обработки персональных данных в нашем Законе «О персональных данных и их защите», которые отличаются от принципов, закрепленных зарубежными источниками права.

В статье 5 Закона РК «О персональных данных и их защите» прямо сформулированы следующие пять принципов сбора и обработки персональных данных: (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. Первые три принципа относятся ко всем отраслям права и праву в целом, являются общеправовыми принципами. Принцип конфиденциальности персональных данных ограниченного доступа и принцип равенства прав субъектов, собственников и операторов являются специфичными для

регулирования отношений в сфере защиты персональных данных.

Закон не содержит описания указанных в нем принципов, и их интерпретация вызывает следующие проблемы.

Во-первых, принцип конфиденциальности персональных данных ограниченного доступа создает трудности в правоприменении, поскольку на законодательном уровне нет ясного перечня персональных данных ограниченного доступа.

Закон определяет общедоступные персональные данные как те, которые не являются конфиденциальными в силу закона, доступ к которым разрешен с согласия субъекта. Если субъект не дал согласия на доступ к своим персональным данным и сведениям, следовательно доступ к ним ограничен. Означает ли это, что отсутствие согласия лица влечет ограниченный доступ к его персональным данным, что доступность персональной информации определяется согласием лица?

Но помимо согласия субъекта данных, персональными данными ограниченного доступа являются те, которые отнесены к таковым иным законам. Рассмотрим, что по этому поводу предусматривают другие источники права Казахстана.

Закон РК от 24 ноября 2015 года «Об информатизации» дает классификацию электронных информационных ресурсов по типу содержащихся в них персональных данных как электронные информационные ресурсы, (1) содержащие общедоступные персональные данные и (2) содержащие персональные данные ограниченного доступа. Тип доступа к электронному информационному ресурсу определяется законом, его собственником или владельцем. При этом Закон РК «Об информатизации» тоже устанавливает перечня электронных информационных ресурсов с персональными данными ограниченного доступа, отсылая к Закону РК «О персональных данных и их защите». А в соответствии с последним Законом персональными данными ограниченного доступа являются те, доступ к которым ограничен законом или самим физическим лицом. Таким образом, при определении персональных данных ограниченного доступа Закон «Об информатизации», как и Закон «О персональных данных и их защите» не указывает перечень таких данных и также отсылает к другим законодательным актам.

Далее, рассмотрим другие законы. Закон РК от 30 декабря 2016 года «О дактилоскопической

и геномной регистрации» ясно указывает, что дактилоскопическая и геномная информация относится к персональным данным ограниченного доступа. Другой закон, Закон РК от 19 марта 2010 года «О государственной статистике» указывает, что первичные статистические данные являются конфиденциальными, кроме тех, которые перечислены в этом Законе. Иными словами, Закон «О государственной статистике» очерчивает круг неконфиденциальных статистических данных. Следовательно, *любые другие* данные относятся к конфиденциальным статистическим данным, что говорит о широкой интерпретации понятия. Еще один нормативный акт, Закон РК от 22 декабря 2003 года «О государственной правовой статистике и специальных учетах» регулирует порядок сбора, хранения и обработки персональных данных для специальных учетов, которые как правило касаются правоохранительных и исполнительных функций государственного регулирования общественных отношений. Данным Законом в специальные учеты могут быть внесены *любые сведения* о физическом лице, при этом, не требуется его согласие. Тем не менее, доступ к и использование информации и данных о физическом лице строго регламентированы и должны осуществляться с соблюдением конфиденциальности и требований Закона «О персональных данных и их защите». Очевидно, что такой режим конфиденциальности, установленный в Законе «О государственной правовой статистике и специальных учетах», относит электронные информационные ресурсы государственной правовой статистической системы к электронным информационным ресурсам, содержащим персональные данные ограниченного доступа, но в самом законе нет прямого указания на это. Далее перейдем к Уголовно-Процессуальному и Гражданско-Процессуальному Кодексам, которые ограничивают принцип гласности в связи с охраняемой тайной частной жизни, ссылаясь на требования закона и требование лица о проведении закрытого судебного разбирательства. То есть доступ к и использование персональной информации, характер ограниченного доступа определяются самим лицом, а суд и правоохранительные органы обязаны соблюсти и обеспечить реализацию права на неприкосновенность частной жизни.

В связи с не ясным нормативным закреплением понятий персональных данных ограниченного доступа на практике расходятся позиции регуляторных органов. К примеру, следуя позиции Министерства юстиции РК (Открытый диалог

eGov 2022a) индивидуальный идентификационный номер физического лица-индивидуального предпринимателя является общедоступной информацией о субъекте бизнеса согласно статье 28 Предпринимательского Кодекса РК. С другой стороны, то же Министерство Юстиции РК согласилось с мнением Министерства Внутренних Дел РК (Открытый диалог *eGov 2022б*) о том, что индивидуальный идентификационный номер физического лица относится к персональным данным ограниченного доступа. В пояснениях указанных двух Министерств прослеживается конфликт: индивидуальный предприниматель выступает в двух ипостасях – как обычное лицо и как предприниматель, субъект бизнеса. Соответственно, распространяя в открытом доступе информацию о его контактных данных, индивидуальном идентификационном номере (ИИН), месте ведения бизнеса, которое часто является и его же местом жительства, государство не позаботилось об обеспечении права индивида на неприкосновенность частной жизни и защиту персональных данных. Законодатель не продумал, какие данные все-таки следует особо тщательно защищать, не подвергая риску субъекта от неправомерного посягательства на его интересы, собственность и даже жизнь. Что касается уполномоченного органа в сфере защиты персональных данных, то само Министерство Цифрового Развития и Аэрокосмической Промышленности РК (Открытый диалог *eGov 2022в*) не дало конкретного ответа на вопрос, что входит в перечень персональных данных ограниченного доступа.

Таким образом, законодатель не дал ясной и конкретной интерпретации и правоприменения принципа конфиденциальности персональных данных ограниченного доступа как для самого физического лица, так и для любых лиц и субъектов правоотношений, с кем придется взаимодействовать этому физическому лицу.

Во-вторых, принцип равенства прав субъектов, собственников и операторов является не реализуемым в контексте специального закона о персональных данных, правоотношений, к которым он применяется, правового статуса и позиции сторон правоотношений. Субъекты, собственники и операторы баз персональных данных всегда противостоят друг другу в правоотношении. Объектом правоотношения является информация о субъекте, который контролирует судьбу этой информации, определяет пределы ее распространения и использования собственниками и операторами баз данных. Свобода личности и автономия предполагает независимость

лица, субъекта персональных данных, требует свободы «от принуждения и манипуляции со стороны других» (Sætra 2022: 5). Субъект персональных данных всегда более слабое лицо и находится в неэквивалентном положении, так как его контрагентом в правоотношении на стороне собственника или оператора баз данных выступает либо государственный орган как институт публичной власти, либо субъекты бизнеса, которые имеют экономическое и технологическое преимущество перед физическим лицом. Указанные контрагенты осуществляют чрезмерный сбор данных и имеют доступ к персональным данным лица, несмотря на его согласие, могут осуществлять непрозрачную и неконтролируемую субъектом обработку персональных данных. Американский правовед Даниель Солове (Solove 2023: 22, 40) отмечает, что люди очень доверчивы и поддаются манипулированию, а организации найдут способы манипулировать пользователями, чтобы они согласились на сбор и обработку данных. Чаще всего человек соглашается на сбор и обработку данных здесь и сейчас, так как видит немедленное удовлетворение, конкретные преимущества – получить скидку, использовать продукты и услуги, получить более широкий (премиальный, элитный) доступ к новостям, информации, развлечениям, играм, музыке и многим другим преимуществам и благам. Люди не имеют или имеют смутное представление о том, что произойдет с их данными в отдаленном будущем. Из изложенного следует, что закрепленный Законом РК «О персональных данных и их защите» принцип равенства прав субъектов, собственников и операторов не находит отражения в практической плоскости ввиду неравного и неэквивалентного положения субъектов правоотношения в сфере защиты персональных данных.

Таким образом, Закон РК «О персональных данных и их защите» содержит общеправовые и специальные принципы защиты персональных данных, однако, их интерпретация и правоприменение проблематичны.

Какие принципы содержатся в европейских законах, регламентирующих защиту персональных данных? Рассмотрим некоторые из них.

Прежде всего следует отметить, что на территории Европейского Союза действует Общий Регламент ЕС о защите данных (GDPR), закрепляющий минимальные нормативно-правовые требования защиты персональных данных. Эти требования могут быть детализированы и «усилены» национальным законодательством. Статья

5 GDPR устанавливает 6 основных принципов обработки персональных данных и определяет их значение:

1) Принцип законности, справедливости и прозрачности – персональные данные обрабатываются законно, справедливо и прозрачно по отношению к субъекту данных;

2) Принцип целевого ограничения – персональные данные собираются для определенных, явных и законных целей и не обрабатываются в дальнейшем способом, несовместимым с этими целями;

3) Принцип минимизации данных – персональные данные являются адекватными, актуальными и ограниченными тем, что необходимо в связи с целями, для которых они обрабатываются;

4) Принцип точности – персональные данные должны быть точными и, при необходимости, обновляемыми; должны быть предприняты все разумные меры для обеспечения того, чтобы личные данные, которые являются неточными, с учетом целей, для которых они обрабатываются, были удалены или исправлены без промедления;

5) Принцип ограничения хранения – персональные данные хранятся в форме, позволяющей идентифицировать субъектов данных, не дольше, чем это необходимо для целей, для которых обрабатываются персональные данные;

6) Принцип целостности и конфиденциальности – персональные данные обрабатываются таким образом, который обеспечивает надлежащую безопасность персональных данных, включая защиту от несанкционированной или незаконной обработки, а также от случайной потери, уничтожения или повреждения с использованием соответствующих технических или организационных мер.

В сравнении с принципом законности казахстанского Закона, в GDPR принцип законности, справедливости и прозрачности носит более определенный и специфичный характер. Он касается не только соблюдения закона при сборе и обработке данных, а является одним из фундаментальных понятий и наиболее существенных условий защиты персональных данных. Законность обработки персональных данных подкрепляется в GDPR требованием о наличии согласия физического лица (пункт 11) статьи 4, статья 6). Чтобы быть легитимным согласие должно быть свободно предоставленным, конкретным, информированным (осознанным) и недвусмысленным. Соответственно, без этих обязательных признаков согласия в Европе сбор и обработка

данных признаются незаконными кроме случаев, установленными законом.

Более того, статьи 13 и 14 GDPR устанавливают четкие требования к информации, с которой контролер данных обязан ознакомить субъекта на момент сбора персональных данных. К обязательным сведениям на момент получения согласия от субъекта относятся контакты лица, ответственного за защиту персональных данных, цели обработки, условие о передаче данных третьим лицам с указанием наличия или отсутствия мер по защите персональных данных со стороны третьих лиц, срок или критерии определения срока хранения данных, указание на наличие автоматизированной обработки данных, включая профилирование, и др. Также, на момент сбора персональных данных контролер данных обязан проинформировать субъекта данных о его правах, в особенности о праве отозвать согласие в любой момент, праве на защиту в государственном органе по защите персональных данных, праве на доступ к своим персональным данным, внесение в них уточнений, праве на их стирание (удаление) и др. При этом, согласно статье 12 GDPR контролер и оператор обязаны предоставлять субъекту информацию, касающуюся обработки данных в краткой, прямой, понятной и легкодоступной форме, с использованием ясного и простого языка.

Закон РК «О персональных данных и их защите» в сравнении с GDPR не содержит (а) указанных обязательств собственников баз и операторов при сборе персональных данных, (б) важных требований к информации, предоставляемой субъекту данных до получения согласия на сбор и обработку персональных данных, (в) требований к свободе предоставления согласия и качеству информированности согласия.

Казахстанский Закон (пункт 4 статья 8) и уполномоченный орган устанавливают (Приказ МЦРИАП №395), какие сведения должны содержаться в согласии, как оно может быть предоставлено и даже срок действия согласия, что довольно странно с практической стороны и больше относится к периоду хранения и использования персональных данных. Закон допускает, что собственники и операторы баз данных могут запросить в согласии субъекта иные сведения о нем, однако, уполномоченный орган уточнил (Открытый диалог *eGov* 2022г), что операторы не вправе утверждать и использовать формулировку о возможности сбора и обработки иных персональных данных, перечень должен быть исчерпывающим.

На практике очень часто сбор персональных данных субъектами бизнеса и государственными служащими производится «по умолчанию», потому что в большинстве случаев известно о таком требовании законодательства. Но, как правило, действия операторов и собственников баз данных не подкреплены оформленным запросом на сбор данных, ни предоставлением пояснений о данных, достаточных для конкретного случая, о сроках и безопасности хранения персональных данных. Такая практика широко распространена в силу отсутствия специальных принципов для сбора и обработки персональных данных, а также в связи с отсутствием информированности и правовой культуры среди самих физических лиц, собственников и операторов баз данных.

Далее рассмотрим принципы минимизации данных, целевого ограничения и ограничения хранения персональных данных GDPR (статьи 5.1(b), (c), (e)). Европейским Регламентом *на уровне исходных основополагающих начал* закреплено, 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.

Казахстанский Закон «О персональных данных и их защите» не содержит указанных принципов, но содержит похожие обязательства для собственников и операторов баз данных. В частности, пунктами 8 и 9 статьи 7 Закона установлено, что обработка персональных данных должна быть совместима с целями сбора данных, а содержание и объем данных, подлежащих обработке, не должны быть избыточными по отношению к целям обработки. Согласно пункту 1 статьи 12 Закона сбор персональных данных ограничивается только теми, которые необходимы и достаточны для выполнения *задач*, осуществляемых собственником и (или) оператором, а также третьим лицом. При этом, указанная статья 12 вызывает ряд вопросов. Во-первых, использование терминов и формулировок могут запутать любого человека, не обладающего достаточным уровнем компьютерной или информационной грамотности. Во-вторых, сбор ограничен не целями обработки, а «выполнением задач, осуществляемых собственником и (или) оператором, а также третьим лицом». В-третьих, Закон разрешает обработку персональных данных, совместимую с целями сбора, но что является совместимым с целями обработки определяется собственником и оператором базы данных, а следовательно,

указанные лица могут манипулировать субъектом данных и сформировать необоснованно широкий перечень персональных данных.

Обычному гражданину сложно понять хитросплетения законодательства в сфере защиты персональных данных и информационно-коммуникационных технологий. В *Открытом диалоге eGov* немало обращений граждан, касающихся сбора и обработки персональных данных в соответствии с условиями достаточности и соответствия целям обработки. К примеру, ответ Министерства труда и социальной защиты населения (Открытый диалог *eGov* 2022д) по поводу законности внедрения работодателем пропускной системы и идентификации путем снятия отпечатков пальцев в рамках трудовых отношений не дает полной информации о том, что отпечатки пальцев относятся к биометрическим персональным данным и законодательством определено, в каких случаях и порядке производится сбор дактилоскопии, а также какие лица уполномочены его осуществлять. Кроме того, сбор отпечатков пальцев для целей пропуска и идентификации сотрудников может нарушать условия о сборе и обработке персональных данных, необходимых и достаточных для целей обработки, ведь идентифицировать работника при входе в помещение можно и просто по фотографии. В своих ответах (Открытый диалог *eGov* 2022е) относительно видеонаблюдения и видеосъемки в процессе трудовой деятельности и коммерческих отношений между физическими лицами и субъектами бизнеса государственные органы отвечают гражданам общими формулировками из закона, не ставят акцент или не придают должного внимания степени необходимости и достаточности сбора и обработки персональных данных. Нельзя исключить, что при наличии нормативно закрепленных специальных принципов защиты персональных данных, аналогичных европейским принципам, всем субъектам правоотношений было бы ясно, как осуществлять права и исполнять обязанности по сбору и обработке персональных данных.

Рассмотрим закрепление принципов в иных источниках европейского законодательства о защите персональных данных. Закон о защите персональных данных Эстонии (Personal Data Protection Act of the Republic of Estonia 2007) закрепляет следующие принципы:

1) принцип законности – персональные данные собираются только честным и законным образом;

2) принцип целенаправленности – персональные данные собираются только для дости-

жения определенных и законных целей, и их обработка не должна осуществляться способом, не соответствующим целям обработки данных;

3) принцип минимализма – персональные данные собираются только в объеме, необходимом для достижения определенных целей;

4) принцип ограниченного использования – использование персональных данных в иных целях возможно только с согласия субъекта данных или с разрешения компетентного органа;

5) принцип качества данных – персональные данные должны быть актуальными, полными и необходимыми для достижения цели обработки данных;

6) принцип безопасности – меры безопасности должны применяться в целях защиты персональных данных от невольной или несанкционированной обработки, раскрытия или уничтожения;

7) принцип индивидуального участия – субъект данных уведомляется о собранных о нем данных, субъекту данных предоставляется доступ к касающимся его данным, и субъект данных имеет право требовать исправления неточных или вводящих в заблуждение данных.

Закон о защите данных Великобритании (Data Protection Act 2018), регулирует общие вопросы обработки персональных данных (Part 2), к которым применяются положения и принципы GDPR, а также закрепляет принципы для обработки персональных данных в связи с правоохранительными целями (Part 3). Правоохранительными целями являются цели предотвращения, расследования, выявления или судебного преследования уголовных преступлений или исполнения уголовных наказаний, включая защиту от и предотвращение угроз общественной безопасности. Для правоохранительных целей Законом Великобритании установлены следующие шесть принципов:

1) законности и справедливости обработки – обработка персональных данных для любых правоохранительных целей является законной только в том случае, если и в той степени, в которой она основана на законе, при наличии согласия субъекта на обработку для этой цели или необходимости обработки для выполнения задачи, выполняемой для правоохранительной цели компетентным органом;

2) конкретные, явные и законные цели обработки – цели обработки должны быть конкретными, явными и законными, собранные данные не должны обрабатываться способом, несовместимым с целями обработки;

3) адекватные, актуальные и не чрезмерные персональные данные – обработка данных должна быть адекватной, связанной с целями обработки и не чрезмерной по отношению к цели, для которой они обрабатываются;

4) точные и обновляемые персональные данные – персональные данные должны быть точными и актуальными, своевременно корректироваться, уточняться и удаляться в соответствии с целями обработки;

5) ограничение хранения персональных данных – не храниться дольше, чем необходимо для целей обработки, с учетом регулярного пересмотра необходимости хранения для любых правоохранительных целей;

6) надлежащей безопасности обработки персональных данных – Обработка осуществляется при условии надлежащей защиты персональных данных с использованием соответствующих технических или организационных мер (и в этом принципе «надлежащая безопасность» включает защиту от несанкционированной или незаконной обработки, а также от случайной потери, уничтожения или повреждения).

Закон Великобритании также содержит отдельный раздел (Part 4), посвященный регулированию обработки ПД специальными службами – Службой безопасности, Секретной разведывательной службой, Штабом правительственной связи. Данный раздел закрепляет 6 аналогичных принципов и их описание.

Как видно из вышеприведенных положений, европейские источники права о защите персональных данных устанавливают более конкретные, специфичные принципы для регулирования отношений в сфере защиты персональных данных. Указанные принципы имеют существенное и даже первостепенное значение для защиты персональных данных. Составленные в законодательных актах именно как принципы (основополагающие положения), а не условия исполнения отдельных обязанностей они выполняют роль «проводника» для любых лиц, задействованных в правоотношениях по сбору, обработке и защите персональных данных.

Недостаточно конкретизированное на законодательном уровне закрепление принципов сбора, обработки, хранения и передачи персональных данных собственниками и операторами баз данных, как частных, так и государственных, позволяют третьим лицам получать доступ к личной информации субъектов данных и использовать ее для рекламы, профилирования

пользователей, отслеживания местоположения и прочих целей.

В современных условиях глобализации и реально-виртуальной конвергенции технологического общества новые технологии будут глубоко вмешиваться в личную жизнь каждого человека (Althabhwā 2022: 44). Продолжающееся развитие технологий сделают обмен личной информацией неизбежным и необходимым для участия в жизни современного общества (Saglam 2022: 15). С учетом постоянного развития информационно-коммуникационных технологий, умных домов, умных городов (Smart City) и других умных объектов (smart objects), Интернета Вещей (Internet of Things), Искусственного Интеллекта, роботизации социально-экономических и публично-властных процессов, перед обществом могут встать новые юридические проблемы. Сингапурские авторы (Araz 2019: 119), проанализировав риски, связанные с обработкой персональных данных при использовании автономных транспортных средств (например, электромобилей), отметили, что риски устранимы путем принятия новых законов о защите персональных данных и выработки рекомендаций по принципам конфиденциальности. Основы многих правовых принципов и теорий должны быть пересмотрены в соответствии с новыми реалиями, созданными новой эпохой (Althabhwā 2022: 52). В современных зарубежных законах уже закреплены новые принципы, применимые к защите персональных данных, например, конфиденциальность по умолчанию (Privacy by Default), принцип проектируемой конфиденциальности или конфиденциальность по замыслу (Privacy by Design).

Повсеместное использование передовых информационно-коммуникационных технологий и интенсивный и обширный анализ данных в коммерческой и государственной сферах требуют пересмотра этических и правовых принципов (Raab 2020: 6). Для эффективной защиты персональных данных необходимы принципы регулирования, «которые могут оставаться устойчивыми к быстрым изменениям, простыми перед лицом часто непостижимой сложности, и единообразным по всему спектру отдельных нововведений» (Raab 2020: 14).

Принципы защиты персональных данных, сформулированные в европейских законодательных актах как принципы-нормы, стали продуктом «юридического закрепления объективно сложившейся или желательной практики реализации правовых норм», «обладают универсаль-

ностью, высшей императивностью и общезначимостью» (Вопленко 2013: 6). Юридическая конструкция закрепления принципов права в нормативно-правовом акте играет важную роль на практике (Демичев 2014: 5). Как указывает Врabeц (Vrabec 2021: 33), эти принципы устанавливают «границы для обработки данных и предлагают инструкции для контролеров и обработчиков данных по обработке персональных данных законным и ответственным образом». В законе следует установить данные принципы именно в качестве основных положений или принципов закона о защите персональных данных, поскольку персональные данные являются неотъемлемым элементом конституционного права на неприкосновенность личности и частной жизни, а «каждому самостоятельному праву соответствуют и свои принципы ограничений» (Романовский 2001: 34).

Заключение

Рассмотрев принципы защиты персональных данных, отраженных в национальном и зарубежном законодательстве, можно сделать следующие выводы.

В отличие от казахстанского законодательства в европейских нормативных актах положения, касающиеся всех действий контроллеров, операторов и третьих лиц с персональными данными, а также их обязательства основываются на нормативных принципах.

Несмотря на успешную цифровизацию казахстанского общества и принятие специального Закона «О персональных данных и их защите» многие его элементы не отвечают мировым стандартам. В национальном законодательстве о защите персональных данных отсутствует стратегическое видение движения в сторону принятия ключевых принципов европейского Общего регламента по защите данных GDPR» (Гусарова 2021: 5).

Основой для законодательства являются принципы права. Принципы – это руководящие идеи не только для фиксации их в законе, но и для реализации. Принципы права задают направление и вектор правоприменения, исполнения и соблюдения права на защиту персональных данных. Именно принципы закладывают фундамент всего законодательства и правоприменения и служат основой для любого правоотношения, прав и обязательств его сторон, действия, закрепленных в законодательстве сейчас или в будущем. Иначе говоря, принципы обеспечивают

«единство правотворчества, интерпретации и реализации правовых норм, являются ценностными ориентирами создания и реализации права» (Вопленко 2013 : 7). Поэтому, для целей единогообразного правоприменения и обеспечения

реализации права на защиту персональных данных и неприкосновенность частной жизни, важно максимально учесть нормативные принципы европейского законодательства и закрепить их в казахстанском законодательстве.

Литература

- Data Protection Act 2018 – [электрон. ресурс]. – URL: <<https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>> (дата обращения 15.04.2023)
- Nabeel Mahdi Althabhwawi, Zinatul Ashiqin Zainol, Parviz Bagherib. “Society 5.0: A New Challenge to Legal Norms”. *Sriwijaya Law Review* Vol. 6, Issue 1. (2022): 41-54 [электрон. ресурс]. – URL: <http://journal.fh.unsri.ac.id/index.php/sriwijayalawreview/article/view/1415/pdf> (дата обращения 30.01.2023)
- Personal Data Protection Act of the Republic of Estonia 2007 – [электрон. ресурс]. – URL: <https://www.riigiteataja.ee/en/eli/523012019001/consolide> (дата обращения 15.04.2023)
- Raab, Charles. “Information privacy, impact assessment, and the place of ethics”. *Computer Law & Security Review* Vol.37. (2020):1-16 – [электрон. ресурс]. – URL: <https://doi.org/10.1016/j.clsr.2020.105404> (дата обращения 15.04.2023)
- Rahime Belen Saglam, Jason R.C. Nurse, Duncan Hodges. ‘Personal information: Perceptions, types and evolution’. *Journal of Information Security and Applications*, Volume 66, 2022, 1-31, [электрон. ресурс]. – URL: <https://doi.org/10.1016/j.jisa.2022.103163>, (дата обращения 10.02.2023).
- 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) – [электрон. ресурс]. – URL: <<https://eur-lex.europa.eu/eli/reg/2016/679/oj>> (дата обращения 12.04.2023)
- Sætra, Henrik Skaug. “The ethics of trading privacy for security: The multifaceted effects of privacy on liberty and security”. *Technology in Society* Volume 68. (2022):1-10, -[электрон. ресурс]. – URL: <https://doi.org/10.1016/j.techsoc.2021.101854> (дата обращения 02.03.2023).
- Solove, Daniel J. “Murky Consent: An Approach to the Fictions of Consent in Privacy Law”. *Boston University Law Review* (Forthcoming): 1-51 [электрон. ресурс]. – URL: <http://dx.doi.org/10.2139/ssrn.4333743> (дата обращения 24.02.2023г.)
- Taeihagh, Araz, Hazel Si Min Lim. “Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks”. *Transport Reviews* Vol. 39, Issue 1. (2019):103-128 [электрон. ресурс]. – URL: <<https://doi.org/10.1080/001441647.2018.1494640>> (дата обращения 12.04.2023)
- Vrabec, Helena. *Data Subject Rights under the GDPR*. Oxford Scholarship Online July 2021. Print ISBN-13: 9780198868422. DOI:10.1093/oso/9780198868422.001.0001
- Вопленко Н.Н. и В.А.Рудковский. “Понятие и классификация принципов права”. *Вестник Волгоградского государственного университета* Сер.5, Юриспруд., 2013. №1(18), 5-11 – [электрон. ресурс]. – URL: <https://cyberleninka.ru/article/n/ponyatie-i-klassifikatsiya-printsipov-prava-1> (дата обращения 18.04.2023г.)
- Гусарова, Анна, Серик Джаксылыков. *Защита персональных данных в Казахстане 2.0: Цифровой след Covid-19*, Фонд Сорос-Казахстан 2021, – [электрон. ресурс]. – URL: https://www.soros.kz/wp-content/uploads/2021/03/Personal-Data_Covid-Implications.pdf (дата обращения 15.12.2022г.)
- Демичев, Алексей. “Позитивистская классификация принципов современного российского права”. *Государство и право*. № 5. (2014): 5-13.
- Конституционный Совет РК. “Конституция РК. Научно-практический комментарий” под ред. И.И.Рогова, Астана: 2018. 640 с ISBN 978-601-06-4944-6 УДК 342(035.3)
- Министерство Юстиции РК «Ежегодный обзор о ситуации с правами человека в Республике Казахстан» (2022) – [электрон. ресурс] – URL <https://www.gov.kz/uploads/2022/9/12/97dffcf184945d7c14377ac9e7fbb882_original.1469423.pdf> (дата обращения 15.04.2023)
- Открытый диалог eGov* 2022a – [электрон. ресурс]. – URL: <https://dialog.egov.kz/blogs/all-questions/758957> (дата обращения 18.01.2023г.)
- Открытый диалог eGov* 2022b – [электрон. ресурс]. – URL: <https://dialog.egov.kz/blogs/all-questions/582584> (дата обращения 18.01.2023г.)
- Открытый диалог eGov* 2022в – [электрон. ресурс]. – URL: <https://dialog.egov.kz/blogs/all-questions/702238> (дата обращения 18.01.2023г.)
- Открытый диалог eGov* 2022г – [электрон. ресурс]. – URL: <https://dialog.egov.kz/blogs/all-questions/700318> (дата обращения 18.01.2023г.)
- Открытый диалог eGov* 2022д – [электрон. ресурс]. – URL: <https://dialog.egov.kz/blogs/all-questions/727791> (дата обращения 18.01.2023г.)
- Открытый диалог eGov* 2022е – [электрон. ресурс]. – URL: <https://dialog.egov.kz/blogs/all-questions/724888>, <https://dialog.egov.kz/blogs/all-questions/724882>, <https://dialog.egov.kz/blogs/all-questions/691916> (дата обращения 18.01.2023г.)

Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 21 октября 2020 года № 395/НҚ «Об утверждении Правил сбора, обработки персональных данных» – [электрон. ресурс]. – URL: <<https://adilet.zan.kz/rus/docs/V2000021498>> (дата обращения 17.01.2023).

Романовский, Георгий. *Право на неприкосновенность частной жизни*. Москва: МЗ-Пресс 2001. 312 с., ISBN 5-94073-018-3 – [электрон. ресурс]. – URL: <https://library.khpg.org/files/docs/1430850257.pdf> (дата обращения 15.04.2023)

Спутник-Казахстан 2022а – [электрон. ресурс]. – URL: <https://ru.sputnik.kz/20221019/tsifrovoy-kazakhstan-strana-vzletaet-v-reytingakh-razvitiya-digital-sfery-28609363.html>, (дата обращения 19.01.2023г.)

Спутник-Казахстан 2022б – [электрон. ресурс]. – URL: <https://ru.sputnik.kz/20221014/kazakhstan-vkhodit-v-tridtsatku-samykh-otsifrovannykh-stran-oon--tokaev--28483227.html>, (дата обращения 19.01. 2023г.)

“Стратегия «Казахстан-2050»: новый политический курс состоявшегося государства.” – [электрон.ресурс] – URL <<https://adilet.zan.kz/rus/docs/K1200002050>> (дата обращения 23.01.2023)

References

Data Protection Act 2018 – [electron. resource]. – URL: <<https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>> (accessed 15.04.2023)

Nabeel Mahdi Althabhwai, Zinatul Ashiqin Zainol, Parviz Bagherib. “Society 5.0: A New Challenge to Legal Norms”. Sriwijaya Law Review Vol. 6, Issue 1. (2022):41-54 [electron. resource]. – URL: <http://journal.fh.unsri.ac.id/index.php/sriwijayalawreview/article/view/1415/pdf> (accessed 30.01.2023)

Personal Data Protection Act of the Republic of Estonia 2007 – [electron. resource]. – URL: <https://www.riigiteataja.ee/en/eli/523012019001/consolide> (accessed 15.04.2023)

Raab, Charles. “Information privacy, impact assessment, and the place of ethics”. Computer Law & Security Review Vol.37. (2020):1-16 – [electron. resource]. – URL: <https://doi.org/10.1016/j.clsr.2020.105404> (accessed 15.04.2023)

Rahime Belen Saglam, Jason R.C. Nurse, Duncan Hodges. ‘Personal information: Perceptions, types and evolution’. Journal of Information Security and Applications, Volume 66, 2022, 1-31, [electron. resource]. – URL: <https://doi.org/10.1016/j.jisa.2022.103163> , (accessed 10.02.2023).

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) – [electron. resource]. – URL: <<https://eur-lex.europa.eu/eli/reg/2016/679/oj>> (accessed 12.04.2023)

Sætra, Henrik Skaug. “The ethics of trading privacy for security: The multifaceted effects of privacy on liberty and security”. Technology in Society Volume 68. (2022):1-10, -[electron. resource]. – URL: <https://doi.org/10.1016/j.techsoc.2021.101854> (accessed 02.03.2023).

Solove, Daniel J. “Murky Consent: An Approach to the Fictions of Consent in Privacy Law”. Boston University Law Review (Forthcoming):1-51 [electron. resource]. – URL: <http://dx.doi.org/10.2139/ssrn.4333743> (accessed 24.02.2023)

Taeihagh, Araz, Hazel Si Min Lim. “Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks”. Transport Reviews Vol. 39, Issue 1. (2019):103-128 [electron. resource]. – URL: <<https://doi.org/10.1080/01441647.2018.1494640>> (accessed 12.04.2023)

Vrabec, Helena. Data Subject Rights under the GDPR. Oxford Scholarship Online July 2021. Print ISBN-13: 9780198868422. DOI:10.1093/oso/9780198868422.001.0001

Voplenko N.N. and V.A. Rudkovsky. “The concept and classification of the principles of law”. Bulletin of Volgograd State University Ser.5, Yurisprud., 2013. №1(18), 5-11 – [electron. resource]. – URL: <https://cyberleninka.ru/article/n/ponyatie-i-klassifikatsiya-printsipov-prava-1> (accessed 18.04.2023).

Gusarova, Anna, Serik Dzhaksylykov. Personal Data Protection in Kazakhstan 2.0: Covid-19 Digital Footprint, Soros Foundation-Kazakhstan 2021, – [electron. resource]. – URL: https://www.soros.kz/wp-content/uploads/2021/03/Personal-Data_Covid-Implications.pdf (accessed 15.12.2022)

Demichev, Alexey. “Positivist classification of the principles of modern Russian law”. State and law. № 5. (2014): 5-13.

Constitutional Council of the Republic of Kazakhstan. “The Constitution of the Republic of Kazakhstan. Scientific and Practical Commentary” edited by I.I.Rogov, Astana: 2018. 640 with ISBN 978-601-06-4944-6 UDC 342(035.3)

Ministry of Justice of the Republic of Kazakhstan “Annual review of the human rights situation in the Republic of Kazakhstan” (2022) – [electron.resource] – URL <https://www.gov.kz/uploads/2022/9/12/97dffcf184945d7c14377ac9e7fbb882_original.1469423.pdf> (accessed 15.04.2023)

Open Dialogue eGov 2022a – [electron. resource]. – URL: <https://dialog.egov.kz/blogs/all-questions/758957> (accessed 18.01.2023)

Open Dialogue eGov 2022b – [electron. resource]. – URL: <https://dialog.egov.kz/blogs/all-questions/582584> (accessed 18.01.2023)

Open Dialogue eGov 2022b – [electron. resource]. – URL: <https://dialog.egov.kz/blogs/all-questions/702238> (accessed 18.01.2023)

Open Dialogue eGov 2022 – [electron. resource]. – URL: <https://dialog.egov.kz/blogs/all-questions/700318> (accessed 18.01.2023)

Open Dialogue eGov 2022d – [electron. resource]. – URL: <https://dialog.egov.kz/blogs/all-questions/727791> (accessed 18.01.2023)

Open Dialogue eGov 2022e – [electron. resource]. – URL: <https://dialog.egov.kz/blogs/all-questions/724888> , <https://dialog.egov.kz/blogs/all-questions/724882> , <https://dialog.egov.kz/blogs/all-questions/691916> (accessed 18.01.2023)

Order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated October 21, 2020 No. 395/NK “On approval of the Rules for the collection and processing of personal data” – [electron. resource]. – URL: <https://adilet.zan.kz/rus/docs/V2000021498> > (accessed 17.01.2023).

Romanovsky, George. The right to privacy. Moscow: MZ-Press 2001. 312 p., ISBN 5-94073-018-3 – [electron. resource]. – URL: <https://library.khpg.org/files/docs/1430850257.pdf> (accessed 15.04.2023)

Sputnik-Kazakhstan 2022a – [electron. resource]. – URL: <https://ru.sputnik.kz/20221019/tsifrovoy-kazakhstan-strana-vzletaet-v-reytingakh-razvitiya-digital-sfery-28609363.html> , (accessed 19.01.2023)

Sputnik-Kazakhstan 2022b – [electron. resource]. – URL: <https://ru.sputnik.kz/20221014/kazakhstan-vkhodit-v-tridtsatku-samykh-otsifrovannykh-stran-oon--tokaev--28483227.html> , (accessed 19.01. 2023)

“Strategy “Kazakhstan-2050”: a new political course of the established state.” – [electron.resource] – URL < <https://adilet.zan.kz/rus/docs/K1200002050> > (accessed 23.01.2023)