ҚҰҚЫҚ

УДК 343.982.35
МРНТИ 10.77.51

DOI: https://doi.org/10.37788/2025-3/112-122

О.Б. Дубовицкая[1*]
[1]Торайгыров университет, Казахстан
[*](e-mail: o.b.d.1970@mail.ru)

Обзор судебной практики по персональным данным в Казахстане

Аннотация

Основная проблема: Несмотря на наличие в Казахстане специального законодательства о защите персональных данных, включая Закон «О персональных данных и их защите», правоприменительная практика остается неразвитой и несистемной. Отсутствие четких критериев законности обработки данных, слабая регламентация требований к согласию субъекта, а также недостаточная информированность населения и бизнеса приводят к массовым нарушениям прав на конфиденциальность. Существенные проблемы возникают в сфере обработки данных субъектами малого и среднего бизнеса, а также при взаимодействии граждан с государственными и частными структурами.

Цель: Проанализировать современное состояние правового регулирования и судебной практики в Казахстане по вопросам персональных данных, выявить ключевые пробелы и несоответствия законодательных норм международным стандартам, в частности GDPR, а также предложить направления для совершенствования правоприменительной практики и законодательства.

Методы: В исследовании использованы сравнительно-правовой, нормативно-правовой, эмпирический (анализ судебных кейсов), а также системный подходы. Проведен сопоставительный анализ национального законодательства Казахстана и европейского законодательства (включая GDPR) с акцентом на практические кейсы.

Результаты и их значимость: Установлено, что в Казахстане отсутствуют четкие требования к форме и содержанию согласия субъекта персональных данных, не обеспечен механизм информирования граждан о целях и способах обработки данных. Обнаружены существенные расхождения с международными стандартами, в том числе в части принципов минимизации, целевого ограничения и прозрачности. Проанализированные судебные кейсы свидетельствуют о низком уровне правовой культуры среди операторов данных и слабой реализации надзорных функций уполномоченных органов. Предложены рекомендации по приведению законодательства в соответствие с международными нормами, усилению институциональной роли органов контроля и развитию правосознания у субъектов персональных данных.

Ключевые слова: персональные данные, защита информации, судебная практика, казахстанское законодательство, GDPR.

Введение

Вопросы защиты персональных данных (или конфиденциальности) на протяжении нескольких лет привлекают все больше внимания со стороны правительств, бизнеса и населения. Тем не менее сложно сказать, что в Казахстане представители государственных и частных структур, а также население полностью «созрело» или всецело осознает, как важно с должным вниманием относиться к персональным данным, вопросам их сбора и обработки.

Европейский опыт показывает, насколько серьезно относится к защите персональных данных Европейский Союз, его регуляторные органы по защите персональных данных, частный сектор и, что немаловажно, само население. С 1970-х годов Европа планомерно и поступательно движется в совершенствовании законодательства и правоприменения в сфере защиты персональных данных. Коллизии национальных законов, трудности правоприменительной практики, в особенности применительно к международной передаче

данных, привели к таким международным инструментам, как Руководящие принципы ОЭСР (OECD Guidelines [1]) и Конвенция 108 (Convention 108 [2]). Данные международные акты стали одними из первых, определявших основные принципы и нормы в сфере защиты персональных данных в Европейском союзе. Основываясь на принципах указанных международных документов, в Европе была принята Директива о защите персональных данных 1995 года (Директива ЕС 1995 года [3]). Более чем 20-летняя практика правоприменения Директивы 1995 года и судебные решения Европейского суда сформулировали глобальный «золотой стандарт» в правовом регулировании защиты персональных данных – Общий Регламент ЕС о Защите Данных (GDPR [4]).

Не секрет, что именно под влиянием Директивы ЕС 1995 года, а теперь и GDPR, неевропейские государства практически во всем мире «вынуждены» были принять или изменить свое законодательство в сфере защиты персональных данных, чтобы отвечать требованиям адекватного правового режима защиты персональных данных резидентов Европейского Союза. К слову, трудно сказать, что казахстанский режим полностью отвечает таким требованиям, а это может означать, что в нашей стране существуют риски для сбора и обработки персональных данных физических лиц Европейского Союза, до тех пор, пока не будет реализован соответствующий правовой режим.

Тем не менее, Казахстан также стремится идти в ногу со временем и мировым веянием. Наш Закон РК №94-V от 21 мая 2013 года «О персональных данных и их защите» (далее – Закон), продолжает развиваться и эволюционирует, и к слову сказать неплохо. Но, мы все еще далеки от мировых стандартов, исчерпывающей интерпретации и реализации правовых норм.

Следует отметить, что в последние годы защита персональных данных в Казахстане приобрела особую актуальность. Государство ужесточает регулирование в этой сфере, а ответственность за нарушения становится все более серьезной. Причина этого очевидна: в открытом доступе регулярно появляются новости о масштабных утечках информации, затрагивающих казахстанцев.

Материалы и методы

В основе анализа лежит метод сравнительного правового исследования, в рамках которого было сопоставлено законодательство Республики Казахстан и Европейского союза, включая:

Закон РК «О персональных данных и их защите»;

Приказ № 395/НҚ от 21 октября 2020 года, регулирующий правила сбора и обработки персональных данных;

Постановление Правительства РК №1214, устанавливающее порядок определения перечня необходимых данных;

Общий регламент по защите данных (GDPR) – в качестве эталонного международного документа;

Судебная практика Казахстана, представленная через конкретные кейсы;

Ответы государственных органов РК на вопросы граждан в системе eGov;

Результаты социологических исследований по уровню цифровой грамотности населения и знанию своих прав.

Анализу также подвергались практические кейсы из казахстанской действительности, примеры из международной правоприменительной практики, включая знаковые европейские дела, такие как Google Spain и обращения Максимилиана Шремса.

Методология включает в себя анализ норм права, сопоставление практик, выявление пробелов и недостатков, а также эмпирические наблюдения на основе обращений граждан и поведения бизнеса в реальных условиях.

Результаты

Одним из громких примеров стали факты продажи персональных данных граждан банками, а также случаи их утечки в Китай. Такие инциденты не могли остаться без внимания, и теперь государство вводит новые правила, согласно которым защита персональных данных становится приоритетом. Уже с марта 2025 года штрафы за незаконный сбор и обработку персональных данных увеличились в два-три раза. Теперь малый и средний бизнес столкнется со штрафами в размере 450 и 750 евро соответственно, а крупный бизнес – около 1500 евро. Причем эти суммы применяются за каждый выявленный факт незаконного сбора и обработки персональных данных.

Такой подход приближает Казахстан к уровню регулирования в странах региона. Например, в Беларуси за аналогичное нарушение предусмотрен штраф до 600 евро, тогда как в России за те же деяния штрафы значительно выше – до 7 000 евро для юридических лиц.

При этом, если сравнивать с европейскими странами, где за нарушение законодательства о персональных данных (GDPR) компании могут получить штрафы в миллионы евро, казахстанские меры остаются относительно мягкими.

Обсуждение

К числу важных вопросов относятся такие как правильно оформлять документы, регулирующие обработку персональных данных, включая согласия и политики. Проанализируем, как эти нормы применяются на практике: какие кейсы уже рассматривались судами в Казахстане, кого привлекали к ответственности и насколько эта проблема касается малого и среднего бизнеса.

И, так, кого касаются требования по обработке персональных данных в Казахстане?

Распространено мнение, что регулирование персональных данных затрагивает только крупные корпорации, поскольку их деятельность связана с обработкой больших массивов информации. Это мнение во многом обусловлено сложностью нормативных требований, включающих локализацию серверов, разработку внутренних политик, назначение ответственных сотрудников и внедрение технических мер защиты данных. Эти требования действительно требуют значительных ресурсов, и их выполнение может оказаться сложным для малого и среднего бизнеса. Однако законодательство не делает различий по размеру компании – все субъекты бизнеса обязаны соблюдать требования по обработке и защите персональных данных. На практике это означает, что даже небольшие компании могут столкнуться с санкциями за халатное отношение к обработке персональных данных, если не уделят этому вопросу должного внимания.

Рассмотрим некоторые европейские и казахстанские требования к согласию субъекта на сбор и обработку персональных данных.

В европейском законодательстве о защите данных согласие являлось и является одним из ключевых понятий и наиболее существенных условий фундаментального принципа защиты данных – законности. В соответствии со статьей 2 Директивы ЕС 1995 года согласие определялось как: «Любое свободно предоставленное конкретное и информированное указание на его пожелания, которым субъект данных выражает свое согласие на обработку персональных данных, касающихся его». Действующий GDPR (пункт 11) статьи 4) в определении согласия устанавливает обязательные условия для сбора и обработки персональных данных. Чтобы быть легитимным согласие должно быть свободно предоставленным, конкретным, информированным (осознанным) и недвусмысленным. Соответственно, при отсутствии этих обязательных признаков согласия в Европе сбор и обработка данных будут незаконными за некоторыми исключениями.

Казахстанский Закон (пункт 4 статья 8) и Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 21 октября 2020 года № 395/НҚ «Об утверждении Правил сбора, обработки персональных данных» устанавливают, что должно содержаться в согласии, как оно может быть предоставлено и даже срок действия согласия (что кажется абсурдным и должно касаться больше информации о сроке хранения и использования персональных данных). Более того, наше законодательство предоставляет право контролеру и оператору данных определять в согласии субъекта иные сведения (персональные данные субъекта). Однако, в своем ответе МЦРИАП [5] уточнил, что «утверждение и использование операторами перечня открытого типа (содержащего формулировки относительно возможности сбора и обработки иных персональных данных, прямо не перечисленных в перечне) не допускается».

Таким образом, казахстанские нормы не содержат обязательных признаков, при которых согласие считается полученным и легитимным, к примеру, свободно предоставленное (то есть без какого-либо давления или «вынужденности» дать согласие) и информированное (осознанное). Стоит отметить, что обязательное информированное согласие лица (пациента) предусмотрено Кодексом Республики Казахстан от 7 июля 2020 года № 360-VI «О здоровье народа и системе здравоохранения» (с изменениями и дополнениями по состоянию на 26.02.2023 г.).

В отношении информированного согласия рассмотрим два примера сбора и обработки персональных данных, с которым на практике столкнулся гражданин – обращение к услугам

фитнес-центра и оформление абонемента. В первом случае членство в фитнес-центре оформлялось сотрудником, который внес в базу ФИО лица, дату рождения, номер телефона. Далее, сотрудник фитнес-центра попросил посмотреть в камеру и выдал электронный браслет, сказав, что в нем хранятся все персональные данные, которые предоставляют доступ гражданину к услугам фитнес-центра согласно условиям членства.

Другой пример, заключение договора с образовательным учреждением на образовательные услуги для школьника, когда учреждение образования собирает сведения о ребенке, его родителях, их образовании, социальном статусе, месте жительства и работы, контактные данные.

Ни одно действие сотрудников фитнес-центра и образовательного учреждения не сопровождалось ни запросом согласия на сбор и обработку персональных данных, ни предоставлением пояснений о данных, достаточных для оказания услуг фитнес-центра или образовательных услуг, о сроках и безопасности хранения персональных данных. И такое происходит повсеместно в силу отсутствия обязательств для собственников баз персональных данных и операторов, а также в связи с отсутствием информированности и правовой культуры среди населения и предпринимательства.

В отличие от казахстанских норм, статьи 13 и 14 GDPR устанавливают четкие требования к информации, которую контролер данных обязан предоставить субъекту на момент сбора персональных данных. В числе таких обязательных сведений при получении согласия от субъекта указаны 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 [6], включая профилирование, и др. Кроме того, на момент сбора персональных данных GDPR обязывает контролера данных проинформировать субъекта данных о его правах, в частности праве отозвать согласие в любой момент [7], 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.

Очевидно, что казахстанский Закон не содержит такого спектра информации, которая должна предоставляться собственниками баз персональных данных и их операторами, ни таких обязательств собственников баз и операторов при сборе персональных данных, то есть до получения согласия субъекта данных на сбор и обработку персональных данных. Дополнительно хотелось бы отметить, что наш Закон не содержит обязанность собственника базы персональных данных и оператора, аналогично статье 12 GDPR, в краткой, прямой, понятной и легкодоступной форме, с использованием ясного и простого языка предоставлять субъекту информацию, касающуюся обработки данных.

Как видно из вышеприведенных положений, европейские нормы о защите персональных данных устанавливают более конкретные обязательства для контролеров и операторов персональных данных, а также третьих лиц. Тем самым физические лица получают возможность контролировать действия в отношении своих персональных данных, имеют больше информации о том, как используются и защищаются их данные. В свою очередь, информированность повышает правовое сознание и правовую культуру в обществе, создает эффективность правоприменения.

Обратимся к такой практике. Часто мы не задумываясь отправляем с помощью мобильных приложений фото личных и иных документов, не говоря о банковских картах и иной информации, по запросу сотрудников государственных органов и предпринимательства, знакомым и совсем не знакомым людям. Мы не задумываемся, что действительно нужно в конкретной ситуации, а что излишне, кому будет дальше передана информация и кто может иметь к ней доступ. Конечно, с целью быстрого получения какой-либо государственной услуги, товара или услуги в сфере бизнеса, люди не задумываются о последствиях. Чаще всего это происходит от незнания и неинформированности не только самих граждан, но и государственных служащих и бизнеса. А бизнес не задумывается, пока не придет проверка и не будет возбуждено дело об административном правонарушении.

В то же время, любой субъект бизнеса, организация и государственный орган могут быть отнесены к собственникам и операторам баз персональных данных, которые обязаны соблюдать условия сбора, обработки и хранения персональных 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. Казалось бы, что положения указанных норм позволяют получить (собрать) персональные данные больше, чем необходимо для целей обработки, но обрабатывать следует только те, которые совместимы с целью обработки. Однако, пункт 1 статьи 12 Закона не позволяет выполнять излишний сбор персональных данных, ограничивая 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, в ней законодатель использует формулировку «накопление, осуществляемое путем сбора», а в статье 1 Закона даются определения накопления [8] и сбора [9] персональных данных, которые могут запутать обычного 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». Это положение уточняется Постановлением Правительства от 12 ноября 2013 года № 1214 «Об утверждении Правил определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач». Постановление устанавливает, что цели являются однозначными, законными и соответствуют осуществляемым собственником и (или) оператором задачам. Тем не менее, понимание этих формулировок остается не до конца ясным. В-третьих, учитывая, что пункт 8 статьи 7 Закона позволяет обработку персональных данных, совместимую с целями сбора, собственник и оператор, как лица, определяющие совместимость целям обработки, могут сформировать широкий перечень персональных данных.

Указанным Постановлением предусмотрена обязанность собственников, операторов провести анализ осуществляемых задач на предмет использования персональных данных. Проще говоря, собственники и операторы должны проанализировать свою деятельность и действия, которые они совершают с персональными данными, почему и для чего они их совершают (есть ли законные основания), какие именно персональные данные им для этого необходимы. По результатам такого анализа, который должен проводиться ежегодно, собственники и операторы утверждают перечень [10] персональных данных, необходимый и достаточный для выполнения осуществляемых задач и ежегодно его корректируют. Следовательно, в соответствии с данным перечнем от субъекта надлежит получить согласие с перечислением конкретных персональных данных (подпункт 7) пункта 4 статьи 8 Закона).

До того, как брать согласие Закон требует от собственников и операторов ясно знать, какие именно персональные данные, какой их минимум достаточен и для каких целей и задач нужны. На практике все происходит иначе. К примеру, при заключении договора на обучение ребенка в образовательном учреждении, достаточны ФИО ребенка, дата рождения, адрес, возможно свидетельство о рождении, ФИО родителей, номера их удостоверений личности и контакты, включая контакты по месту работы.

Каким образом ИИН родителей связан с процессом оказания образовательных услуг ребенку? Присутствует ли в этом случае совместимость целям обработки? Образовательному учреждению достаточно сверить данные о родителях в свидетельстве о рождении и удостоверении личности. Будет ли сбор и хранение ИИН родителя образованием учреждения нарушать пункты 8 и 9 статьи 7 Закона? Обычному гражданину сложно понять хитросплетения законодательства в сфере защиты персональных данных и информационно-коммуникационных технологий.

Казахстанцы обеспокоены этими вопросами, стараются получить больше информации и повысить правовую грамотность. В Открытом диалоге eGov немало обращений граждан, касающихся сбора и обработки персональных данных в соответствии с условиями достаточности и соответствия целям обработки. Рассмотрим некоторые из них.

Еще пример. Женщина обратилась [11] к Министру труда и социальной защиты населения по поводу законности внедрения работодателем пропускной системы и идентификации путем снятия отпечатков пальцев, отнесения отпечатков пальцев к персональным данным. Министерство в ответе сослалось на необходимость соблюдения принципов Закона и получения согласия работника. Понятно, что ответ Министерства не дает полной информации относительно отнесения отпечатков пальцев к биометрическим персональным данным и органов, уполномоченных осуществлять сбор дактилоскопической

информации. Кроме того, в зависимости от вида деятельности компании-работодателя сбор отпечатков пальцев для целей пропуска и идентификации сотрудников все-таки может нарушать условия о сборе и обработке персональных данных, необходимых и достаточных для целей обработки.

Несколько обращений граждан к министерствам касались видеонаблюдения и видеосъемки [12] в процессе трудовой деятельности и коммерческих отношений между физическими лицами и субъектами бизнеса. Ответы государственных органов ограничивались общими формулировками о необходимости соответствия сбора и обработки персональных данных требованиям законодательства, наличии уведомления о проведении видеонаблюдения и согласия субъекта. Возможно, в этих ответах скрыто послание о законности собирать и обрабатывать персональные данные посредством видеофиксации при условии, что изображение человека является необходимой и достаточной информацией для целей обработки (а именно, задач работодателя и субъекта бизнеса). Тем не менее, государственные органы в своих ответах гражданам не ставят акцент или не придают должного внимания степени необходимости и достаточности сбора и обработки персональных данных. Как уже отмечалось выше, отсутствие надлежащей информированности среди населения и бизнеса формирует правовую культуру и эффективное правоприменение в стране.

Перейдем к похожим положениям об ограничении сбора, обработки и хранения GDPR, а именно к важным принципам защиты персональных данных GDPR: целевого ограничения (статья 5.1(b)), минимизации данных (статья 5.1(c)) и ограничения хранения (статья 5.1(e)).

Принцип целевого ограничения означает, что персональные данные собираются для определенных, явных и законных целей и не обрабатываются в дальнейшем способом, несовместимым с этими целями.

Принцип минимизации данных требует, чтобы персональные данные были адекватными (достаточными), соответствующими (относящимися) и ограниченные тем, что необходимо в связи с целями обработки.

Принцип ограничения хранения означает, что персональные данные хранятся в форме, позволяющей идентифицировать субъектов данных, не дольше, чем это необходимо для целей, для которых обрабатываются персональные данные. При этом допускается последующее хранение персональных данных в течение более длительного периода исключительно для целей архивирования в общественных интересах, научных или исторических исследований или статистических при условии выполнения соответствующих технических и организационных мер для защиты прав и свобод субъекта данных.

Эти принципы имеют существенное и даже первостепенное значение для защиты персональных данных. Сформулированные в Европейском Регламенте именно как принципы (основополагающие положения), а не условия, они выполняют роль «проводника» для всех лиц, задействованных в правоотношениях по сбору, обработке и защите персональных данных. Эти основополагающие идеи прослеживаются в дальнейших нормах GDPR, касающихся прав и обязательств контролеров, операторов, третьих лиц, государственных органов и самих субъектов. 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.

Стоит согласиться с мнением А. Гусаровой и С. Джаксылыкова, что в Казахстане «несмотря на наличие Закона о персональных данных, многие его элементы на практике пробуксовывают, а также отсутствует стратегическое видение движения в сторону принятия ключевых принципов европейского Общего регламента по защите данных GDPR».

Важно отметить, что роль населения и органов по защите персональных данных в Европе имела значительную роль в формировании правового режима и правоприменительной практики. Некоторыми примерами служат известное не только в Европе дело Google Spain, впервые закрепившее the Right to be Forgotten (право на забвение), определившее роль поисковых систем при обработке персональных данных и вопрос о совместимости и чрезмерности обработки персональных данных целям сбора и обработки. В последние годы несколько обращений г-на Максимилиана Шремс в Европейский суд оказали влияние на вопросы адекватности защиты персональных данных.

Как и во всем мире, вопрос защиты персональных данных не безразличен и для казахстанцев. Серьезную озабоченность среди граждан проблемы защиты личной информации вызвали в период пандемии, особенно касательно приложения ASHYQ. В Открытом диалоге

eGov задавались вопросы о сборе, обработке персональных данных, в частности ИИН лица, платформой ASHYQ. В своих ответах МЦРИАП указал, что ИИН и статус лица в приложении ASHYQ не являются персональными данными, поскольку в отдельности от других дополнительных сведений о лице не позволяет его идентифицировать. Иными словами, в зависимости от ситуации ИИН сам по себе без дополнительных личных сведений не позволяет определить или сделать лицо определяемым.

Конечно, значительный рост использования интернета и предоставления персональных данных во время пандемии COVID-19, повлияли на культуру обращения с персональной информацией. К примеру, в 2019 году, в рамках исследования был проведен опрос общественного мнения, который показал отсутствие знаний или поверхностные знания пользователей интернет по защите личной информации и незнание своих прав как субъектов персональных данных. Исследование А. Гусаровой и С. Джаксылыкова, проведенное в сентябре 2020 года, показало, что только 20 % опрошенных хорошо осведомлены о защите персональных данных. То есть наблюдается незначительная положительная динамика, хотя среди самых старших пользователей интернета, а также среди сельских жителей наблюдается наиболее низкий уровень знаний о защите персональных данных. Следует заметить, что в том же 2020 году по данным Официального Информационного ресурса Премьер-Министра РК 78 % населения осведомлены об угрозах кибербезопасности. Возможно не совсем корректно сопоставлять данные исследования о защите персональных данных и кибербезопасности, тем не менее, это взаимосвязанные явления, и, скорее всего, официальные данные мало отражают действительное положение дел.

Несомненно, следует повышать осведомленность граждан об их правах на защиту персональных данных и прежде всего регулирующими эту сферу государственными органами путем предоставления и распространения простых и понятных печатных и видеоматериалов. Возможно следует перенять европейский опыт, который на уровне нормативного акта высокого уровня закрепил обязательства контролеров и операторов данных о предоставлении полной информации о перечне собираемых персональных данных и правах физического лица до получения согласия на сбор и обработку данных.

Рассмотрим еще некоторые примеры из судебной практики Казахстана.

Кейс 1

Небольшая компания, оказывающая услуги проводной телекоммуникационной связи для государственных органов, была привлечена к ответственности за незаконное использование персональных данных бывшего сотрудника. Компания участвовала в тендере, для которого требовалось наличие квалифицированного персонала, и включила в конкурсную документацию данные бывшего сотрудника без его явного согласия.

Обнаружив это, бывший сотрудник подал жалобу в уполномоченный орган по защите персональных данных, что привело к внеплановой проверке и составлению административного протокола. По итогам рассмотрения компании был назначен штраф в размере 140 евро.

Не согласившись с решением, компания обратилась в суд, заявив, что согласие сотрудника было получено устно, а доступ к документам имели только участники закупок. Однако суд указал, что устного согласия недостаточно – требуется письменное подтверждение. Кроме того, штраф был оплачен в порядке сокращенного производства, что фактически расценивается как признание нарушения. В итоге суд подтвердил законность наложенного штрафа.

Кейс 2

Гражданин Казахстана оформил кредит в местном банке и при подаче заявки указал в качестве контактных данных ФИО и телефон своего знакомого, не имея на это его явного согласия. В результате банк на протяжении двух лет систематически звонил по этому номеру с целью поиска заемщика.

Обладатель номера, не имеющий отношения к кредитному договору, неоднократно сообщал сотрудникам банка, что его ФИО и контактные данные используются без его согласия, и требовал прекратить обработку. Однако звонки продолжались.

В итоге суд установил, что банк не имел законных оснований для обработки персональных данных данного гражданина, поскольку он не давал согласия на их использование. Более того, банк не предпринял мер для проверки правомерности обработки данных, несмотря на поступавшие обращения.

Суд квалифицировал действия банка как незаконный сбор и обработку персональных данных и назначил административный штраф в размере 400 евро.

Кейс 3

Государственное учреждение в городе Алматы было привлечено к ответственности за использование персональных данных граждан в информационной системе без получения их согласия. Суд установил, что в системе хранились персональные данные граждан, при этом согласие на их обработку не было оформлено надлежащим образом.

Представители учреждения пытались оспорить составленный протокол, указывая на процессуальные недостатки и на то, что данные обрабатывались сторонней организацией. Однако суд признал нарушение обоснованным и отказал в удовлетворении жалобы и назначил учреждению административный штраф в размере 140 евро.

Заключение

В заключении следует отметить, что в данной статье была затронута лишь часть комплексного института защиты персональных данных. Многими авторами и сообществами затрагиваются и иные вопросы правоприменения и регулирования защиты личных данных, в том числе с активным обсуждением на уровне Правительства и Парламента. Наше законодательство в этой сфере будет продолжать развиваться вслед за развитием информационно-коммуникационных технологий и процессами глобализации экономики. Возможно будет перенят и европейский опыт.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Рекомендация Совета ОЭСР относительно руководящих принципов, регулирующих защиту конфиденциальности и трансграничных потоков персональных данных от 23 сентября 1980 года (обновлена 11 июля 2013 года).

2 Конвенция Совета Европы №108 «О защите лиц в связи с автоматизированной обработкой персональных данных» от 28 января 1981 года.

3 Директива Европейского Парламента и Совета ЕС 95/46/ЕС от 24 октября 1995 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных.

4 Регламент (ЕС) 2016/679 Европейского Парламента и Совета от 27 апреля 2016 года о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46/ЕС (General Data Protection Regulation).

5 Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года № 94-V // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет».

6 Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК // ИПС «Әділет».

7 Постановление Правительства Республики Казахстан от 12 ноября 2013 года № 1214 «Об утверждении Правил определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач» // ИПС «Әділет».

8 Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 21 октября 2020 года № 395/НҚ «Об утверждении Правил сбора и обработки персональных данных» // ИПС «Әділет».

9 Google Spain v Agencia Española de Protección de Datos (AEPD) and González, Case C-131/12, 13 May 2014 // EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131

10 Гусарова А., Джаксылыков С. Защита персональных данных в Казахстане: статус, риски и возможности. – Алматы: Фонд Сорос-Казахстан, 2020. – 56 с. URL: https://www.soros.kz/wp-content/uploads/2020/04/Personal_data_report.pdf

11 Гусарова А., Джаксылыков С. Защита персональных данных в Казахстане 2.0: Цифровой след Covid-19. – Алматы: Фонд Сорос-Казахстан, 2021. – 80 с. URL: https://www.soros.kz/wp-content/uploads/2021/03/Personal-Data_Covid-Implications.pdf

12 Ташкараев Ж. Обзор судебной практики по персональным данным в Казахстане // Revera Kazakhstan. URL: https://kazakhstan.revera.legal/info-centr/news-and-analytical-materials/229-obzor-sudebnoj-praktiki-po-personalnym-dannym-v-kazaxstane/

REFERENCES

1 Rekomendatsiya Soveta OESR otnositel'no rukovodyashchikh printsipov, reguliruyushchikh zashchitu konfidentsial'nosti i transgranichnykh potokov personal'nykh dannykh ot 23 sentyabrya 1980 goda (obnovlena 11 iyulya 2013 goda) [OECD Council Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of September 23, 1980 (updated July 11, 2013)]. [in Russian].
2 Konventsiya Soveta Evropy №108 «O zashchite lits v svyazi s avtomatizirovannoy obrabotkoy personal'nykh dannykh» ot 28 yanvarya 1981 goda [Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, January 28, 1981]. [in Russian].
3 Direktiva Evropeyskogo Parlamenta i Soveta ES 95/46/EC ot 24 oktyabrya 1995 goda o zashchite fizicheskikh lits pri obrabotke personal'nykh dannykh i o svobodnom obrashchenii takikh dannykh [Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data]. [in Russian].
4 Reglament (ES) 2016/679 Evropeyskogo Parlamenta i Soveta ot 27 aprelya 2016 goda o zashchite fizicheskikh lits v otnoshenii obrabotki personal'nykh dannykh i o svobodnom peremeshchenii takikh dannykh, a takzhe ob otmene Direktivy 95/46/ES (General Data Protection Regulation) [Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (GDPR)]. [in Russian].
5 Zakon Respubliki Kazakhstan «O personal'nykh dannykh i ikh zashchite» ot 21 maya 2013 goda № 94-V [Law of the Republic of Kazakhstan "On Personal Data and Their Protection" dated May 21, 2013 No. 94-V]. Informatsionno-pravovaya sistema normativnykh pravovykh aktov Respubliki Kazakhstan «Ədilet». [in Russian].
6 Zakon Respubliki Kazakhstan «Ob informatizatsii» ot 24 noyabrya 2015 goda № 418-V ZRK [Law of the Republic of Kazakhstan "On Informatization" dated November 24, 2015 No. 418-V ZRK]. Ibid. [in Russian].
7 Postanovlenie Pravitel'stva Respubliki Kazakhstan ot 12 noyabrya 2013 goda № 1214 «Ob utverzhdenii Pravil opredeleniya sobstvennikom i (ili) operatorom perechnya personal'nykh dannykh, neobkhodimogo i dostatochnogo dlya vypolneniya osushchestvlyaemykh imi zadach» [Resolution of the Government of the Republic of Kazakhstan No. 1214 dated November 12, 2013 "On Approval of the Rules for Defining the List of Personal Data Necessary and Sufficient to Fulfill Their Tasks by the Owner and/or Operator"]. Ibid. [in Russian].
8 Prikaz Ministra tsifrovogo razvitiya, innovatsiy i aerokosmicheskoy promyshlennosti Respubliki Kazakhstan ot 21 oktyabrya 2020 goda № 395/NQ «Ob utverzhdenii Pravil sbora i obrabotki personal'nykh dannykh» [Order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan No. 395/NQ dated October 21, 2020 "On Approval of the Rules for Collection and Processing of Personal Data"]. Ibid. [in Russian].
9 Google Spain v Agencia Española de Protección de Datos (AEPD) and González, Case C-131/12, 13 May 2014 // EUR-Lex. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131 [accessed: 09.09.2025].
10 Gusarova, A., Dzhaksylykov, S. (2020) Zashchita personal'nykh dannykh v Kazakhstane: status, riski i vozmozhnosti [Protection of Personal Data in Kazakhstan: Status, Risks, and Opportunities]. Almaty: Fond Soros-Kazakhstan, 56 p. Available at: https://www.soros.kz/wp-content/uploads/2020/04/Personal_data_report.pdf [in Russian].
11 Gusarova, A., Dzhaksylykov, S. (2021) Zashchita personal'nykh dannykh v Kazakhstane 2.0: Tsifrovoy sled Covid-19 [Protection of Personal Data in Kazakhstan 2.0: Digital Footprint of COVID-19]. Almaty: Fond Soros-Kazakhstan, 80 p. Available at: https://www.soros.kz/wp-content/uploads/2021/03/Personal-Data_Covid-Implications.pdf [in Russian].
12 Tashkaraev, Zh. Obzor sudebnoy praktiki po personal'nym dannym v Kazakhstane [Review of Judicial Practice on Personal Data in Kazakhstan]. Revera Kazakhstan. Available at: https://kazakhstan.revera.legal/info-centr/news-and-analytical-materials/229-obzor-sudebnoj-praktiki-po-personalnym-dannym-v-kazaxstane/ [accessed: 09.09.2025]. [in Russian].

О.Б. Дубовицкая[1]
[1]Торайғыров университеті, Қазақстан

Қазақстандағы дербес деректерге қатысты сот практикасына шолу

Қазақстанда «Дербес деректер және оларды қорғау туралы» Заңды қоса алғанда, дербес деректерді қорғауға арналған арнайы заңнама болғанына қарамастан, құқық қолдану тәжірибесі жеткіліксіз әрі жүйесіз болып отыр. Деректерді өңдеудің заңдылығына қатысты нақты өлшемдердің болмауы, субъектінің келісіміне қойылатын талаптардың әлсіз реттелуі, сондай-ақ халық пен бизнес өкілдерінің жеткіліксіз хабардар болуы азаматтардың құпиялық құқықтарының жаппай бұзылуына әкеп соғады. Атап айтқанда, деректерді шағын және орта бизнес субъектілері тарапынан өңдеу кезінде, сондай-ақ азаматтардың мемлекеттік және жекеменшік құрылымдармен өзара іс-қимылы барысында елеулі проблемалар туындайды.

Қазақстанда дербес деректерге қатысты құқықтық реттеу мен сот практикасының қазіргі жай-күйін талдау, заңнамалық нормалардың халықаралық стандарттарға, әсіресе GDPR-ға сәйкессіздігін, негізгі олқылықтарын анықтау және құқық қолдану тәжірибесін, сондай-ақ заңнаманы жетілдіру бағыттарын ұсыну.

Зерттеу барысында салыстырмалы-құқықтық, нормативтік-құқықтық, эмпирикалық (сот істерін талдау) және жүйелі тәсілдер қолданылды. Қазақстан ұлттық заңнамасы мен еуропалық заңнама (GDPR қоса алғанда) арасында салыстырмалы талдау жүргізілді, нақты тәжірибелік істерге баса назар аударылды.

Қазақстанда дербес деректер субъектісінің келісімі нысаны мен мазмұнына қойылатын нақты талаптардың жоқтығы, азаматтарды деректерді өңдеу мақсаттары мен тәсілдері туралы хабардар ету тетігінің қамтамасыз етілмегені анықталды. Деректерді минимизациялау, мақсатты шектеу және ашықтық қағидаттарына қатысты халықаралық стандарттармен елеулі алшақтықтар бар. Талдауға алынған сот істері деректер операторларының құқықтық мәдениетінің төмен деңгейін және уәкілетті органдардың бақылау функцияларын іске асыруда әлсіздігін көрсетті. Заңнаманы халықаралық нормаларға сәйкестендіру, бақылаушы органдардың институционалдық рөлін күшейту және дербес деректер субъектілерінің құқықтық санасын арттыру бойынша ұсыныстар берілді.

Түйінді сөздер: Дербес деректер, ақпаратты қорғау, сот практикасы, Қазақстан заңнамасы, GDPR.

O.B. Dubovitskaya[1]
[1]Toraygyrov University, Kazakhstan

Overview of Judicial Practice on Personal Data in Kazakhstan

Despite the existence of specialized legislation on the protection of personal data in Kazakhstan, including the Law "On Personal Data and Their Protection", law enforcement practice remains underdeveloped and inconsistent. The absence of clear criteria for the legality of data processing, weak regulation of consent requirements, and insufficient public and business awareness lead to widespread violations of privacy rights. Significant issues arise particularly in the processing of data by small and medium-sized businesses, as well as in the interaction of citizens with public and private entities.

To analyze the current state of legal regulation and judicial practice in Kazakhstan regarding personal data issues, to identify key gaps and inconsistencies between national legal norms and international standards, particularly the GDPR, and to propose directions for improving law enforcement practices and legislation.

The study uses comparative legal, normative legal, empirical (case law analysis), and systematic approaches. A comparative analysis of Kazakhstan's national legislation and European legislation (including the GDPR) is conducted, with a focus on practical cases.

It was found that there are no clear requirements in Kazakhstan regarding the form and content of data subject consent, and there is no effective mechanism to inform citizens about the purposes and methods of data processing. Significant discrepancies with international standards were identified, including in the principles of data minimization, purpose limitation, and transparency. The analyzed

court cases demonstrate a low level of legal awareness among data controllers and weak implementation of supervisory functions by the authorized bodies. Recommendations are proposed for bringing national legislation in line with international norms, strengthening the institutional role of regulatory authorities, and fostering legal awareness among data subjects.

Keywords: Personal data, information protection, judicial practice, Kazakhstani legislation, GDPR.

Дата поступления рукописи в редакцию: 10.09.2025 г.