УДК 340.13:004.056.5
DOI: 10.36979/1694-500X-2023-23-7-96-101

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ И ФОРМИРОВАНИЯ СИСТЕМ ОБЩИХ И СПЕЦИАЛЬНЫХ МЕР

Н.А. Сейдакматов, К.С. Омельченко

Аннотация. Раскрываются особенности и проблемы правового регулирования и формирования системы защиты персональных данных в Кыргызской Республике. В работе рассматриваются вопросы наличия законодательных мер в области защиты персональных данных, а также мероприятий по техническому регулированию деятельности по сбору, хранению и обработке персональных данных. Поднимаются вопросы проблемных частей в правоприменительной практике ввиду отсутствия необходимых норм права, в том числе в вопросах обеспечения государственного контроля за соблюдением законодательства Кыргызской Республики в области информации персонального характера.

Ключевые слова: проблемы правового регулирования; персональные данные; хранение; обработка; обеспечение государственного контроля.

МААЛЫМАТТЫК КООПСУЗДУКТУ КАМСЫЗ КЫЛУУ: УКУКТУК ЖӨНГӨ САЛУУ, ЖАЛПЫ ЖАНА АТАЙЫН ЧАРАЛАР СИСТЕМАСЫН ТҮЗҮҮ МАСЕЛЕСИ

Н.А. Сейдакматов, К.С. Омельченко

Аннотация. Макалада Кыргыз Республикасындагы жеке маалыматтарды коргоо системасын укуктук жөнгө салуунун жана калыптандыруунун өзгөчөлүктөрү жана көйгөйлөрү аныкталган. Эмгекте жеке маалыматтарды коргоо жаатындагы мыйзамдык чаралардын болушу, ошондой эле жеке маалыматтарды чогултуу, сактоо жана иштетүү боюнча ишти техникалык жөнгө салуу боюнча иш-чаралардын маселелери каралат. Укук колдонуу практикасында, анын ичинде жеке мүнөздөгү маалыматтар жаатында Кыргыз Республикасынын мыйзамдарынын сакталышына мамлекеттик контролду камсыз кылуу маселелеринде зарыл болгон укуктук ченемдеринин жоктугунан, көйгөйлүү бөлүктөрдүн маселелери көтөрүлөт.

Түйүндүү сөздөр: укуктук жөнгө салуу көйгөйлөрү; жеке маалыматтар; сактоо; иштетүү; мамлекеттик көзөмөлдү камсыз кылуу.

ENSURING INFORMATION SECURITY: PROBLEMS OF LEGAL REGULATION AND FORMATION OF SYSTEMS OF GENERAL AND SPECIAL MEASURES

N.A. Seidakmatov, K.S. Omelchenko

Abstract. The article reveals the features and problems of legal regulation and the formation of a personal data protection system in the Kyrgyz Republic. The paper discusses the existence of legislative measures in the field of personal data protection, as well as measures for the technical regulation of activities for the collection, storage and processing of personal data. The article raises issues of problematic parts in law enforcement practice due to the lack of necessary rules of law, including in matters of ensuring state control over compliance with the legislation of the Kyrgyz Republic in the field of personal information.

Keywords: problems of legal regulation; personal data; storage; processing; provision of state control.

Законодательство Кыргызской Республики в сфере персональных данных состоит из статей 29 и 63 Конституции Кыргызской Республики, где закреплено право каждого человека на неприкосновенность частной жизни, защиту чести и достоинства. Одновременно не

допус-кается сбор, хранение, использование и расп-ространение конфиденциальной информации, информации о частной жизни человека без его согласия, кроме случаев, установленных законом. Каждому гарантируется защита, в том числе судебная, от неправомерного сбора, хранения, распространения конфиденциальной информации и информации о частной жизни человека. Конституция гарантирует право на возмещение материального и морального вреда, причиненного неправомерными действиями, а также защиту персональных данных каждого гражданина.

Несмотря на принятие в 2008 году Закона Кыргызской Республики «Об информации персонального характера» (далее – Закон), до 2021 года отсутствовал эффективный механизм защиты персональных данных и прав субъектов персональных данных. В ходе совершенствования ключевых законов по цифровизации – Закона Кыргызской Республики «Об электронном управлении» и Закона Кыргызской Республики «Об электронной подписи» – должное внимание вопросам защиты информации персонального характера не уделялось, что в итоге создало дополнительные риски, особенно учитывая внедряемые процессы цифровой трансформации.

Закон Кыргызской Республики «Об информации персонального характера» направлен на правовое регулирование работы с персональными данными на основе общепринятых международных принципов, в целях обеспечения защиты прав и свобод человека и гражданина, связанных со сбором, обработкой и использованием персональных данных.

Основной проблемой института защиты прав субъектов персональных данных является то, что до настоящего момента отсутствовали практики единого правоприменительного подхода. В итоге, за 14 лет с момента принятия отраслевого Закона правоприменительная практика локализовалась и институционализировалась с различными особенностями среди наиболее крупных держателей персональных данных в Кыргызской Республике.

Среди наиболее крупных держателей массивов персональных данных можно выделить несколько основных акторов, в том числе по отраслям: среди государственных держателей персональных данных, к примеру, это Министерство цифрового развития Кыргызской Респуб-лики, поскольку оно является уполномоченным государственным органом в области регистрации населения [1], Государственная налоговая служба и Социальный фонд Кыргызской Республики. В частном секторе наиболее крупными держателями массивов персональных данных являются финансово-кредитные учреждения и сотовые операторы.

Еще на этапах внедрения электронного управления существовали трудности, заключавшиеся в нежелании крупных государственных держателей массивов персональных данных взаимодействовать с частным сектором по вопросам обмена персональными данными. Такая ситуация сложилась ввиду отсутствия методологии и правоприменительной практики в вопросах обмена персональными данными в интересах их субъектов, что в значительной мере усложнило и продолжает влиять на внедрение процессов электронного управления и развитие института защиты персональных данных в целом.

Согласно статье 19 Закона, на уполномоченный орган возлагаются функции по осуществлению роли контрольно-надзорного органа в сфере защиты персональных данных.

С целью решения вышеуказанных задач, постановлением Кабинета Министров Кыргызской Республики «О Государственном агентстве по защите персональных данных при Кабинете Министров Кыргызской Республики» от 22 декабря 2021 года № 325 создано Государственное агентство по защите персональных данных при Кабинете Министров Кыргызской Республики. В Положении этого Агентства помимо контрольно-надзорных функций были заложены также координационно-регуляторные функции, в том числе возможность проведения своеобразного арбитража по спорным вопросам, возникающим в ходе обмена персональными данными между участниками электронного взаимодействия, а также разработка технической и методической документации наравне с проведением просветительской работы. Все эти мероприятия в совокупности применения должны оказать позитивный сдвиг к полноценному запуску института защиты персональных данных с едиными систематизированными подходами, основанными на нормативных правовых актах, выработанных

методологических подходах и правоприменительных практиках.

На начальных этапах своего становления Агентство приступило к разработке отсутствующих нормативных правовых актов в области защиты персональных данных, которые должны были быть реализованы во исполнение отраслевого Закона.

Необходимо также отметить, что изначально полноценное применение норм Закона Кыргызской Республики «Об информации персонального характера» было затруднено из-за неисполнения постановления Правительства Кыргызской Республики «Об утверждении Требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных» от 21 ноября 2017 года № 760 (далее – Требования к обеспечению безопасности). Так, еще в 2017 году должны были быть разработаны документы, обеспечивающие защиту персональных данных, собираемых держателями массивов персональных данных. В частности, с 2017 года не были разработаны следующие документы:

1. Типовой перечень угроз безопасности персональных данных при обработке персональных данных в информационных системах;
2. Методика определения угроз безопасности в информационных системах персональных данных;
3. Форма перечня видов угроз [2].

Отсутствие перечисленных документов блокирует реализацию Требований к обеспечению безопасности, что, в свою очередь, влияет на эффективность реализации законодательства, а также выстраивание надежной системы защиты персональных данных.

Незамедлительная разработка и внедрение документов, вытекающих из Требований к обеспечению безопасности, является краеугольным камнем не только для полноценного правового реанимирования и запуска системы защиты персональных данных, но и дает организационно-технические меры защиты персональных данных, реализуемые держателями персональных данных. Кроме того, соблюдение Требований к обеспечению безопасности и контроль их соблюдения является лакмусовой бумажкой в оценке уровня защищенности информационных систем персональных данных.

Из-за длительного отсутствия нормативных правовых актов в части процедуры и порядка регистрации в реестре до недавнего времени частный сектор в настоящее время еще не приступил к регистрации своих массивов, что также влияет на транспарентность процессов, имеющихся в области сбора, обработки и хранения персональных данных. Так, в соответствии с Порядком регистрации держателей (обладателей) массивов персональных данных в Реестре держателей (обладателей) массивов персональных данных, утвержденным постановлением Кабинета Министров Кыргызской Республики от 18 ноября 2022 года № 638, держателям массивов персональных данных отводится шестимесячный срок для прохождения учетной регистрации.

Поскольку существенным юридическим основанием для сбора и обработки персональных данных, в соответствии с частью 2 статьи 6 Закона Кыргызской Республики «Об информации персонального характера», является именно регистрация в Реестре держателей, а при ее отсутствии сбор, хранение и обработка персональных данных не допускаются, то в настоящее время установился проблемный правоприменительный аспект, который заключается в том, что те держатели, которые не зарегистрированы в реестре держателей массивов персональных данных, не могут считаться держателями и, следовательно, могут аппелировать к тому факту, что не обладают деликтоспособностью как держатель персональных данных. Принятое положение о порядке регистрации в Реестре в значительной мере урегулировало этот вопрос, который «висел в воздухе» с момента принятия отраслевого Закона.

За 14 лет, которые прошли со времени принятия Закона, произошли глобальные технологические изменения. Внедряются новые информационные и коммуникационные технологии. Изменился не только подход к сбору личной информации, но и отношение общества к этой проблематике. В связи с этим назрела необходимость зафиксировать современный уровень развития информационных и иных технологий, дать ответ на актуальные вызовы и угрозы, обусловленные постоянно расширяющимися

возможностями обработки и трансграничной передачи данных личного характера. Отдельным проблемным вопросом является то, что до настоящего момента отсутствует соответствующий механизм административного воздействия на лица, нарушающие положения действующего законодательства.

Одним из методов обеспечения неукоснительного соблюдения правовых норм сторонами правоотношений, связанных с обработкой персональных данных, является наличие юридической ответственности за нарушение норм права. В условиях отсутствия юридических оснований для привлечения к ответственности лиц, виновных в нарушении законов, органы государственной власти не могут обеспечить режим законности – важную составляющую правового государства, которая предполагает гарантии выполнения содержащихся в нормах права предписаний. Именно законодательное установление процедуры обеспечения законности будет восприниматься гражданами как гарантированное закрепление их реальных возможностей, обеспечиваемых государством.

Еще в 2016 году Международный деловой совет выпустил статью относительно защиты персональных данных в Кыргызской Республики, в которой было отмечено, что для полноценного развития института защиты персональных данных должны быть разработаны нормативы по порядку организации и проведения государственного контроля над соответствием сбора, обработки, хранения и защиты персональных данных, по предупреждению и выявлению нарушений, а также система санкций за нарушение законодательства в сфере защиты персональных данных. В свою очередь, уполномоченный орган должен установить доступную для общества процедуру обжалования неправомерных действий субъектов ПД, а также систему санкций за нарушение установленных требований [3].

Меры ответственности за правонарушения и преступления с персональными данными, закрепленные в законодательстве, носят общий характер, что затрудняет вопросы их применения в процессе квалификации преступлений и правонарушений на предмет наличия признаков состава таковых, а также степени общественной опасности (необходимы дополнения в кодексы – о правонарушениях, а в последующем – и в уголовный). Определяющими факторами при этом должны стать вопросы не столько наказаний за допущенные нарушения, сколько восстановления нарушенных прав субъектов и восстановление причиненного им незаконными действиями вреда в досудебном порядке.

Данные меры могут быть реализованы посредством секвестирования налагаемых штрафных санкций, где часть из этих средств будет направлена субъекту персональных данных, а другая – в пользу бюджета, это позволит стимулировать и создать соответствующие предпосылки для активного наращивания института защиты персональных данных. Другим вариантом реализации восстановления нарушенных прав субъектов и восстановление причиненного вреда может быть внедрение независимого арбитража и включение элементов из системы медиации.

Данные меры направлены на решение нескольких вопросов. Во-первых, снижается нагрузка на судебную систему Кыргызской Республики. Во-вторых, происходит стимулирование гражданского общества на защиту своих прав, что, в свою очередь, будет способствовать развитию института защиты персональных данных. В-третьих, реализация данной меры позволит привлечь в систему защиты персональных данных не только гражданский сектор, но и частный, который будет заинтересован в формировании надежной системы защиты персональных данным. При этом, некоторые участники рынка будут заинтересованы оказывать медиационные и иные услуги, связанные с защитой персональных данных, в случаях, если будет закреплена возможность получения прибыли в процессе восстановления нарушенных прав субъектов персональных данных.

В целом, мировая практика показывает, что для правильного функционирования системы защиты персональных данных функции и полномочия уполномоченного государственного органа должны соответствовать стандартам самостоятельности, независимости, компетенциям, задачам и полномочиям надзорных органов в этой сфере, согласно общепринятым международным стандартам, которые являются существенным и необходимым компонентом защиты физических лиц в отношении обработки их персональных данных.

Подчеркнем, что независимость и самостоятельность института уполномоченного органа по защите персональных данных является одним из краеугольных камней в вопросе создания эффективной системы защиты персональных данных и прав их держателей в республике.

В настоящее время следует признать, что уполномоченный государственный орган по персональным данным в той или иной мере не имеет необходимого объема самостоятельности. Отсутствие полномочий и в определенной степени ограниченная независимость Агентства в том числе продиктована и незначительным кадровым потенциалом. Например, в Грузии с населением в 3,8 млн человек в уполномоченном государственном органе работает свыше 60 человек. На фоне практического расширения сферы применения функций Агентства, учитывая методы цифровой слежки по данным о геолокации, обработки цифрового фото- и видеоизображения, передачу телеметрических данных о состоянии здоровья по каналам связи, перевод государственных услуг в цифровой формат с требованием однозначной идентификации / подтверждения личности с получением и хранением персональных данных, включая биометрические, в цифровой среде, имеется острая необходимость проводить работу по увеличению кадрового потенциала Агентства ввиду того, что на всех держателей массивов персональных данных, количество которых приблизительно равняется количеству юридических лиц, приходится только 11 человек, а также продолжать работу, в том числе на законодательном уровне по приданию ему большей независимости и самостоятельности.

Именно достаточная степень независимости основного регулятора является одним из основных показателей результативности всего института права и последующего поступательного развития основополагающих прав человека. В этом смысле интересен международный опыт по созданию и функционированию подобных агентств за рубежом.

Например, в Грузии руководитель уполномоченного государственного органа по защите персональных данных избирается парламентом сроком на шесть лет [4]. Во Франции уполномоченный орган, созданный в 1978 году, в соответствии с Законом о защите данных является независимым административным органом, состоящим из Коллегии из 18 членов и группы государственных служащих, работающих по контракту. При этом 12 из 18 членов избираются судами или местными органами власти, к которым они относятся. Другими словами, структура французского регулятора выглядит следующим образом:

- четыре парламентария (два депутата, два сенатора);
- два члена Экономического, Социального и Экологического Совета;
- шестеро представителей высших судов (два статских советника, два советника Кассационного суда, 2 советника Счетной палаты);
- пять квалифицированных лиц, назначаемых Председателем Национального собрания (один человек), Председателем Сената (один человек) и в Совет министров (три человека).

Срок полномочий уполномоченных составляет пять лет или, в случае членов парламента, срок, равный их выборному сроку полномочий [5].

В Беларуси руководитель национального регулятора находится в прямом ведении президента, назначается и снимается с должности по решению президента.

В целом, имеется большое количество появившихся проблемных вопросов ввиду устаревания основного законодательства, которое принималось в эпоху аналогового права и в значительной степени не предусматривало наличие цифровых правоотношений и норм. Это, в свою очередь, к настоящему времени создает определенные затруднения, в том числе следующие:

- при получении согласия субъекта персональных данных в соответствии с постановлением Правительства Кыргызской Республики «Об утверждении Порядка получения согласия субъекта персональных данных на сбор и обработку его персональных данных, порядка и формы уведомления субъектов персональных данных о передаче их персональных данных третьей стороне» от 21 ноября 2017 года № 759 до сих пор требуется получение письменного согласия или в виде электронного документа, подписанного электронной подписью, что создает трудности

в правоприменительной практике, а также значительно сокращает возможности оказания электронных услуг ввиду несущественного количества пользователей с электронными подписями;

- отсутствует закрепленное требование по публикации политик и правил по обработке персональных данных субъектов, то есть, в соответствии с постановлением Правительства Кыргызской Республики «Об утверждении Требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных» от 21 ноября 2017 года № 760, вышеуказанные документы должны быть доведены до контрагентов только при наличии договорных отношений, что также снижает возможности по защите прав, в случаях, когда осуществляется обработка персональных данных без заключения договоров, в том числе в сети Интернет;
- требованиями пункта 12 Порядка получения согласия субъекта персональных данных на сбор и обработку его персональных данных порядок и форма уведомления субъектов персональных данных о передаче их персональных данных третьей стороне, утвержденного постановлением Правительства Кыргызской Рес-публики от 21 ноября 2017 года № 759, предусматривается обязанность в недельный срок с момента передачи персональных данных информировать субъекта персональных данных об осуществленной передаче его персональных данных третьей стороне, однако данная мера не реализована и не действует.

Одновременно с совершенствованием законодательства в сфере защиты персональных данных, необходимо обратить особое внимание на придание необходимых надзорных полномочий уполномоченному государственному органу по персональным данным, что является одной из ключевых задач для пресечения нарушений.

Все эти вопросы в настоящее время находятся в разработке у Агентства. В ближайшее время планируется проведение мероприятий по существенной модернизации законодательства в области защиты персональных данных, что позволит заложить условия для укрепления аспектов информационной безопасности, повысить качество защиты персональных данных субъектов и обеспечить единообразный подход в вопросах организации сбора, хранения и обработки персональных данных. Только в период с апреля по ноябрь 2022 года на законодательном уровне (разработка отраслевой политики) в сфере защиты персональных данных Агентством разработаны 14 НПА и локальных актов.

Таким образом, работа по направлениям формирования систем общих и специальных мер началась спустя 14 лет после принятия отраслевого Закона с параллельной работой по его модернизации и созданию условий для трансформационных изменений, происходящих в экономике Кыргызской Республики.

Поступила: 01.12.23; рецензирована: 15.12.23;
принята: 19.12.23.

Литература

1. Положение о Министерстве цифрового развития Кыргызской Республики, утвержденное постановлением Кабинета Министров Кыргызской Республики от 15 ноября 2017 года № 257. URL: http://cbd.minjust.gov.kg/act/view/ru-ru/158713 (дата обращения: 23.11.2022).
2. Постановление Правительства Кыргызской Республики «Об утверждении Требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных» от 21 ноября 2017 года № 760. URL: http://cbd.minjust.gov.kg/act/view/ru-ru/11512 (дата обращения: 22.11.2022).
3. Международный деловой совет: Защита персональных данных в Кыргызской Республике. URL: http://www.ibc.kg/ru/analysis/articles/2112_zaschita_personalnyh_dannyh_v_kyrgyzskoi_respublike (дата обращения: 23.11.2022).
4. The Personal Data Protection Service of Georgia. URL: https://www.personaldata.ge/en/about-us (дата обращения: 22.11.2022).
5. CNIL. Commission Nationale de Informatigue et des Libertes. URL: https://www.cnil.fr/en/node/287 (дата обращения: 22.11.2022).