THE LEGAL MECHANISM FOR THE PROTECTION OF PERSONAL DATA IN KAZAKHSTAN ON THE BASIS OF THE GENERAL DATA PROTECTION REGULATION (GDPR)

Maksutov B.M. (Republic of Kazakhstan)
Email: Maksutov511@scientifictext.ru

Maksutov Bauyrzhan Mukhataevich – Master Student international law,
DEPARTMENT OF INTERNATIONAL LAW,
KAZAKH HUMANITARIAN LAW UNIVERSITY NAMED AFTER M.S. NARIKBAEV
NUR-SULTAN, REPUBLIC OF KAZAKHSTAN

Abstract: *this article is devoted to a comparative analysis of the legislation of the Republic of Kazakhstan on personal data and their protection and the General data protection regulation. The methods of comparative legal analysis and legal modeling were applied. Treaties in the field of personal data protection, the conclusions of the working party on data protection were considered. The author notes the inefficiency of the law of the Republic of Kazakhstan "On personal data and their protection" and the need to make changes to it, guided by the provisions of the General data protection regulation. Particular attention is paid to the main provisions of the General data protection regulation, such as personal data, controllers and processors, the data protection authority, etc. These provisions are examined in more detail by the author by referring to the doctrine, international agreements and preliminary preparation documents. Ensuring the protection of personal data is the cornerstone in the development of a democratic society. Improving the legislation of the Republic of Kazakhstan in the field of personal data is a step forward in the race for digital development and technological independence of the country. "Digital Kazakhstan" can be reached only under the conditions of technological development, on the one hand, and in the effectiveness of legal regulation, on the other. Today, there are already many technical mechanisms for ensuring data protection, such as blockchain, cryptography (in a separate application from the blockchain), cloud technologies, etc. However, legal development in this context is very far behind, which is confirmed by the inability to properly resolve these areas. The author sees significant opportunities for the country in adopting the Kazakhstani analogue of the GDPR. Based on the analysis, the urgent need to revise domestic legislation is determined. The author believes that GDPR is the very world standard in the field of ensuring high protection of personal data, on which it is necessary to develop state policy in the field of personal data protection in Kazakhstan.*

Keywords: *personal data, the law of the Republic of Kazakhstan "On personal data and their protection", General data protection regulation, GDPR, controller, processor, processing of personal data, protection of personal data.*

ПРАВОВОЙ МЕХАНИЗМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В КАЗАХСТАНЕ НА ОСНОВЕ ОБЩЕГО РЕГЛАМЕНТА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ (GDPR)

Максутов Б.М. (Республика Казахстан)

Максутов Бауыржан Мухатаевич – магистрант международного права, кафедра международного права, Казахский гуманитарно-юридический университет им. М.С. Нарикбаева, г. Нур-Султан, Республика Казахстан

Аннотация: *настоящая статья посвящена сравнительному анализу законодательства Республики Казахстан о персональных данных и их защите и Общего Регламента по защите персональных данных. В статье применены методы сравнительного правового анализа и правового моделирования. Рассмотрены международные договоры в сфере защиты персональных данных, заключения рабочей группы по защите данных и т.д. Автор отмечает неэффективность закона РК «О персональных данных и их защите» и необходимость внесения в него изменений, руководствуясь положениями Общего Регламента по защите персональных данных. Особое внимание уделяется основным положениям Общего Регламента по защите персональных данных, таким как персональные данные, контроллеры и процессоры персональных данных, орган по защите персональных данных, и др. Данные положения более детально рассматриваются автором посредством обращения к научным трудам, международным договорам и документам предварительной подготовки. Обеспечение защиты персональных данных является краеугольным камнем в развитии демократического общества. Совершенствование законодательства РК в сфере персональных данных является шагом вперед в гонке за цифровым развитием и технологической независимости страны. «Цифровой Казахстан» реален лишь при условиях технологического развития, с одной стороны, и в эффективности правового регулирования, с другой. На сегодняшний день уже существует множество технических механизмов обеспечения защиты данных, как блокчейн, криптография (в отдельном применении от блокчейна), облачные технологии и др. Однако, правовое развитие в данном контексте очень сильно отстает, что и подтверждается неспособностью правильного урегулирования указанных сфер. Автор видит значительные возможности для страны в принятии казахстанского аналога GDPR. На основе анализа определяется острая необходимость в пересмотре отечественного законодательства. Автор считает, что GDPR является тем самым мировым стандартом в сфере обеспечения высокой защиты персональных данных, на которой*

необходимо развивать государственную политику в сфере защиты персональных данных в Казахстане.

Ключевые слова: *персональные данные, закон РК «О персональных данных и их защите», Общий Регламент по защите персональных данных, GDPR, котроллер, процессор, обработка персональных данных, защита персональных данных.*

В связи с быстрым ростом информационных технологий и повседневным сёрфингом мировой сети Интернет, на сегодняшний день практический каждый человек имеет свою личную электронную почту и активно пользуется социальными сетями, а также Интернетом в целом. Информационные технологии все чаще используются для сбора личной информации, последствия которого могут быть как полезными, так и вредными для отдельных лиц. Ведь, помимо огромных преимуществ, которые принес нам Интернет, он в то же время может поставить под угрозу нашу конфиденциальность, так как наша информация распространяется по всему Интернету. Например, при совершении покупок в онлайн-режиме, когда нам приходится предоставлять данные кредитных карт или при заполнении полей регистрации на различных веб-сайтах. В связи с этим, возникает весьма логичный вопрос: где, кем и каким образом хранится наша личная информация? И безопасно ли предоставлять такую информацию о себе в целом? Для решения такой проблемы необходим правовой механизм, например, в виде закона, в котором нашли бы отражение положения о правах и обязанностях физических и юридических лиц в отношении личной информации, её сбора, хранения, использование и правил обработки в целом. В Республике Казахстан такой закон был принят 21 мая 2013 года, а именно закон РК «О персональных данных и их защите» (далее - ЗРК «О персональных данных и их защите»), который призван регулировать общественные отношения в сфере персональных данных. Однако до сих пор существуют различные разногласия и споры в связи с его применением, а понятие персональных данных, которое даётся в законе является ограниченным. Для улучшения правовой ситуации в сфере защиты персональных данных в стране, необходимым является, в первую очередь, принятие того факта, что ЗРК «О персональных данных и их защите» по своему существу является рамочным и неэффективным, а во-вторых, существует острая необходимость в пересмотре положений законодательства о персональных данных, а именно с учётом уже имеющейся мировой практики в сфере защиты персональных данных, речь о которой пойдёт в основном разделе настоящей статьи.

Основная часть.

1) Принятие ЗРК «О персональных данных и их защите» было обусловлено множеством факторов, к которым можно отнести развитие

информационно-коммуникационных технологий, электронной коммерции и др. Но на наш взгляд, основная причина закрепляется в том факте, что за сравнительно небольшой период Независимости республики, Интернет для граждан и юридических лиц стал местом осуществления сделок и договоренностей, например по купле-продаже какого-либо товара, получения какой-либо услуги и т.д. в режиме онлайн. В связи с чем существует риск возникновения возможных нарушений прав физических лиц, связанных с предоставлением необходимой личной информации (далее – персональные данные), которые нуждаются в правовом регулировании.

ЗРК «О персональных данных и их защите» определяет понятие «персональные данные» следующим образом: сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе. [1, п.2 ст.1]. Данное определение, на наш взгляд, является ограниченным, так как, перечень сведений, которые могут подпадать под понятие персональных данных, четко не регламентируется, что может привести к неоднозначности толкования данных норм. Ведь теоретически под понятие персональных данных могут подпадать любые сведения о лице. Данное положение закона не должно нести закрытый или ограничительный перечень сведений, которые могут признаваться персональными данными.

Немаловажным является и тот факт, что в законе нет ни единого положения об уполномоченном органе по защите персональных данных, что в свою очередь, очень сильно затрудняет саму реализацию закона. Как обеспечивается защита персональных данных и кем? Отсутствие независимого органа, на наш взгляд, является одним из самых больших минусов и упущений законодателя. Положение о том, что органы прокуратуры осуществляют высший надзор за соблюдением законности в сфере персональных данных и их защиты [1, п. 1 ст. 28] не подкрепляется ни судебной, ни иной правоприменительной практикой. Отсутствие четких разъяснений органов прокураторы, например, в процедурах подачи жалоб касательно защиты персональных данных, а также каких-либо подзаконных актов, ставит правовую ситуацию по защите персональных данных в тупик. Гражданам не совсем понятно, кому и как обращаться за защитой своих нарушенных прав. Следовательно, обеспечение права на защиту, а также регулирование персональных данных осуществляется каждым уполномоченным государственным органом в своем секторе по-разному. Из этого исходит и то, что ответственность за нарушение права на защиту персональных данных абсолютно игнорируется. Если гражданин считает, что его персональные данные стали объектом нарушения, то ему однозначно надо знать, кому можно обратиться, в какой

государственный орган подавать заявление, и как защитить свои персональные данные в целом.

Ситуация с обработкой персональных данных также оставляет желать лучшего. Под обработкой персональных данных понимаются действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных [1, п. 12 ст. 1]. Данное определение является не столь широким, как например определение, которое закреплено в Директиве 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных [2, ст. 2(a)]. Было бы гораздо лучше, если данная норма [1, п. 12 ст. 1] не носила бы исчерпывающий характер. Здесь стоит принять общую формулировку, что обработка персональных данных представляет собой любую операцию, которая совершается с персональными данными, начиная с момента сбора и до момента уничтожения. [3, с. 81-82]. В этом аспекте полезным будет обратиться к международному опыту по защите персональных данных, например, опыту Европейского союза (далее – ЕС) со своим Общим Регламентом по защите персональных данных.

2) В целях обеспечения защиты персональных данных своих граждан ЕС принял Общий Регламент по защите персональных данных (далее – GDPR, регламент). Данный регламент стремится обеспечить защиту персональных данных путем установления правил обработки персональных данных, которая является фундаментальным правом согласно Хартии Европейского Союза об Основных правах [4, п. 1 ст. 8], а также Договору о функционировании Европейского Союза [5, п. 1 ст. 16].

Вкратце, GDPR стремится гармонизировать все законы о защите данных в Европе с целью содействия достижению области свободы, безопасности, справедливости, экономического союза, экономического и социального прогресса, укрепления экономики во внутреннем рынке, а также благосостоянию физических лиц [6, с. 1]. GDPR разъясняет существующие правила, а также вводит новые правила обработки персональных данных с целью повышения прозрачности и целостности защиты персональных данных. Главной целью GDPR является повышение целостности, доверия и прозрачности в небезопасных условиях. В данном контексте GDPR возлагает ответственность на контроллеров данных (data controllers) и процессоров данных (data processors), которые, являются поставщиками вычислительных ресурсов и хранилищ [7, с. 47-60]. Считаем разумным рассмотреть, на наш взгляд, самые главные положения, указанные в GDPR, их правовую природу, включая вышеуказанные понятия.

Согласно GDPR, обработкой может быть почти всё, что делается с личными данными, такими как; сбор, запись, организация, структурирование, хранение, адаптация или изменение, поиск, консультация, использование, раскрытие путем передачи, распространения или иного предоставления, выравнивание или сочетание, ограничение, удаление или уничтожение. [7, с. 33]. По сути, обработка персональных данных это то, чем мы сталкиваемся каждый день, например, каждый раз, когда мы покупаем что-нибудь у поставщика услуг, каждый раз, когда мы регистрируемся в социальных сетях, и каждый раз, когда мы покупаем что-то в Интернете, существует базовый процесс, который обрабатывает наши персональные данные. Это, в свою очередь, налагает много обязательств на корпорации, чьи предприятия полагаются на обработку персональных данных для получения денежной выгоды. В связи с этим GDPR очень тщательно разделяет понятия контроллеров данных (data controllers) и процессоров данных (data processors), а также распределяет их обязательство и ответственность. Подобное понятия отсутствуют в законодательстве РК. Например, согласно GDPR контроллером считается юридическое лицо, государственный орган, агентство или другой уполномоченный орган, который совместно или единолично определяет цель и способы обработки персональных данных. [7, с. 33]. Это означает, что контроллер отвечает за обработку персональных данных, что накладывает на него некоторые юридические обязательства. [8, с. 19]. Здесь можно заметить, что определение, которое даёт GDPR является конкретным и обхватывает все возможные аспекты защиты персональных данных в целом.

Юридическое определение контроллера может быть разбито на три компонента; (1) юридическое лицо, государственный орган, агентство или другой уполномоченный орган (2), которые совместно или в одиночку (3) определяют цель и средства обработки. Первый компонент разъясняет, что никто, даже физическое лицо, не освобождается от ответственности, когда речь заходит об обработке персональных данных. Второй компонент расширяет охват определения контроллера и включает совместную ответственность за обработку персональных данных. В GDPR вводится понятие «совместного управления» в статье 26. Что именно это влечет за собой для контроллеров, на данный момент неясно, но, поскольку стороны принимают на себя взаимную ответственность, очевидно, что они должны учитывать четкое распределение обязанностей. [9, с. 18]. Совместное управление может принимать различные формы и, согласно A29WP, не должно быть взаимным. [8, с. 33]. Это означает, что совместные контроллеры могут иметь либо очень тесные отношения с общей инфраструктурой, назначением и средствами обработки, либо слабые отношения только с частично совместно используемыми средствами или целями обработки. Третий компонент, и, возможно, самый важный

компонент, иллюстрирует, что тот, кто обладает полномочиями принятия решений, а не фактическими полномочиями по обработке, должен быть классифицирован как контроллер [8, с. 8].

Процессором, также как и в случае с контроллером, может быть физическое лицо, юридическое лицо, государственный орган, агентство или другой уполномоченный орган, который обрабатывает данные от имени контроллера [7, с. 33]. Но здесь нужно отметить, что для существования процессора необходимо существование контроллера. Кроме того, чтобы классифицироваться как процессор, требуется, чтобы он был отдельным юридическим лицом по отношению к контроллеру [8, с. 25]. Следовательно, процессор действует в интересах контроллера и получает делегированные им задачи в рамках средств и целей собственной повестки дня контроллера [8, с. 25]. Необходимо обратить внимание, что процессор, который превышает свою ответственность и получает должность, которая имеет отношение к определению средств и целей обработки персональных данных, помечается как совместный контроллер вместе с первоначальным контроллером, что расширяет их ответственность [9, с. 20].

GDPR устанавливает очень конкретные критерии, касающиеся того, как контроллер и процессор обрабатывают персональные данные для обеспечения целостности и повышения прозрачности. Цель состоит в том, чтобы обеспечить справедливую и законную обработку. [7, с. 33]. Первый строительный блок обеспечения соблюдения ценностей состоит из ограничения цели и общего принципа, который изображает ядро GDPR, а именно: «Законность, справедливость и прозрачность». [7, с. 35]. Законность в соответствии с GDPR достигается, например, путем получения согласия субъектов данных в отношении одной или нескольких целей [7, с. 36]. Законность может быть достигнута другими способами согласно статье 6, например, если контролер должен сделать это для выполнения юридического обязательства, если обработка требуется для достижения целей, а интересы контролера перевешивают право субъектов данных на целостность и многое другое. Следовательно, при сборе персональных данных контролер должен указать точную цель/цели (ограничение цели), которые должны обслуживаться при обработке собранных персональных данных, и только тогда обработка является законной согласно Статье 5 (1) (a) в GDPR [10, с. 26].

3) Второй структурный блок состоит из принципов, касающихся того, какие личные данные хранятся и как эти данные хранятся [6, p. 2]. Прежде всего, GDPR применяет принцип минимизации данных в соответствии со статьей 5 (1) (c), чтобы данные оставались актуальными, адекватными и ограниченными тем, что необходимо [11, с. 115]. GDPR также обеспечивает соблюдение следующих принципов в статье 5 (1) (г-е): Принцип точности, чтобы обеспечить актуальность данных и удаление

неточных данных. Принцип ограничения хранения гарантирует, что период, в течение которого хранятся персональные данные, ограничен очень строгим минимумом и находится в прямой зависимости от выполнения цели обработки [12, с. 13]. Наконец, принцип целостности и конфиденциальности, который гарантирует, что персональные данные субъектов данных обрабатываются и хранятся таким образом, который обеспечивает меры безопасности для предотвращения несанкционированного доступа и незаконной обработки, а также для предотвращения повреждения и полной потери данных. Эти принципы, изложенные в статье 5 GDPR, изображают ядро GDPR и представляют собой строгое требование к контролеру в отношении персональных данных, обработки и хранения таких данных. Контролер несет ответственность и должен быть в состоянии продемонстрировать соответствие принципам статьи 5 (2) GDPR. Учитывая вышеупомянутые принципы, субъект данных получает огромное количество прав в отношении обработки своих персональных данных, что отражено в статье 12-21 в GDPR. Это, в свою очередь, накладывает определенные обязательства на контроллера. Считаем разумным лишь перечислить некоторые права, а не раскрывать их по-одному, в связи с объемом настоящей статьи.

GDPR наделяет субъекта персональных данных следующими правами: 1) право на доступ к информации [7, с. 39] (право на доступ усиливает возможность субъекта данных проверять, что контроллер действует законно, следовательно, обеспечивает соблюдение прав субъекта данных [6, с. 4]); 2) право на удаление, исправление и ограничение обработки [7, с. 44] (эти три права являются не только способом предоставления субъекту данных контроля над своими персональными данными, но и способом применения средств для субъекта данных для устранения нарушений закона, совершаемых контроллером над его персональными данными [9, с. 154]); 3) право на переносимость данных [7, с.45] (это право создает возможность передачи данных «из одной электронной системы обработки в другую и без нее, что не может быть предотвращено контроллером» [13, с. 9]); 4) право на возражение и автоматизированное принятие решений [7, с. 45-46] (положение в основном направлено на законную обработку, которую субъект данных не хочет, чтобы контроллер выполнял).

Из этого следует, что GDPR направлен на повышения прозрачности и расширения возможностей субъекта данных контролировать свои персональные данные, навязывая определенные права субъекту данных, которые переводятся в обязательства для контроллера и процессора. Эти обязательства принимают две отдельные формы. Первым набором обязательств является ответственность контроллера за то, что он может предоставить вышеупомянутый материал субъекту данных, то есть право

на информацию и переносимость данных. Эти права направлены на повышение прозрачности и обеспечивают понимание предмета данных. Второй набор обязательств – это организационные меры, которые должен выполнять ответственный контроллер/процессор. Они предназначены для повышения безопасности и защиты персональных данных.

Заключение. В последние годы наблюдается всё больше нарушений прав субъектов персональных данных в связи с чрезмерной монетизацией таких данных. Закон РК «О персональных данных и их защите» не приспособлен разрешать подобные нарушения на стадии его сегодняшнего нахождения. Закон существует уже 6 лет, а реальные механизмы правового регулирования нарушений, связанных с персональными данными, так и не были сформулированы. Но законодатель постарался и, всё-таки, установил нормативную базу в сфере защиты персональных данных, однако положения, заложенные в законе четко не сформулированы, для реализации этих правовых механизмов необходимо унифицировать все положения, относящиеся к защите персональных данных, т.е. необходим наш собственный GDPR, который поспособствовал бы принятию политики предоставления субъекту персональных данных большего контроля над своими данными.

Данный регламент является одним из самых эффективных правовых инструментов в сфере защиты персональных данных, который закрепляет фундаментальные принципы и ценности защиты личной информации. GDPR способствует усилению контроля субъекта данных за своими персональными данными. Считается разумным руководствоваться опытом GDPR в составлении нашего собственного правового механизма по защите персональных данных, а именно включение в уже имеющийся закон положений о процессорах и контроллеров, учреждения независимого органа по защите персональных данных, о чем настоящий автор писал более подробно в другой статье [14, с. 1].

Внесение подобных изменений в законодательство непременно будет способствовать, во-первых, эффективному применению положений закона, во-вторых, усилению контроля субъектов персональных данных за своими данными, а также эффективной защите персональных данных в целом. Лишь посредством установления положений о принципах и правилах обработки персональных данных, правовой природы контроллера и процессора, деятельности уполномоченного органа по защите персональных данных, ответственности за нарушения и других подобных положений, как они закрепляются в GDPR, можно действительно претендовать на звание “Цифровой Казахстана в эпоху глобализации”, поскольку именно GDPR является одним из самых высоких на сегодняшний день стандартов безопасности в отношении защиты персональных данных.

Список литературы / References

1. Закон Республики Казахстан // «О персональных данных и их защите», 21 мая 2013 года № 94-V.
2. Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза // «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных», 24 октября 1995 г.
3. *Лозовая О.В.* // Право и государство «Обработка персональных данных без согласия субъекта: практика обеспечения нарушенных прав (на примере Казахстана и Великобритании)», 2016. № 3 (72).
4. Хартия Европейского Союза // «Об основных правах», 7 декабря 2000 года.
5. Договор о функционировании Европейского Союза // Договор о функционировании Европейского Союза, Рим, 25 марта 1957 г., в редакции Лиссабонского договора 2007 г.
6. Комментарий // Общий Регламент по защите данных, V1.1 20170519.
7. Европейский союз // Общий Регламента по защите данных, 27 апреля 2016 года.
8. Рабочая группа по защите данных // Постановление 1/2010 касательно концепции «контроллера» и «процессора», 2014.
9. *Войт и Буше* // Общий Регламент по защите данных, 2017.
10. *Форго Н., Ханольд С. и Шютзе Б.* // «Принцип ограничения цели и Big Data», 2017 г.
11. *Ли А. Бигрейв* // Защита данных в соответствии с замыслом и по умолчанию: расшифровка законодательных требований ЕС, 2017.
12. Уполномоченный по защите данных ЕС // Руководство по защите персональных данных в сфере управления ИТ и управления ИТ институтов ЕС. 19 мая 2018.
13. Предложение о постановлении Европейского парламента и Совета // О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, 2012 г.
14. *Максутов Бауыржан Мухатаевич* // Деятельность независимого органа по защите персональных данных, 2019.