

УДК 342.72/.73
МРНТИ 81.93.29

Е.Е. Ерболатов^{1*}, Г.М. Кубенов², С.К. Жетписов³, Г.А. Алибаева⁴, А.В. Борецкий⁵
^{1,2} Варненский Свободный Университет «Черноризец Храбър», Болгария
^{3,5} Инновационный Евразийский университет, Казахстан
⁴ Евразийская юридическая академия им. Д.А. Кунаева, Казахстан
(E-mail: ernarerbolatov@mail.ru)

Персональные данные в Республике Казахстан: проблемы обеспечения конфиденциальности в условиях цифровизации

Аннотация

В данной статье рассматриваются вопросы обеспечения конфиденциальности персональных данных личности в условиях развития информационного общества. Целью статьи является исследование проблем обеспечения конфиденциальности персональных данных в Республике Казахстан в условиях цифровизации экономики и общества. Методологическую основу настоящего исследования составляют общенаучные методы: философский, диалектический, синергетический, индуктивный, дедуктивный, метод анализа и синтеза, формализацию, аналогию, материалистический и эмпирический методы, позволяющие обеспечить целостность и сбалансированность исследования, а также формально-юридический метод, который позволил провести адекватный анализ содержания системы защиты персональных данных в зарубежных странах и Казахстане.

Процессы глобализации, информационной открытости и цифровизации поставили ряд задач, направленных на решение проблем обеспечения информационной безопасности с соблюдением баланса интересов личности, общества и государства. В этой связи проблемы обеспечения безопасности оборота персональных данных в сети Интернет являются актуальными для науки и правоприменительной практики. Ныне действующее законодательство Республики Казахстан о персональных данных уделяет недостаточное внимание вопросам обработки персональных данных в информационных системах. Совершенствование законодательства Республики Казахстан в сфере обеспечения безопасности обработки персональных данных в сети Интернет актуально в рамках реализации положений Концепции кибербезопасности («Киберщит Казахстана»).

Вместе с тем в национальном законодательстве нет конкретизированных гарантий от несанкционированного сбора персональных данных. Действующее законодательство Республики Казахстан в данной сфере отношений содержит ряд законодательных решений, однако имеются правовые погрешности, требующие своевременных корректив с учетом заимствования прогрессивного опыта зарубежных государств. Особое внимание в данной статье уделяется изучению современных угроз нарушения персональных данных и предусматриваются способы их защиты. Авторы приходят к выводу о том, что установленные Законом Республики Казахстан «О персональных данных и их защите» требования к порядку обеспечения конфиденциальности персональных данных носят общий характер и нуждаются в дальнейшей конкретизации. Кроме того, имеется целый ряд существенных аспектов, имеющих непосредственное отношение к обеспечению конфиденциальности персональных данных, которые до настоящего момента не получили своей должной правовой регламентации.

Ключевые слова: персональные данные, информационное общество, цифровизация, права личности, информационная безопасность.

Введение

Крупномасштабные преобразования, которые сегодня происходят практически во всех странах, обусловлены стремительным развитием информационно-коммуникационных технологий. Развитие информационных технологий ускоренными темпами приводит к появлению возможности у всех субъектов информационных отношений доступа и использования различных баз данных. Становление и развитие информационного общества – процесс достаточно сложный и противоречивый, который с безусловными положительными результатами привел к возникновению правовых, моральных, социальных и иных проблем и угроз. В этой связи данный этап движения современного общества к информационной открытости нуждается в осмыслении и понимании его последствий для дальнейшего развития.

В процессе формирования информационного общества постепенно модернизируются способы и методы распространения и обмена информацией, радикально меняется структура информационного пространства. Сегодня совершенствование методов автоматической обработки данных, формирование глобальных коммуникационных сетей, внедрение технологий электронного управления создают возможности сбора, обработки, компиляции и распространения информации с необычайной скоростью и невероятной точностью передачи. При таких условиях возникает серьезная угроза использования

персональных данных гражданами органами государственной власти и частными лицами вопреки интересам субъектов таких данных, а часто – и с целью нарушения их прав и законных интересов. Технические средства предоставляют широкие возможности для сбора, хранения и обработки существенных объемов социально значимых сведений в различных автоматизированных системах. Но именно эти системы, направленные на структурирование, хранение и поиск необходимой социально значимой информации, создали проблему утечки и иных форм незаконного доступа к персональным данным, что привело к необходимости обеспечения правовой защиты персональной информации.

Помимо создания законодательного механизма по обеспечению защиты персональных данных Республика Казахстан, как и многие современные государства, столкнувшись с данными вызовами, использует в нем и значительный спектр исполнительно-управленческих и организационно-технических мер. Несмотря на отсутствие в Казахстане практики работы с персональными данными и обеспечением их правовой защиты основу разработанного механизма защиты персональных данных составляют демократические ценности и идеи, заимствованные из богатого положительного опыта, накопленного европейскими государствами, а также современные тенденции развития права. Чрезвычайная актуальность изложенных проблем привела к необходимости научного анализа и осмысления возможностей правовой науки по обеспечению защиты конфиденциальности персональных данных.

Материалы и методы

Методологическая основа заключается в том, чтобы обеспечить целостность и сбалансированность исследования, используя общенаучные методы (в частности, философский, диалектический, синергетический, индуктивный, дедуктивный, метод анализа и синтеза, формализацию, аналогию, материалистический и эмпирический методы), а также формально-юридический для адекватного анализа содержания системы защиты персональных данных в зарубежных странах и Казахстане. С помощью системного и структурно-функционального методов были определены основные механизмы защиты персональных данных в зарубежных странах и Казахстане. Важное место в системе методов исследования занял также метод юридического анализа нормативно-правовых актов международных и европейских институтов с целью усовершенствования существующей системы защиты персональных данных в Республике Казахстан.

Авторами статьи проанализированы следующие источники: Конституция Республики Казахстан, международные правовые акты, конституционное, административное, гражданское, уголовное законодательство, подзаконные акты, а также иной юридический и технический материал стран СНГ и ЕС.

Зарубежные авторы уделяют особое внимание рассмотрению понятия различных видов конфиденциальной информации и персональных данных, а также подробно рассматривают вопросы их защиты от неправомерного использования третьими лицами, в частности, M. Bibent [1], D. Banisar [2], B. Weigner [3], K. Вугум [4].

Признавая важность вклада ученых в разработку вопросов правовой охраны конфиденциальности персональных данных, их юридических гарантий, необходимо отметить, что они требуют дополнительного изучения многогранной проблематики в условиях становления демократического гражданского общества и правового государства в соответствии с международно-правовыми актами защиты прав и свобод человека.

Результаты

Любой человек, будучи частью социума, не может быть единственным и безусловным обладателем информации о самом себе. Информация о человеке неизбежно циркулирует в обществе, объективно существуя как в виде документов, так и в сознании других людей, а оборот его часто осуществляется независимо от воли индивида. В то же время, очевидно, что индивид должен иметь право быть осведомленным о том, какая информация о нем накапливается в обществе, и иметь право влиять на процесс ее накопления. Особую остроту этой проблеме придает широкое применение средств компьютерной техники в сфере обработки информационных ресурсов.

В свете указанных факторов возникает объективная потребность в гармонизации интересов личности и государства – частных и публичных интересов в сфере оборота информации персонального характера.

Юридическая природа права на персональные данные обуславливает рассмотрение персональных данных с публично-правовых позиций, поскольку их использование связано, в первую очередь, с реализацией государственного интереса по сбору информации о гражданах. Можно привести множество сфер деятельности государства, где накапливаются, хранятся и используются персональные данные: здравоохранение, правосудие и деятельность правоохранительных органов, кредитно-финансовая сфера, средства массовой информации, образование, Интернет. С появлением современной торговли, банков, кредитования и страхования к государству присоединяются частные институты. Они также активно заинтересованы в информации о своих клиентах и потенциальных потребителях: от этого зависит их процветание и надежность заключенных ими договоров. В связи с этим регламентация данного процесса должна быть заложена в конституционных нормах.

Конкретизация данных конституционных норм содержится в Законе РК «О защите персональных данных и их защите», где в качестве одной из цели защиты персональных данных

называется реализация прав на неприкосновенность частной жизни, личную и семейную тайну [5]. Речь идет о персональных данных ограниченного доступа. Кроме того, все электронные информационные ресурсы в соответствии с Законом РК «Об информатизации» по степени доступа подразделяются на общедоступные и ограниченные (статья 32) [6]. Электронные информационные ресурсы, содержащие сведения, доступ к которым ограничен законами Республики Казахстан либо их собственником или владельцем, являются электронными информационными ресурсами ограниченного доступа. Они, в свою очередь, подразделяются на ресурсы, содержащие сведения, составляющие государственные секреты и конфиденциальные. Последние имеют ограниченный доступ, поскольку содержат персональную информацию конфиденциального характера, в том числе и персональные данные ограниченного доступа.

Таким образом, в соответствии с Конституцией Республики Казахстан и иными законодательными актами информация о частной жизни личности относится к информации, находящейся под правовой охраной. Соответственно, доступ к информации подобного характера без согласия лица, которому она принадлежит, запрещен. Иначе говоря, информация о частной жизни личности, включая и персональные данные, является конфиденциальной.

Конфиденциальность (от лат. *confidentia* – доверие) – необходимость предотвращения разглашения, утечки какой-либо информации. Конфиденциальная информация содержит не общеизвестные и нелегко доступные сведения в связи с ограничением к нему доступа лицом, фактически контролирующим такую информацию. Конфиденциальная информация – информация, являющаяся «доверительной, не подлежащей огласке, секретной»; это понятие равнозначно понятиям тайны или секрета [7, с. 559].

Появление категории «Конфиденциальная информация» – это логическое следствие ограничения доступа к информации, обусловленное необходимостью обеспечения баланса интересов личности, общества, государства. В правовой литературе и в законодательной практике встречаются и иные термины обеспечения режима конфиденциальности информации, это и различного рода «тайны» и «секреты».

Обсуждение

Конфиденциальную информацию о лице необходимо ограничивать от тайной информации. Однако, когда вопрос ставится именно таким образом, возникают дополнительные значительные трудности, связанные с наличием в законодательстве не только понятия тайной информации, но и различных правовых режимов «тайн», в названии которых есть термин «тайна» (банковская, врачебная, адвокатская и др.). Исследователи выделяют от 40 до 50 видов «тайн» [8, С. 157]. Все они различны по предмету правовой охраны, но, по мнению А.А. Фатьянова, имеют объединяющий признак. Таковым признаком является ущерб, который может наступить от распространения такой информации [9, С. 8].

На сегодня основное различие между конфиденциальной и тайной информацией о лице сводится к тому, что регулирование правового режима конфиденциальной информации базируется на принципе диспозитивности (лицо по своему желанию может установить такой режим для определенной информации или не делать этого), а ограничение доступа к тайной информации императивное, требуется законом. Следовательно, предоставление информации статуса конфиденциальной в конкретных случаях всегда является проявлением реализации права определенным субъектом информационных отношений, а при ограничении доступа к тайной информации – исполнением обязанности, предусмотренной соответствующим законом.

Конфиденциальными являются персональные данные, доступ к которым ограничен субъектом персональных данных, а тайными являются данные, на которые режим тайны распространяется в соответствии с требованиями законодательства (тайна состояния здоровья, тайна частной жизни, тайна усыновления и др.).

Законодательство Республики Казахстан содержит множество различных видов конфиденциальной информации (тайн), которые на сегодняшний день не систематизированы. Поэтому существует насущная проблема систематизации конфиденциальной информации путем выработки единого законодательного акта, в котором она будет классифицирована, и определении ее правового режима. На что уже обращали внимание казахстанские исследователи [10].

С проблемой обеспечения конфиденциальности персональных данных сегодня сталкивается любое общество. Эту проблему можно считать ключевой как с теоретической, так и практической позиции, требующей скорейшего решения.

Угрозы в области обеспечения персональных данных становятся актуальнее с повсеместным внедрением информационных технологий. В Республике Казахстан за последнее время произошел ряд резонансных случаев утечки персональных данных. Например, 9 июля 2019 года специалисты Центра анализа и расследований кибератак (ЦАРКА) обнаружили в сети одну из крупнейших утечек персональных данных. База с полной информацией 11 млн. человек (это всё совершеннолетнее население Республики Казахстан) находилась в общем доступе сети Интернет. Персональные данные сотен тысяч пациентов казахстанских медицинских организаций, подключенных к медицинской информационной системе «Data Med», попала в сеть. Сообщается, что виной утечки стала элементарная ошибка – неавторизованный доступ к медицинским документам организации. Данные 11 млн граждан Казахстана находились в открытом доступе в интернете. Любой желающий мог свободно получить доступ к системе

или полностью загрузить её к себе локально [11]. В 2018 году стало известно, что у нескольких казахстанских бухгалтерских сайтов, таких как *balans.kz*, *kodeks.kz*, *urist.kz*, были обнаружены признаки взлома. Хакерам удалось похитить около 10 тысяч бухгалтерских учетных данных. В 2017 году хакерами были взломаны сразу 20 сайтов государственных органов Казахстана, злоумышленникам с помощью вирусных программ удалось получить доступ к информационным системам трех казахстанских банков второго уровня [12].

По данным Аналитического центра компании «Info Watch», мировой объем утечек информации и скомпрометированных данных в 2017 году вырос в 4,2 раза по сравнению с 2016 годом – до 13,3 млрд записей. В 2018 году было зарегистрировано 2263 публичных случаев утечки конфиденциальной информации. В 86 % инцидентов были скомпрометированы персональные данные (ПДн) и платежная информация – всего около 7,3 млрд записей пользовательских данных против 13,3 млрд записей данных годом ранее [13].

Вышеприведенные показатели подтверждают особую значимость и необходимость обеспечения конфиденциальности персональных данных. Применение информационно-коммуникационных технологий, с одной стороны, значительно облегчает жизнь индивида, с другой – заставляет заботиться о необходимости защиты информации персонального характера.

Государство, развиваясь в эпоху открытого информационного пространства, стремится к цифровизации всех сфер общественной жизни. Создавая эффективные способы предоставления информации и оказания государственных услуг гражданам, государство минимизирует взаимодействие органов и человеком, используя возможности, предоставляемые информационными технологиями, мобильными технологиями и сетью Интернет.

С 2006 года в Казахстане функционирует портал Электронного правительства. Пользователям портала *egov.kz* предлагается 235 интерактивных и транзакционных услуг. Это самый масштабный проект Казахстана, содержащий огромное количество персональных данных практически всего населения. Вместе с тем, персональные данные на портале электронного правительства не всегда защищены должным образом.

Одна из резонансных историй, которая заставила многих задуматься о безопасности личных данных, случилась сравнительно недавно в г. Алматы. Некий сотрудник компании «Global Capital» (посредник для оказания консалтинговых услуг) без доверенности обратился в Центр обслуживания населения (ЦОН) Алмалинского района и получил адресную справку и документ о наличии (отсутствии) недвижимого имущества у гражданки А.Д. Ивановой (ФИО изменено) без ее ведома [14]. Нарушения подобного рода имеют место в Республике Казахстан. Причем, неприменение правовых мер по защите от таких ситуаций со стороны государства приводит к их учащению.

Некоторые эксперты говорят, что через сотрудников ЦОНов за отдельную плату можно получить информацию практически о любом гражданине. Неофициально ценники варьируются от 15 тысяч за незначительную справку до 100 тысяч тенге за более серьезные операции. Особенно часто к такой негласной помощи прибегают некоторые юристы, адвокаты, коллекторы и судебные исполнители [14].

Государственные органы и негосударственные организации Республики Казахстан также создают свои автоматизированные информационные системы. Например, на официальном сайте Верховного суда РК функционирует автоматизированная информационно-аналитическая система судебных органов Республики Казахстан. Внедрение данной автоматизированной системы (далее – ЕАИАС) способствует реализации принципов и задач судопроизводства (таких как гласность судебного разбирательства, обеспечение доступа участников процесса к материалам дела, содействие своевременному рассмотрению дел, снижение административных барьеров).

С 2012 года органами юстиции разрабатывается информационная система «Автоматизированная информационная система органов исполнительного производства» (АИС ОИП), реализующая электронный сервис по исполнительному производству для истца, должника, покупателя в онлайн-режиме.

В 2011 году начат проект внедрения информационной системы электронного обучения (e-Learning). В сельском хозяйстве эксплуатируются информационные системы: единая автоматизированная система управления отраслями агропромышленного комплекса «e-agriculture», система электронных торгов в аграрном секторе, система электронных зерновых расписок. Также осуществляется реализация проектов «e-минфин», «e-статистика», «e-лицензирование», «e-нотариат» и т.д.

Таким образом, развитие комплекса проектов электронного правительства – это объективно необходимое явление современной жизни, которое пользуется постоянно растущей популярностью среди пользователей и поддерживается со стороны государства. Однако ядром всех вышеперечисленных систем являются персональные данные индивида, зачастую конфиденциальные. Вполне закономерно возникает вопрос, каковы шансы сохранить в тайне информацию, составляющую персональные данные, которые не желательно разглашать.

Изложенное дает основание утверждать, что проблема обеспечения конфиденциальности персональных данных имеет двойственный характер. С одной стороны, персональные данные содержат

информацию о частной жизни личности и должны находиться в ограниченном доступе и под правовой охраной. С другой – персональные данные позволяют лицу реализовывать принадлежащие ему права и обязанности.

Двойственное значение персональных данных учел и казахстанский законодатель, закрепив в Законе их деление на общедоступные и ограниченные в доступе (ст. 6 Закона РК «О персональных данных и их защите»). Это позволяет учитывать двойственный характер правового обеспечения конфиденциальности персональных данных.

Поэтому при правовой регламентации оборота персональных данных возникают два основных направления, обеспечивающих особенности правового режима персональных данных. Во-первых, обеспечение защиты конфиденциальности персональных данных, при их сборе и обработке в информационных системах, когда личность взаимодействует с государственными органами и иными организациями в процессе жизнедеятельности. Во-вторых, обеспечение защиты конфиденциальности персональных данных при взаимодействии индивида со средствами массовой информации. Каждый индивид использует принадлежащие ему персональные данные, совершая действия, направленные на реализацию прав и обязанностей. Иначе говоря, личность вовлекается в общественные отношения, урегулированные правовыми нормами, путем предоставления персональных данных в правовой оборот. Таким образом, происходит накопление персональных данных. В накоплении персональных данных задействованы собственник базы, содержащей персональные данные и оператор базы, содержащей персональные данные.

Тщательная правовая регламентация механизма обеспечения конфиденциальности персональных данных, хоть и является необходимым условием их правового оборота, несет в себе определенные сложности. Процедура обеспечения конфиденциальности персональных данных характеризуется организационно-техническими и финансово-экономическими расходами. Данная ситуация создает сложности для некоторых операторов персональных данных, которые не всегда должным образом исполняют предписания норм законодательства в связи с чрезмерной урегулированностью.

На обеспечение конфиденциальности персональных данных могут влиять процессы интегрирования информационных систем различных субъектов. С одной стороны, интегрирование электронных информационных ресурсов преследует благую цель – быстрое и оперативное получение сведений, информационный обмен персональными данными для оперативности процессов проверки персональных данных, совершения иных действий. С другой стороны, в процессе интеграции порой могут не учитываться цели сбора персональных данных (сбор данных имел одну цель, при интеграции информационных ресурсов цель изменилась). Закон РК о персональных данных устанавливает, что использование персональных данных должно осуществляться собственником, оператором и третьим лицом только для ранее заявленных целей их сбора (статья 14). В противном случае персональные данные подлежат уничтожению.

В Казахстане была создана единая техническая платформа для интеграции информационных систем субъектов, участвующих в Государственной образовательной накопительной системе. Для этого были интегрированы информационные ресурсы следующих субъектов: Финансового центра Министерства образования и науки РК, Государственной базы данных физических лиц Министерства юстиции РК, Республиканского государственного предприятия «Государственный центр по выплате пенсий» посредством шлюза электронного правительства. Это позволило объединить базы данных для быстрого и оперативного получения сведений по гражданству вкладчиков образовательной накопительной системы, подтверждению приоритетных категорий вкладчиков, а также информационного обмена данными вкладчиками-участниками для оперативности процессов проверки персональных данных, открытия и закрытия вклада, формирования отчетности, безопасного обмена информацией [15].

Несомненно, данный процесс интеграции был направлен на улучшение положения вкладчиков накопительной образовательной системы. Однако возникает вопрос, насколько будут защищены персональные данные граждан, которые давали согласие на их сбор с другой целью.

Процесс обеспечения конфиденциальности персональных данных усложняет также вторичное использование персональных данных. Вторичное использование персональных данных, в первую очередь, касаются общедоступных данных, которые были первично распространены (с определенной целью), но в дальнейшем их используют абсолютно бесконтрольно.

В правовой литературе вторичное использование персональных данных получило название «Рутинное использование», которое было впервые применено в США. Оно представляет собой исключение из общих правил обеспечения режима конфиденциальности персональных данных и создает широкие возможности для обмена персональной информацией различными государственными ведомствами. Эта оговорка разрешает ведомству использовать персональные данные и раскрывать их для целей, совместимых (но не обязательно совпадающих) с той целью, для которой была собрана информация [16, С. 93].

Такой способ объединения и сверки баз с персональными данными был направлен на получение более полной информации о личности. К тому же она позволяла обнаружить злоупотребление со

стороны лиц, получающих пособия и услуги одновременно по нескольким программам социальной помощи. Например, в Казахстане государство, применив данную методику в 2019 году, выявило более 21 тысячи людей, незаконно получивших адресную социальную помощь [17]. Адресная социальная помощь в Казахстане назначается через информационную систему «Е-халык», которая интегрирована со многими нужными для формирования такой помощи базами государственных органов, где происходит обработка персональных данных всех членов семьи.

Однако в данном случае мы опять сталкиваемся с проблемой использования персональных данных, с не заявленной для первоначального сбора целью. Полагаем, данную ситуацию необходимо перевести в правовое поле и конкретизировать в законодательстве процедуру интегрирования информационных систем, с указанием цели, исчерпывающих оснований и точное перечисление сопоставляемых данных. Кроме того, следует уточнить, для чего будет использоваться вновь созданный информационный ресурс с персональными данными.

Вторичное использование персональных данных создает также проблему с незаконным распространением персональных данных, порой и конфиденциального характера. Как правило, вторичное использование происходит в результате незаконного приобретения базы с персональными данными, которые продаются недобросовестными операторами. В связи с развитием процедур создания баз данных клиентов крупными магазинами, банками, медицинскими, образовательными учреждениями возросли риски незаконной перепродажи или кражи персональных данных. Связано это, в первую очередь, с тем, что операторы не обеспечивают должную защиту информационных ресурсов с персональными данными, во-вторых, зачастую недобросовестные либо уволенные работники перепродают базы с данными клиентов другим компаниям.

В решении данного вопроса законодательство некоторых стран на постсоветском пространстве, в отличие от казахстанского законодательства, закрепляет нормы защиты. Например, статья 15 Закона Российской Федерации о персональных данных регулирует вопрос о защите прав субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации [18].

Для того, чтобы наладить контакт с потребителем продукции либо услуги через средства электронной связи, необходимо получить согласие субъекта персональных данных. В противном случае отсутствие согласия является нарушением законодательства, и контакт должен быть прекращен. Однако в настоящее время происходит массовая рассылка рекламной и иной корреспонденции без предварительного запроса согласия субъекта персональных данных. Это происходит в результате незаконной продажи клиентских электронных баз с персональной информацией.

Данную проблему следовало бы решить, предусмотрев законодательно норму, чтобы сторона, рассылающая подобную информацию, указывала источник получения персональных данных субъекта. В этом случае законодательно наложенный запрет на получение персональных данных незаконным способом получил бы реальную реализацию. Это позволило бы минимизировать навязчивый и бесконечный поток информации рекламного характера. В этой связи очень важно решить данную проблему правовыми средствами. В частности, законодательно урегулировать процедуру и порядок вторичного использования персональных данных с указанием условий, оснований, принципов, а также мер ответственности.

Проблемы человеческого фактора в механизме обеспечения конфиденциальности персональных данных играет немаловажную роль. Исследователи считают, что человеческий фактор должен учитываться и являться основным элементом построения эффективной системы защиты автоматизированных информационных систем [19, С. 42].

Полагаем, что данный аспект рассматриваемой проблемы обеспечения конфиденциальности персональных данных является чрезвычайно актуальным. В основе массовой утечки персональных данных в открытый доступ либо торговля персональными данными лица, а иногда и продажа клиентской базы данных компании совершаются, как правило, недобросовестными и безответственными сотрудниками, ущемленными в трудовых правах. Наряду с перечисленными характеристиками росту рисков способствуют низкая социально-экономическая защищенность сотрудников и отсутствие жестких мер реагирования подобных нарушений.

В числе причин несанкционированного использования персональных данных можно отнести пренебрежение безопасностью при использовании Интернет-ресурсов и социальных сетей со стороны сотрудников и их низкая правовая грамотность в вопросах информационной безопасности. Помимо этого, слабый уровень осведомленности в методах защиты персональных данных субъектов малого и среднего бизнеса, которые не придают серьезного значения обеспечению безопасности своих информационных ресурсов. Низкая заинтересованность работников, отсутствие профессионализма и норм этики создают предпосылки для занятия последних незаконными видами деятельности.

Имеющуюся проблему необходимо решать комплексно. Прежде всего, необходимо детализировать локальные нормативные акты, в которых регламентируется компетенция работников с персональными данными. А именно в трудовом договоре работника с персональными данными необходимо предусмотреть положения о соблюдении требований конфиденциальности, прохождении работником соответствующего инструктажа и обучения и т.д. Очень важно, чтобы сотрудник,

сталкивающийся в процессе работы с персональными данными, был письменно уведомлен о необходимости обеспечения конфиденциальности и правовой охраны персональных данных. В должностные инструкции такого сотрудника необходимо включить подробный порядок работы с конфиденциальными персональными данными. Иначе говоря, в локальных нормативных актах должен быть предусмотрен весь спектр особенностей работы с персональными данными, с конкретизированными мерами ответственности за несанкционированное их использование и распространение.

Анализ национального законодательства Республики Казахстан обнажает немаловажную сторону в механизме обеспечения конфиденциальности персональных данных, нуждающуюся в совершенствовании. Несмотря на то, что в Законе РК «О персональных данных и их защите» закреплено, что персональные данные ограниченного доступа являются конфиденциальными, порядок обеспечения конфиденциальности урегулирован поверхностно. В решении данного вопроса примечателен опыт зарубежных стран. Например, в законодательных актах о защите персональных данных ряда европейских стран, где подобные вопросы урегулированы законодательным актом. Принимая во внимание важность обеспечения защиты персональных данных, считаем целесообразным организационное и техническое регулирование осуществлять через закон. Подзаконные нормативные правовые акты слишком многочисленны, изменчивы и зачастую противоречивы. Кроме того, систематическая реорганизация органов исполнительной власти не самым лучшим образом сказывается на качественной стороне подзаконного нормотворчества.

Заключение

Таким образом, законодательство, определяющее деятельность правоохранительных органов, требует приведения его в соответствие демократическим принципам правового регулирования в этой сфере, прежде всего, путем выработки механизма недопущения существования в правоохранительных органах секретных баз персональных данных. Тайный характер обработки информации о лице в целях борьбы с преступностью входит в противоречие с принципом прозрачности, который является существенным для эффективной реализации права человека на защиту персональных данных. Не зная о сборе персональных данных, лицо не может защитить свои права. Следовательно, необходима выработка правового механизма, который позволит учесть интересы лица, чьи права ограничиваются. В частности, в международных актах по защите персональных данных говорится о контроле со стороны общественности (общества) через орган надзора за обработкой персональных данных, которая осуществляется правоохранительными органами. То есть не должно существовать тайных файлов или баз данных, которые неизвестны общественности. Все они должны быть легализованными и их использование должно регулироваться в законодательстве, доступном для общественности.

В целом, изложенное позволяет заключить, что Закон Республики Казахстан «О персональных данных и их защите», хоть и устанавливает требования к порядку обеспечения конфиденциальности персональных данных, носит общий характер и нуждается в конкретизации. Помимо этого, ряд важных аспектов, имеющих непосредственное отношение к обеспечению конфиденциальности персональных данных, не регламентирован.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Bibent M. Le Droit du Traitement de l'Information / M. Bibent. – Paris: ADBS, Nathan, 2000.
- 2 Banisar D. National Comprehensive Data Protection / Privacy Laws and Bills 2019 (August 1, 2019) / D. Banisar. Retrieved from <https://ssrn.com/abstract=1951416> or <http://dx.doi.org/10.2139/ssrn.1951416>.
- 3 Beignier B. Réflexions sur la protection de la vie privée / B. Beignier // Droit de la famille. – 1997. Retrieved from <http://publications.ut-capitole.fr/id/eprint/9648>.
- 4 Byrum K. The European right to be forgotten: A challenge to the United States Constitution's First Amendment and to professional public relations ethics / K. Byrum // Public Relations Review. – 2017. – Vol. 43. – No. 1. – P. 102-111.
- 5 Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 28.12.2017 г.). [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=31396226.
- 6 Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» (с изменениями и дополнениями по состоянию на 11.04.2019 г.). [Электронный ресурс] – Режим доступа: https://online.zakon.kz/document/?doc_id=33885902.
- 7 Большой юридический словарь / Под ред. А.Я. Сухарева. 3-е изд., перераб. и доп. – М.: ИНФРА-М, 2008. – 858 с.
- 8 Куликова С.А. Информационное право России. Учебное пособие. – Саратов: Изд-во Саратовского ун-та, 2010. – 194 с.
- 9 Фатьянов А.А. Тайна и право. – М.: МИФИ, 1999. – 288 с.
- 10 Жетписов С.К., Алибаева Г.А. Безопасность современного казахстанского общества и неприкосновенность частной жизни: определение баланса // Вестник КазНУ им. Аль-Фараби. Серия юридическая. – 2017. - № 1(81). - С. 78-85.

11 Оразбекова А. Произошла новая утечка персональных данных сотен тысяч казахстанцев // Информационный портал «Отырар». – 2019 [Электронный ресурс] – Режим доступа: <https://newtimes.kz/obshchestvo/93283-proizoshla-novaya-utechka-personalnykh-dannykh-soten-tysyach-kazakhstantsev>.

12 Данилин Н. Впервые в Казахстане создан прецедент: эксперт об утечке персональных данных бухгалтеров // Медиа портал «Караван». – 2019 [Электронный ресурс] – Режим доступа: <https://www.caravan.kz/news/vpervye-v-kazakhstane-sozdan-precedent-ehkspert-ob-utechke-personalnykh-dannykh-bukhgalterov-407641>.

13 В 2018 году мировой объем утечек пользовательских данных сократился в два раза – наибольшее снижение в хай-теке, банках и страховании // Аналитический центр компании «InfoWatch». – 2019 [Электронный ресурс] – Режим доступа: <https://www.infowatch.ru/company/presscenter/news/15465>.

14 Энелане Н. Насколько защищены персональные данные граждан в Казахстане? // Информационный портал «InformБюро». – 2017 [Электронный ресурс] – Режим доступа: <https://informburo.kz/stati/naskolko-zashchishcheny-personalnye-dannye-grazhdan-v-kazahstane.html>.

15 В РК образовательная накопительная система интегрирована с электронным правительством и банками // Международное информационное агентство «KazInform». – 2014 [Электронный ресурс] – Режим доступа: https://www.inform.kz/ru/v-rk-obrazovatel-naya-nakopitel-naya-sistema-integrirovana-s-elektronnym-pravitel-stvom-i-bankami_a2649505.

16 Петросян М.Е. Защита персональных данных: американская модель // США-Канада: экономика, политика, культура. – 2000. – № 6. С 92-107.

17 Алёхова А. Людей, смошенничавших при получении адресной помощи, наказывать не будет // Информационный портал «365info.kz». – 2019 [Электронный ресурс] – Режим доступа: <https://365info.kz/2019/09/lyudej-smoshennichavshih-pri-poluchenii-adresnoj-pomoshhi-nakazyvat-ne-budut>.

18 Федеральный закон «О персональных данных» от 27 июля 2006 № 152-ФЗ. [Электронный ресурс] – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801.

19 Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учеб.пособие. – М.: ИНФРА-М, 2001. – 304 с.

REFERENCES

- 1 Bibent, M. (2000). *Le Droit du Traitement de l'Information*. Paris. 2000 [In French].
- 2 Banisar, D. (2019). *National Comprehensive Data Protection / Privacy Laws and Bills 2019* (August 1, 2019). Retrieved from <https://ssrn.com/abstract=1951416> or <http://dx.doi.org/10.2139/ssrn.1951416>.
- 3 Beignier, B. (1997). *Réflexions sur la protection de la vie privée. Droit de la famille*. Retrieved from <http://publications.ut-capitole.fr/id/eprint/9648>. [In French].
- 4 Byrum, K. (2017). The European right to be forgotten: A challenge to the United States Constitution's First Amendment and to professional public relations ethics. *Public Relations Review*. Vol. 43, 1, 102–111.
- 5 Zakon Respubliki Kazahstan ot 21 maya 2013 goda № 94-V «O personal'nyh dannyh i ih zashchite» (s izmeneniyami i dopolneniyami po sostoyaniyu na 28.12.2017 g.) [Law of the Republic of Kazakhstan dated may 21, 2013 No. 94-V "On personal data and their protection" (with amendments and additions as of December 28, 2017)]. [online.zakon.kz](https://online.zakon.kz/Document/?doc_id=31396226). Retrieved from https://online.zakon.kz/Document/?doc_id=31396226.
- 6 Zakon Respubliki Kazahstan ot 24 noyabrya 2015 goda № 418-V «Ob informatizacii» (s izmeneniyami i dopolneniyami po sostoyaniyu na 11.04.2019 g.) [Law of the Republic of Kazakhstan dated November 24, 2015 No. 418-V "On Informatization" (with amendments and additions as of 11.04.2019)]. [online.zakon.kz](https://online.zakon.kz/Document/?doc_id=33885902). Retrieved from https://online.zakon.kz/Document/?doc_id=33885902.
- 7 Suharev, A.Y. (Eds.) (2008). *Bol'shoj yuridicheskij slovar'* [Large legal dictionary]. 3rd ed. Moscow: INFRA-M.
- 8 Kulikova, S.A. (2010). *Informacionnoe pravo Rossii* [Information law of Russia]. Textbook. Saratov.
- 9 Fatyanov, A.A. (1999). *Tajna i pravo* [The secret and law]. Moscow: MIFI.
- 10 Zhetpisov, S.K., & Alibaeva, G.A. (2017). Bezopasnost' sovremennogo kazahstanskogo obshchestva i neprikosnovennost' chastnoj zhizni: opredelenie balansa [The security of a modern Kazakhstan society and the inviolability of private life: finding the balance]. *Vestnik KazNU im. Al'-Farabi. Seriya yuridicheskaya - Bulletin Of al-Farabi Kazakh national University. A series of legal*. 1(81), 78-85.
- 11 Orazbekova, A. (2019). Proizoshla novaya utechka personal'nyh dannyh soten tysyach kazahstancev [There was a new leak of personal data of hundreds of thousands of Kazakhstanis]. There was a new leak of personal data of hundreds of thousands of Kazakhstanis // Information portal “Otyrar”. Retrieved from <https://otyrar.kz/2019/07/proizoshla-novaya-utechka-personalnyh-dannyh-soten-tysyach-kazahstantsev>.
- 12 Danilin, N. (2019). Vpervye v Kazahstane sozdan precedent: ekspert ob utechke personal'nyh dannyh buhgalterov [For the first time in Kazakhstan, a precedent has been set: an expert on the leakage of personal data of accountants]. Media portal “Karavan”. Retrieved from <https://www.caravan.kz/news/vpervye-v-kazakhstane-sozdan-precedent-ehkspert-ob-utechke-personalnykh-dannykh-bukhgalterov-407641>.
- 13 “InfoWatch”. (2019). V 2018 godu mirovoj ob'em utechek pol'zovatel'skih dannyh sokratilsya v dva raza - naibol'shee snizhenie v haj-teke, bankah i strahovanii [In 2018, the global volume of user data leaks

decreased by half - the Largest decrease in high-tech, banking and insurance. Analytical center of the company "InfoWatch" // Retrieved from <https://www.infowatch.ru/company/presscenter/news/15465>.

14 Enelane, N. (2017). Naskol'ko zashchishcheny personal'nye dannye grazhdan v Kazahstane? [How protected are personal data of citizens in Kazakhstan?]. Information portal "Politburo". Retrieved from <https://informburo.kz/stati/naskolko-zashchishcheny-personalnye-dannye-grazhdan-v-kazahstane.html>.

15 "KazInform". (2014). V RK obrazovatel'naya nakopitel'naya sistema integrirovana s elektronnyim pravitel'stvom i bankami [In the Republic of Kazakhstan, the educational accumulative system is integrated with e-government and banks]. International news Agency "KazInform". Retrieved from https://www.inform.kz/ru/v-rk-obrazovatel-naya-nakopitel-naya-sistema-integrirovana-s-elektronnym-pravitel-stvom-i-bankami_a2649505.

16 Petrosyan, M.E. (2000). Zashchita personal'nyh dannyh: amerikanskaya model' [Personal data protection: the American model. SShA - Kanada: ekonomika, politika, kul'tura - USA - Canada: economy, politics, culture. 6, 92-107.

17 Alyohova, A. (2019). Lyudej, smoshennichavshih pri poluchenii adresnoj pomoshchi, nakazyvat' ne budut [People who cheated when receiving targeted assistance will not be punished]. Information portal "365info.kz". Retrieved from <https://365info.kz/2019/09/lyudej-smoshennichavshih-pri-poluchenii-adresnoj-pomoshhi-nakazyvat-ne-budut>.

18 Federal'nyj zakon «O personal'nyh dannyh» ot 27 iyulya 2006 № 152-FZ [Federal law No. 152-FZ of July 27, 2006 "On personal data".]. www.consultant.ru. Retrieved from http://www.consultant.ru/document/cons_doc_LAW_61801.

19 Stepanov, E.A., & Korneev, I.K. (2001). Informacionnaya bezopasnost' i zashchita informacii [Information security and information protection]. Textbook. Moscow: INFRA-M.

Е.Е. Ерболатов^{1*}, Г.М. Кубенов², С.К. Жетписов³, Г.А. Алибаева⁴, А.В. Борецкий⁵

^{1,2} Варна Еркін Университеті «Черноризец Храбър», Болгария

^{3,5} Инновациялық Еуразия университеті, Қазақстан

⁴ Д.А. Қонаев атындағы Еуразиялық заң академиясы, Қазақстан

(E-mail: ernarerbolatov@mail.ru)

Қазақстан Республикасындағы дербес деректер: цифрландыру жағдайында құпиялылықты қамтамасыз ету мәселелері

Бұл мақалада ақпараттық қоғамның дамуы жағдайында жеке тұлғаның жеке деректері құпиялылығын қамтамасыз ету мәселелері қарастырылады. Мақаланың мақсаты - экономика мен қоғамды цифрландыру жағдайында Қазақстан Республикасында жеке деректердің құпиялылығын қамтамасыз ету мәселелерін зерттеу. Осы зерттеудің әдіснамалық негізін жалпы ғылыми әдістер құрайды: философиялық, диалектикалық, синергетикалық, индуктивті, дедуктивті, талдау және синтез әдісі, формализация, ұқсастық, зерттеудің тұтастығы мен тепе-теңдігін қамтамасыз етуге мүмкіндік беретін материалистік және эмпирикалық әдістер, сондай-ақ шет елдерде және Қазақстанда дербес деректерді қорғау жүйесінің мазмұнына барабар талдау жүргізуге мүмкіндік берген формальды-заңдық әдіс.

Жаһандану, ақпараттық ашықтық және цифрландыру процестері жеке адам, қоғам және мемлекет мүдделерінің теңгерімін сақтай отырып, ақпараттық қауіпсіздікті қамтамасыз ету проблемаларын шешуге бағытталған бірқатар міндеттер қойды. Осыған байланысты Интернет желісіндегі Дербес деректер айналымының қауіпсіздігін қамтамасыз ету проблемалары бүгінгі күні ғылым мен құқық қолдану тәжірибесі үшін өзекті болып табылады. Қазақстан Республикасының Дербес деректер туралы қолданыстағы заңнамасы ақпараттық жүйелерде дербес деректерді өңдеуге қатысты мәселелерге жеткілікті назар аудармайды. Интернет желісінде дербес деректерді өңдеу қауіпсіздігін қамтамасыз ету саласындағы Қазақстан Республикасының заңнамасын жетілдіру киберқауіпсіздік тұжырымдамасының («Қазақстанның Киберқалқаны») ережелерін іске асыру шеңберінде өзекті болып отыр.

Сонымен қатар, ұлттық заңнамада дербес деректерді рұқсатсыз жинаудан нақты кепілдіктер жоқ. Қазақстан Республикасының осы қатынастар саласындағы қолданыстағы заңнамасында бірқатар заңнамалық шешімдер бар, алайда шет мемлекеттердің озық тәжірибесін пайдалануды ескере отырып, уақтылы түзетулерді талап ететін құқықтық қателіктер бар. Бұл мақалада жеке деректерді бұзудың заманауи қауіптерін зерттеуге ерекше назар аударылады және оларды қорғау әдістері қарастырылған. Авторлар «Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының Заңында дербес деректердің құпиялылығын қамтамасыз ету тәртібіне қойылатын талаптар белгіленгеніне қарамастан, олар жалпы сипатқа ие және одан әрі нақтылауды қажет етеді деген қорытындыға келеді. Бұдан басқа, осы уақытқа дейін тиісті құқықтық регламенттеуді алмаған дербес деректердің құпиялылығын қамтамасыз етуге тікелей қатысы бар бірқатар елеулі аспектілер бар.

Түйін сөздер: жеке деректер, ақпараттық қоғам, цифрландыру, жеке құқықтар, ақпараттық қауіпсіздік.

E.E. Yerbolatov^{1*}, G.M. Kubenov², S.K. Zhetpisov³, G.A. Alibaeva⁴, A.V. Boretskiy⁵

^{1,2}Varna Free University «Chernorizets Hrabar», Bulgaria

^{3,5}Innovative University of Eurasia, Kazakhstan

⁴Eurasian Law Academy named after D.A.Kunayev, Kazakhstan

(E-mail: ernarerbolatov@mail.ru)

**Personal data in the Republic of Kazakhstan:
problems of ensuring confidentiality in the context of digitalization**

This article discusses the issues of ensuring the confidentiality of personal data in the context of the development of the information society. The purpose of the article is to study the problems of ensuring the confidentiality of personal data in the Republic of Kazakhstan in the conditions of digitalization of the economy and society. The methodological basis of this research is based on General scientific methods: philosophical, dialectical, synergetic, inductive, deductive, method of analysis and synthesis, formalization, analogy, materialistic and empirical methods that ensure the integrity and balance of research, as well as a formal legal method that allowed an adequate analysis of the content of the personal data protection system in foreign countries and Kazakhstan.

The processes of globalization, information openness and digitalization have set a number of tasks aimed at solving the problems of ensuring information security while maintaining a balance of interests of the individual, society and the state. In this regard, the problems of ensuring the security of personal data turnover on the Internet, today, is relevant for science and law enforcement practice. The current legislation of the Republic of Kazakhstan on personal data does not pay enough attention to issues related to the processing of personal data in information systems. Improving the legislation of the Republic of Kazakhstan in the field of ensuring the security of personal data processing on the Internet is relevant in the framework of implementing the provisions of the Cybersecurity concept («Cyber shield of Kazakhstan»).

However, national legislation does not provide specific guarantees against unauthorized collection of personal data. The current legislation of the Republic of Kazakhstan in this sphere of relations contains a number of legislative decisions, but there are legal errors that require timely adjustments, taking into account the borrowing of progressive experience of foreign countries. Special attention in this article is on the study of contemporary threats of violations of personal data, and provided ways to protect them. The authors conclude that, despite the fact that the law of the Republic of Kazakhstan «On personal data and their protection» sets requirements for the procedure for ensuring the confidentiality of personal data, at the same time they are general in nature and need further specification. In addition, there are a number of significant aspects that are directly related to ensuring the confidentiality of personal data, which have not yet received their proper legal regulation.

Keywords: personal data, information society, digitalization, personal rights, information security.

Дата поступления рукописи в редакцию: 04.09.2020 г.