АНАЛИЗ
НЕКОТОРЫХ СТАТЕЙ ПРОЕКТА ЗАКОНА РЕСПУБЛИКИ КАЗАХСТАН «О ВНЕСЕНИИ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ В НЕКОТОРЫЕ ЗАКОНОДАТЕЛЬНЫЕ АКТЫ РЕСПУБЛИКИ КАЗАХСТАН ПО ВОПРОСАМ РЕГУЛИРОВАНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ»

Подготовлен: И.Лоскутов,

юрист, начальник юридического отдела ТОО «ИнфоТех&Сервис»,

май, 2020

Содержание:

Прим. – проект Закона был подписан Президентом РК Касым-Жомартом Токаевым 25 июня 2020 г.

Данный анализ был подготовлен при поддержке Информационной программы Фонда Сорос-Казахстан. Содержание данной публикации отражает мнение автора и не обязательно совпадает с точкой зрения Фонда Сорос-Казахстан.

1. Компетенции уполномоченного органа в сфере защиты персональных данных

Вопрос о создании Уполномоченного органа поднимался еще в момент обсуждения **проекта Закона Республики Казахстан «О персональных данных»**[1] в 2012 году.

Комитет по социально-культурному развитию Мажилиса Парламента РК предлагал предусмотреть в проекте Закона создание **Уполномоченного органа по защите прав субъектов персональных данных**, наделив его полномочиями по **контролю и надзору** за соответствием обработки персональных данных требованиям законодательства Республики Казахстан в области персональных данных. Одной из приоритетных задач указанного уполномоченного органа должно было стать ведение **Реестра держателей персональных данных**. Кроме того, предлагалось предусмотреть **механизм взаимодействия** Уполномоченного органа с правоохранительными и другими государственными органами в ходе контрольно-надзорной деятельности.

Согласно предложению депутатов, Уполномоченный орган в сфере персональных данных, как государственный орган, осуществляющий руководство в сфере персональных данных, имел следующую компетенцию:

1) разрабатывает и утверждает порядок определения собственником и оператором перечня персональных данных, необходимого для выполнения осуществляемых ими задач;

2) координирует деятельность в сфере персональных данных в соответствии с требованиями настоящего Закона;

3) вносит предложения по совершенствованию нормативных правовых актов в сфере персональных данных;

4) осуществляет контроль и надзор за соблюдением законодательства Республики Казахстан в сфере персональных данных в соответствии с Законом Республики Казахстан «О государственном контроле и надзоре в Республике Казахстан»;

5) запрашивает и получает в порядке, установленном законами Республики Казахстан, от субъекта, собственника и (или) оператора, а в отдельных случаях третьего лица информацию, необходимую для реализации своих полномочий;

6) осуществляет проверку собственников и операторов или привлекает для осуществления такой проверки иные государственные органы в пределах их полномочий;

7) выявляет и принимает меры по устранению нарушений законодательства Республики Казахстан в сфере персональных данных;

8) требует от собственника и (или) оператора подтверждения блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

9) обеспечивает соблюдение прав субъектов, собственников и операторов;

10) рассматривает обращения физических и юридических лиц по вопросам, связанным со сбором, обработкой, защитой персональных данных;

11) в случае необходимости обращается с исковым заявлением в суд в защиту прав субъектов, собственников и операторов и представляет их интересы в суде;

12) информирует субъектов, собственников и операторов по их обращениям о состоянии работы в сфере персональных данных;

13) ведет реестр собственников и (или) операторов;

[1] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=31019141

14) выполняет иные функции, возложенные на него настоящим Законом, иными законами Республики Казахстан и актами Президента Республики Казахстан и Правительства Республики Казахстан.»

Однако в окончательную редакцию **Закона Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите»** (далее – Закон РК «О персональных данных и их защите)[2] эти нормы не прошли.

Рассматриваемый Проект **до внесения** в Мажилис Парламента РК (на сентябрь 2019 года[3]) **не содержал норм** об Уполномоченном органе в сфере защиты персональных данных.

Но необходимость его создания к тому времени уже осознавалась. Так, выступая на **конференции DigitalRights@KZ (21 мая 2019 года)** заместитель председателя Комитета по информационной безопасности Министерства цифрового развития, оборонной и аэрокосмической промышленности Руслан Абдикаликов сказал: «У нас такой менталитет в стране сложился, что если нет уполномоченного госоргана, то закон как бы повис в воздухе. Он не рабочий. Почему? Потому что при его создании МВД избрало такую модель, что **каждый уполномоченный госорган в своей сфере будет регулировать эти отношения**. Если у вас какие-то проблемы с поликлиникой и персональными данными, вы должны обратиться в Минздрав. Если у вас проблема с «Кунделиком», вы должны обратиться в Минобразования. Если у вас с Egov какие-то проблемы, вы должны обратиться в наше министерство. В итоге **гражданину абсолютно непонятно, кому же он должен пожаловаться**. И во-вторых, у всех этих госорганов **нет права наказать потом того, кто виноват в утечке данных**»[4]. А уже в октябре 2019 года Вице-министр цифрового развития, инноваций и аэрокосмической промышленности Марат Нургожин заявил: «Вместе с тем у нас законодательно не определён госорган по защите персональных данных. Мы вносим сейчас поправки в законодательство, где предусматриваем норму - **определить наше министерство уполномоченным органом** по защите прав субъектов персональных данных.»[5].

В действующем **разделе «Защита персональных данных (Data protection agency)» портала «Электронное правительство Республики Казахстан»** [6] заявлено следующее:

«Общий регламент о защите данных (правила по обработке личных данных) является законом прямого действия в 28 странах Евросоюза. На основании общего регламента **будет функционировать организация по Защите персональных данных (Data protection agency) в Казахстане**.

Цель:

- осуществление государственного контроля за единообразным исполнением законодательства в сфере защиты персональных данных
- рассматривание жалоб по нарушениям законодательства в сфере защиты персональных данных

[2] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=31396226

[3] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=33400415

[4] https://www.soros.kz/ru/personal-data-protection-in-kz/

[5] https://forbes.kz/process/technologies/v_kazahstane_ne_okazalos_gosorgana_po_zaschite_personalnyih_dannyih

[6] https://egov.kz/cms/ru/cyberspace

- предоставление разъяснений и методической помощи по вопросам защиты персональных данных

Текущий статус по защите персональных данных:

- Для регулирования общественных отношений в сфере персональных данных существует Закон РК «О персональных данных и их защите»
- Особенности защиты персональных данных в электронной форме для государственных систем определены в Законе РК «Об информатизации»
- Установлена ответственность за нарушение законодательства РК о персональных данных и их защите
- На усмотрение оставлены вопросы защиты собственников и операторов персональных данных

Новые функции Комитета по информационной безопасности:

- Нормативно-правовое регулирование сферы защиты персональных данных
- Ведение реестра операторов персональных данных
- Защита прав субъектов персональных данных
- Контроль за соблюдением требований по защите персональных данных

Ожидаемый результат мероприятия по защите персональных данных

- Приведение сферы обработки персональных данных **в соответствие с требованиями лучших мировых практик (GDPR)**
- Увеличение привлекательности цифровой экономики для граждан и бизнеса
- Содействие развитию отрасли информационной безопасности
- Повышения доверия к государству со стороны граждан и бизнеса».

Так называемый проект «Комитета по информационной безопасности» был реализован в рассматриваемом Проекте в виде «**Уполномоченного органа в сфере защиты персональных данных**».

Представляя документ в Мажилисе, министр цифрового развития, инноваций и аэрокосмической промышленности РК Аскар Жумагалиев отметил, в частности: «внедрение цифровых технологий требует защиты прав граждан нашей страны. В связи с этим, предлагается определить Уполномоченный орган в сфере защиты персональных данных»[7].

Согласно Проекту, это центральный исполнительный орган, осуществляющий **руководство в сфере защиты персональных данных**. Подразумевается, что это будет Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан (далее – МЦРИАП), а внутри него республиканское государственное учреждение «Комитет по информационной безопасности».

Согласно **правительственному проекту:**

«Уполномоченный орган в сфере защиты персональных данных в пределах своей компетенции:

1) участвует в реализации государственной политики в сфере защиты персональных данных;

[7] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=37612313

2) разрабатывает порядок осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных;

3) рассматривает обращения субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение;

4) принимают меры по привлечению лиц, допустивших нарушения законодательства Республики Казахстан о персональных данных и их защите, к ответственности, установленной законами Республики Казахстан;

5) требует от оператора персональных данных уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

6) вносит в Правительство Республики Казахстан предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных;

7) осуществляет меры, направленные на совершенствование защиты прав субъектов персональных данных;

8) утверждает Правила сбора и обработки персональных данных;

9) осуществляют иные полномочия, предусмотренные законами Республики Казахстан, актами Президента Республики Казахстан и Правительства Республики Казахстан».

В **Проекте, утвержденном Мажилисом**, помимо чисто редакционных поправок, из компетенции исчезла норма подпункта 6 о том, что Уполномоченный орган «**вносит в Правительство** Республики Казахстан **предложения о совершенствовании нормативного правового регулирования** защиты прав субъектов персональных данных». Логично, что эта норма охватывается указанием на **иные полномочия**, предусмотренные в подпункте 9 процитированной статьи. У МЦРИАП в силу своего статуса и так есть полномочия по участию в правотворчестве.

При этом она указывает на главную проблему по данному вопросу в Проекте.

Создается **не независимый орган, а орган, входящий в структуру Правительства**, которое «осуществляет руководство деятельностью министерств, обеспечивает исполнение ими законов, актов Президента и Правительства Республики»[8].

Почему МЦРИАП и его ведомство нельзя назвать подлинно независимым органом?

В Резолюции от 14 ноября 2018 года № A/C.3/73/L.49/Rev.1 «Право на неприкосновенность частной жизни в цифровую эпоху»[9] Генеральная Ассамблея Организация Объединенных Наций *призывает* все государства:

«g) рассмотреть вопрос о принятии и обеспечении выполнения законодательства, норм регулирования и политики и в области защиты данных, … которое соответствовало бы их обязательствам по международному праву прав человека, которые могут включать **создание независимых национальных органов**, наделенных **полномочиями и ресурсами** для наблюдения за практикой в области обеспечения конфиденциальности данных, **расследования нарушений и злоупотреблений**, **получения информации и жалоб** от лиц и организаций и предоставления **надлежащих средств правовой защиты**;».

[8] Конституционный закон Республики Казахстан от 18 декабря 1995 года № 2688 «О Правительстве Республики Казахстан» ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=1003973

[9] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=36838318

Таков подход на уровне ООН, участником которой является наша страна.

Что касается европейского опыта, то основой для его применения служит статья 237 **Соглашения о расширенном партнерстве и сотрудничестве между Европейским Союзом и его государствами-членами, с одной стороны, и Республикой Казахстан, с другой стороны (Астана, 21 декабря 2015 года)**[10], которая гласит: «Стороны сотрудничают для обеспечения высокого уровня защиты персональных данных посредством обмена передовым опытом и практикой, **принимая во внимание европейские и международные правовые документы и стандарты**».

Также, если верить вышеприведенной информации на сайте Электронного правительства РК[11], организация по защите персональных данных должна функционировать на основании общего регламента Европейского союза.

Речь в первую очередь о Регламенте № 2016/679 Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС **(Общий Регламент о защите персональных данных). GDPR»** (г. Брюссель, 27 апреля 2016 года)[12] (далее – GDPR), также следует учитывать и Директиву (EU) 2016/680 Европейского парламента и Совета «О защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования уголовных преступлений, ведения розыскных или судебных действий или исполнения уголовных наказаний, а также за свободное перемещение таких данных и отменяя Рамочное решение Совета 2008/977/JHA»[13].

Согласно GDPR, предусматривается создание одного или нескольких независимых органов государственной власти для защиты основных прав и свобод физических лиц при обработке данных. Каждый надзорный орган должен быть **полностью независим при выполнении своих задач и осуществлении своих полномочий**. Если учреждается несколько надзорных органов, должны быть установлены правовые механизмы для обеспечения эффективного участия этих надзорных органов в механизме согласования. Надзорный орган должен функционировать **как единый контактный центр** для эффективного участия этих органов в механизме, чтобы обеспечить оперативное и бесперебойное сотрудничество с другими надзорными органами.

Член или члены каждого надзорного органа при выполнении своих задач и осуществлении своих полномочий **не должны подвергаться прямому или косвенному воздействию внешних факторов**, а также не должны ни стремиться **получить, ни получать указания от кого бы то ни было**. Член или члены каждого надзорного органа должны воздерживаться от любых действий, несовместимых с их обязанностями, и в течение срока действия полномочий не должны участвовать в любой другой несовместимой с их полномочиями оплачиваемой или неоплачиваемой деятельности.

Общие условия для члена/членов надзорного органа должны быть установлены правом и должны предусматривать, **прозрачность процедуры их назначения** Парламентом, Правительством, либо главой государства по представлению Правительства, члена Правительства, Парламента или Палаты Парламента или независимого ответственного органа в соответствии с правом.

---

[10] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=37496546

[11] https://egov.kz/cms/ru/cyberspace

[12] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=39559334

[13] https://ogdpr.eu/ru/gdpr-2016-680

Каждый член должен обладать необходимыми для выполнения своих обязанностей и осуществления своих полномочий **квалификациями, опытом и навыками**, в частности, **в области защиты персональных данных**.

Что касается задач, то в GDPR указаны следующие из них, не отраженные в рамках рассматриваемого Проекта должным образом:

- содействовать информированности общества и пониманию рисков, норм, гарантий и прав в отношении обработки. Особое внимание необходимо уделять деятельности, касающейся детей;
- консультировать в соответствии с законодательством, национальный парламент, правительство и другие институты и органы о законодательных и административных мерах, связанных с защитой прав и свобод физических лиц при обработке их данных;
- содействовать информированности контролеров и обрабатывающих данные лиц относительно их обязанностей;
- по запросу предоставить информацию любому субъекту данных относительно осуществления его прав;
- рассматривать жалобы, поданные субъектом данных или органом, организацией или объединением, расследовать, в соответствующих случаях, предмет жалобы и в приемлемый срок проинформировать заявителя о ходе и результатах расследования, в частности, если необходимо дальнейшее расследование или сотрудничество с другим надзорным органом;
- сотрудничать с другими надзорными органами, включая обмен информацией и предоставление взаимной помощи с тем, чтобы гарантировать согласованное применение и исполнение настоящего Регламента;
- проводить расследования, в том числе на основании информации, предоставленной другим надзорным органом или органом государственной власти;
- контролировать соответствующие изменения, если они влияют на защиту персональных данных, в частности, разработку информационных и коммуникационных технологий и деловых практик;
- вести внутренний учет нарушений законодательства и принятых мер.

Каждый надзорный орган должен располагать следующими следственными полномочиями:

- поручать контролеру и обрабатывающему данные лицу и, в соответствующих случаях, их представителю предоставить любую информацию, необходимую ему для выполнения его задач;
- проводить расследования в форме аудиторских проверок защиты данных;
- уведомить контролера или обрабатывающее данные лицо о предполагаемом нарушении;
- от контролера или обрабатывающего данные лица получить доступ ко всем персональным данным и всей информации, необходимой ему для выполнения его задач;
- получить доступ к любым помещениям контролера или обрабатывающего данные лица, включая оборудование и средства для обработки данных, в соответствии с процессуальным законодательством.

Каждый надзорный орган должен располагать следующими корректирующими полномочиями:

- выдавать предупреждения контролеру или обрабатывающему данные лицу о том, что запланированная обработка данных может нарушать положения законодательства;
- делать предупреждения контролеру или обрабатывающему данные лицу, если обработка данных нарушила положения законодательства;
- требовать от контролера или обрабатывающего данные лица соблюдать запросы субъекта данных относительно осуществления его прав согласно законодательству;
- потребовать от контролера или обрабатывающего данные лица привести процесс обработки данных в соответствие положениям законодательства, при необходимости, в установленном порядке и в установленный срок;
- потребовать от контролера сообщить субъекту данных об утечке персональных данных;
- наложить временное или окончательное ограничение на обработку данных, включая запрет;
- потребовать приостановить передачу данных получателю в третьей стране или международной организации.

Каждый надзорный орган должен располагать следующими разрешительными и консультативными полномочиями:

- консультировать контролера;
- по собственной инициативе или по запросу выдавать национальному парламенту, правительству или другим институтам или органам, а также общественности заключения по любому вопросу, связанному с защитой персональных данных.

На основе вышеизложенного, с точки зрения международных правовых документов и стандартов, МЦРИАП никак не может быть признан **реально независимым надзорным органом** в сфере защиты персональных данных.

Во-первых, налицо **конфликт интересов**, в лице многочисленных структур, входящих в состав МЦРИАП или подчиняющихся ему в той или иной степени, и массово занимающихся обработкой персональных данных.

Соответственно, МЦРИАП будет вынуждено, как представлять и защищать интересы собственников и операторов баз, содержащих персональные данные, так и осуществлять надзор за их деятельностью. Возможно, именно этим можно объяснить, что разработчики Проекта и депутаты включили в него отдельную норму о том, что: «В отношении персональных данных, ставших известными уполномоченному органу в сфере защиты персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных». Хотя конфиденциальности персональных данных и так посвящена статья 11 Закона РК «О персональных данных и их защите» в целом.

Во-вторых, это должен быть **институционально независимый орган** с **достаточными полномочиями** и **квалифицированными сотрудниками**, а не ведомство министерства по факту.

То есть такой орган, который сможет при необходимости проверять другие государственные органы, включая органы прокуратуры (ЦПСИ), специальные и

правоохранительные государственные органы и давать им обязательные к исполнению предписания.

Между тем, действующая компетенция Правительства и других государственных органов в Законе РК «О персональных данных и их защите» оказалась совершенно нетронутой поправками Проекта.

По-прежнему, именно Правительство **разрабатывает основные направления** государственной политики в сфере персональных данных и их защиты, а Уполномоченный орган будет лишь **принимать участие в ее реализации**.

Правительство осуществляет руководство деятельностью центральных исполнительных органов, входящих в структуру Правительства Республики Казахстан, местных исполнительных органов, в сфере персональных данных и их защиты. Ни о какой координирующей роли Уполномоченного органа, предусмотренной GDPR, речи не идет.

Оно же будет утверждать порядок определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач, а также осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных. Указано лишь, что Уполномоченный орган теперь будет готовить их проекты, а раньше этим занималось МВД РК[14].

Нетронутой и непонятной осталась **роль органов прокуратуры**, о которых высказывалось мнение, как о не оправдавших свое назначение центральным координирующим органом по защите персональных данных (по административной ответственности будет указано ниже).

Прочие государственные органы в пределах своей компетенции будут также продолжать разрабатывать и (или) утверждать нормативные правовые акты в сфере персональных данных и их защиты; рассматривать обращения физических и (или) юридических лиц по вопросам персональных данных и их защиты; принимать меры по привлечению лиц, допустивших нарушения законодательства Республики Казахстан о персональных данных и их защите, к ответственности, установленной законами Республики Казахстан.

Получается, что Уполномоченный орган будет просто **наравне с другими государственными органами** рассматривать обращения и привлекать к ответственности.

При этом непонятно, **как будет распределена компетенция** по рассмотрению обращений между Уполномоченным органом и прочими органами.

Более того, согласно статье 23 Закона РК «О персональных данных и их защите»: «Особенности защиты **электронных информационных ресурсов**, содержащих персональные данные, устанавливаются в соответствии с **законодательством Республики Казахстан об информатизации»**.

Однако в Законе Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»[15] компетенция Уполномоченного органа по защите персональных данных не прописана ни на данный момент, ни в Проекте.

Получается, что законодательство об информатизации в части защиты электронных информационных ресурсов, содержащих персональные данные, **будет иметь приоритет** над обычным законодательством о персональных данных. И государственные органы будут в первую очередь использовать нормы, содержащиеся там.

[14] https://kzgov.docdat.com/docs/411/index-636084.html

[15] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=33885902

Что касается ответственности, то в целом корректировки карательного механизма следует признать соответствующим логики Проекта. Так, в связи с созданием Уполномоченного органа, ему **передаются функции в части привлечения к административной ответственности** за нарушение законодательства в сфере защиты персональных данных от Генеральной прокуратуры (в настоящее время органы прокуратуры выносят постановление о возбуждении дел об административных правонарушениях) и специализированных районных и приравненных к ним административных судов (в настоящее время рассматривают дела).

Следует, однако, отметить игнорирование в Проекте способа защиты прав субъектов персональных данных в **судебном порядке**.

Так, в рамках GDPR, любой субъект может передать жалобу в надзорный орган по месту жительства, месту работы или месту предполагаемого нарушения его прав. По факту данного обращения надзорный орган обязан предоставить информацию о получении жалобы, процессе рассмотрения и **возможности судебного разбирательства**. Если надзорный орган не в состоянии, с точки зрения субъекта персональных данных, выполнить свои обязанности по удовлетворению обращения субъекта, то последний **вправе обратится в суд по месту регистрации надзорного органа**. Полномочия, предоставленные надзорному органу согласно GDPR, осуществляются при условии наличия соответствующих гарантий, включая эффективные средства судебной защиты и должную процедуру, установленную в законодательстве государства. Каждое государство должно законодательно предусмотреть, что его надзорный орган вправе довести до сведения органов судебной власти факт нарушения законодательства о персональных данных и, в соответствующих случаях, вправе начать или иным образом участвовать в судебном процессе в целях обеспечения исполнения его положений.

Правом обращения в суд также обладают **любые ассоциации и организации, которые связаны с защитой персональных данных в интересах общества**.

Казахстанский закон ничего не содержит в этом плане.

На основании изложенного, **видятся необходимыми следующие корректировки Проекта в части определения статуса Уполномоченного органа**:

1) право осуществлять межотраслевую координацию деятельности государственных органов по обеспечению реализации государственной политики в сфере защиты персональных данных;

2) право утверждать нормативные правовые акты в сфере защиты персональных данных, в том числе в электронной форме;

3) право запрашивать и получать информацию, необходимую для реализации своих полномочий;

4) право обращается с исковым заявлением в суд в защиту прав субъектов, собственников и операторов и представлять их интересы в суде;

6) право осуществляет проверку собственников и операторов или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

5) обязанность проводить анализ жалоб субъектов и деятельности государственных органов по вопросам защиты персональных данных;

6) обязанность проводить информирование, консультирование и просвещение субъектов, собственников и операторов по их обращениям в сфере защиты персональных данных.

Прочие полномочия, указанные в вышеупомянутых правилах GDPR представляется возможным реализовать на уровне подзаконных актов.

2. Нормы по биометрической аутентификации

Закон Республики Казахстан от 15 апреля 2013 года «О государственных услугах»:

Статья 8. Компетенция уполномоченного органа в сфере оказания государственных услуг

Уполномоченный орган в сфере оказания государственных услуг:

...

8-2) **утверждает** правила сбора, обработки и хранения биометрических данных в сфере оказания государственных услуг для биометрической аутентификации физических лиц **совместно с уполномоченным органом** в сфере защиты персональных данных

Данная норма претерпела следующую трансформацию в процессе рассмотрения в Мажилисе Парламента РК: «8-1) **разрабатывает и утверждает** правила сбора, обработки и хранения биометрических данных физических лиц для их биометрической аутентификации при оказании государственных услуг **по согласованию** с уполномоченным органом в сфере защиты персональных данных;».

То есть, произошло сужение компетенции Уполномоченного органа в сфере защиты персональных данных, теперь он будет только согласовывать указанные правила.

Статья 11-1. Организация деятельности Государственной корпорации

«…4. Государственная корпорация:

…

6-1) осуществляет сбор, обработку и хранение биометрических данных физических лиц в сфере оказания государственных услуг;

6-2) осуществляет ведение биометрической базы данных физических лиц, используемой для биометрической аутентификации в рамках оказания государственных услуг».

Данная норма поступила без изменений в Сенат Парламента РК.

Первоначально планировалось внедрение норм по биометрической аутентификации в рамках рассматриваемого Проекта. Обоснованием для этого было то, что Глава государства в своем Послании народу Казахстана от 31 января 2017 г. «Третья модернизация Казахстана: глобальная конкурентоспособность» указал на необходимость перевести полностью в электронный формат без обязательного физического присутствия процедуру оказания государственных услуг.

В Концепции рассматриваемого Проекта[16] также было сказано на этот счет следующее.

«С развитием информационных технологий стали активно применяться электронные документы. При этом, в электронном документообороте особое внимание уделяется задачам **электронной аутентификации**, то есть удостоверения подлинности электронного документа, а также его принадлежности (лица подписавшего его), при этом законодательством Республики Казахстан об электронном документе, аутентификация ограничивается применением лишь логин/пароля, электронной цифровой подписи и одноразового пароля, при этом к электронной цифровой подписи выдвигаются требование по использованию технологии открытого ключа, имеющего регистрационное

[16] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=33400415

свидетельство. Вместе с тем, в настоящее время все большее распространение получает **биометрическая аутентификация** пользователя, позволяющая уверенно аутентифицировать потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения. К основным достоинствам биометрических методов можно отнести высокую степень достоверности аутентификации по биометрическим признакам, неотделимость биометрических признаков от личности, трудность фальсификации биометрических признаков.

В этой связи, требуется пересмотреть существующий подход к формированию требований к электронной подписи и удостоверения подлинности электронного документа в Республике Казахстан, в том числе снятие имеющихся ограничений по применению иных способов аутентификации в электронном документе, поскольку как показывает международная практика, иные способы аутентификации, в том числе биометрическая аутентификация применяются в различных сферах деятельности.

Так, в проекте Закона будут предусмотрены правила сбора, хранения и использования биометрических данных для биометрической аутентификации физических лиц. Также положения по оказанию интерактивной, транзакционной, композитной услуг, которые могут осуществляться при успешной биометрической аутентификации субъекта, за исключением случаев, где результатом государственной услуги является электронный документ, накладывающий обязательства на заявителя.

Кроме того, внедрение механизма удаленной идентификации клиентов является прогрессивным шагом навстречу дистанционным услугам, что чрезвычайно актуально в век цифровых технологий и способно обеспечить новыми сервисами и продуктами различные категории клиентов, охватить население страны, проживающее в отдаленных регионах. При внедрении данного механизма граждане смогут получать услуги дистанционным способом (используя любое оборудование - смартфоны, планшеты, компьютеры) при первичном обращении в финансовую организацию, а также в последующем при пользовании их услугами».

Следует согласиться с приведенными доводами, отметив и то, что технологии биометрии широко используются финансовыми организациями и другими участниками рынка, выходящими за сферу полномочий уполномоченного органа в сфере оказания государственных услуг. Так, например, в Законе Республики Казахстан от 26 июля 2016 года № 11-VI «О платежах и платежных системах»[17] средство биометрической идентификации указано как идентификационное средство.

В Отчете о деятельности Уполномоченного по правам человека в Республике Казахстан за 2018 год[18] говорится: «В рамках реализации «Цифровой Казахстан» в стране стартовал пилотный проект по оказанию государственных услуг посредством использования биометрических параметров. Механизм по оказанию государственных услуг посредством биометрической базы данных подразумевает использование лица и отпечатков пальцев услугополучателей при получении государственных услуг в ЦОНах и на портале электронного правительства, без предъявления личных документов или электронной цифровой подписи (ЭЦП). В настоящее время посредством биометрических данных можно получить адресную справку, в дальнейшем будет возможно получение еще 42 видов информационных справок».

Очевидно, по этим причинам, процесс легализации биометрии в сфере государственных услуг было решено ускорить и н**ормы по биометрической аутентификации** были внесены в Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об

[17] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=38213728

[18] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=33816084

информатизации»[19] (далее – Закон РК «Об информатизации») уже Законом Республики Казахстан от 25 ноября 2019 года № 272-VI «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам оказания государственных услуг»[20].

В данный закон они попали согласно поправкам депутата Курмановой А.А. с таким обоснованием: «Для законодательного закрепления возможности использования биометрической аутентификации при оказании государственных услуг. Данная поправка направлена на **упрощение процессов получения электронных услуг, идентификации услугополучателя** и защиты персональных данных».

Таким образом, в настоящее время в Законе РК «Об информатизации» уже присутствует понятие «**биометрическая аутентификация** - комплекс мер, идентифицирующих личность на основании физиологических и биологических неизменных признаков». Также указано: «Для получения государственных и иных услуг в электронной форме посредством веб-портала «электронного правительства» и абонентского устройства сотовой связи субъекты получения услуг в электронной форме могут использовать одноразовые пароли или **биометрическую аутентификацию** в соответствии с законодательством Республики Казахстан».

А вот рассматриваемые в данном разделе поправки по какой-то причине оказались оторваны от Проекта и теперь дополняют ранее принятые нормы. То есть, речь в целом идет чисто о юридической технике.

В то же время хотелось бы, чтобы при дальнейшей разработке указанных норм, учитывались принципы, одобренные Казахстаном на международном уровне.

Так, например, в Решении Совета глав правительств Содружества Независимых Государств от 28 октября 2016 года «О Стратегии сотрудничества государств – участников СНГ в построении и развитии информационного общества на период до 2025 года и Плане действий по ее реализации» (город Минск)[21] говорится, что необходимым условием для введения в государствах - участниках СНГ паспортно-визовых и иных идентификационных документов нового поколения является принятие национальных законодательных и иных нормативных правовых актов, определяющих:

- … меры по защите прав и свобод человека и гражданина при фиксации биометрических данных и последующей автоматизированной обработке информации о гражданах, а также принципы контроля системы хранения биометрических данных о гражданах;
- полномочия, ответственность и взаимодействие органов исполнительной власти, участвующих в создании и эксплуатации информационных систем, а также изготовлении, оформлении и контроле паспортно-визовых и иных идентификационных документов нового поколения;
- порядок доступа к информации, содержащейся в системе;
- состав и содержание информации о гражданах, вносимой в паспортно-визовые и иные идентификационные документы нового поколения, порядок ее документирования, обработки, хранения, использования и защиты.

В Соглашении о сотрудничестве в создании государственных информационных систем паспортно-визовых документов нового поколения и дальнейшем их развитии и

[19] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=33885902
[20] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=33267657
[21] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=35479587

использовании в государствах-участниках СНГ (г. Кишинев, 14 ноября 2008 года)[22] говорится, что **биометрические данные** это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (цифровая фотография, отпечатки пальцев, изображение радужной оболочки глаз и другие биометрические персональные данные), которые могут обрабатываться **только при наличии согласия в письменной форме** субъекта персональных данных, в соответствии с законодательством государств-участников настоящего Соглашения.

При создании государственных информационных систем Стороны должны соблюдать следующие условия:

- фиксирование биометрических данных граждан без унижения достоинства личности и причинения вреда здоровью;
- исключение возможности незаконного воспроизведения биометрических данных граждан, содержащихся в паспортно-визовых документах нового поколения;
- обеспечение конфиденциальности информации, содержащейся в государственной информационной системе, и ограничение этой информации только теми сведениями, которые необходимы для проверки подлинности паспортно-визовых документов нового поколения;
- обеспечение доступа граждан к содержащейся в государственной информационной системе информации о них в соответствии с требованиями национального законодательства государств-участников настоящего Соглашения.

В Протокольном решении Экономического совета Содружества Независимых Государств от 15 марта 2019 года «Об обеспечении прав потребителей в сфере электронной торговли в государствах – участниках СНГ»[23] подчеркивается, что основные риски использования биометрических данных для аутентификации пользователей заключаются в том, что **в случае потери или кражи такой информации ее невозможно обновить**. Можно поменять пароль, если его украли, или перевыпустить банковскую карту, если она была скомпрометирована. Но отпечатки пальцев или сетчатку глаза «перевыпустить» уже не получится. **Компрометация каких-либо биометрических данных приведет к невозможности их безопасного использования в дальнейшем**.

3. Нормы о Национальной системе видеомониторинга

«Статья 36-1. Национальная система видеомониторинга

1. Национальная система видеомониторинга является информационной системой, представляющей собой совокупность программных и технических средств, осуществляющих сбор, обработку и хранения видеоизображений для решения задач обеспечения национальной безопасности и общественного правопорядка.

2. Не допускается использование сведений, полученной Национальной системой видеомониторинга для решения задач, не предусмотренных пунктом 1 настоящей статьи.

3. Категории объектов, подлежащих обязательному подключению к Национальной системе видеомониторинга являются:

[22] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=30401084

[23] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=32562697

1) системы видеонаблюдения центральных государственных и местных исполнительных органов;

2) системы видеонаблюдения объектов, уязвимых в террористическом отношении;

3) системы видеонаблюдения общественной и дорожной безопасности.

Перечень объектов, подлежащих обязательному подключению к Национальной системе видеомониторинга определяется Комитетом национальной безопасности Республики Казахстан, по согласованию со Службой государственной охраны Республики Казахстан.

4. Пользователями Национальной системы видеомониторинга являются специальные государственные органы и органы внутренних дел.

Перечень служб, подразделений и категорий сотрудников, имеющих право пользования Национальной системой видеомониторинга определяется руководителями специальных государственных органов и органов внутренних дел.

Сведения, полученные в результате функционирования Национальной системы видеомониторинга могут предоставляться иным государственным органам, в случаях определенным Законами.

5. Правила функционирования Национальной системы видеомониторинга определяются Комитетом национальной безопасности.»;

Как уже упоминалось выше, Постановлением Правительства Республики Казахстан от 12 декабря 2017 года № 827 «Об утверждении **Государственной программы «Цифровой Казахстан**»[24], для обеспечения безопасности, упрощения и развития цифровых услуг, в том числе государственных, социальных и коммерческих, предполагается построить модель **удаленной идентификации, в том числе основанной на различных биометрических показателях**, исходя из принципов рискориентированного подхода. Модель предполагает идентификацию клиентов с использованием базы данных государственных и коммерческих компаний, а также получение сервиса государственными органами, коммерческими компаниями и в социальной сфере (образование, здравоохранение, перепись населения и другие).

В Концепции Проекта[25] относительно разработки данной нормы говорилось следующее. В соответствии с протоколом совещания №18-01-7.13дсп от 15 ноября 2018 года под председательством Первого Президента Республики Казахстан - Елбасы, Правительству Республики Казахстан совместно с КНБ и Службой государственной охраны поручено с учетом реализации государственной программы «Цифровой Казахстан» принять меры по созданию в республике **единой системы интеллектуального видеонаблюдения с выработкой унифицированных технических требований к соответствующему оборудованию**.

На сегодняшний день, в Казахстане насчитывается большое количество систем видеонаблюдения, в том числе предусмотренных в рамках концепции «Smart City».

Владельцами систем видеонаблюдения являются разные государственные органы, а также частные организации, что затрудняет специальным государственным и правоохранительным органам оперативно реагировать при розыске преступников и обеспечить безопасность в различных ситуациях, в то же время данными системами генерируется большой объем видеоданных, в том числе персональные данные.

[24] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=37168057

[25] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=33400415

При этом, действующие требования законодательства РК по обработке и хранению персональных данных недостаточно эффективны. Также отсутствуют единые требования по ввозу, установке и эксплуатации систем видеонаблюдения и видеоанализа на территории РК, вследствие чего возникают риски утечки информации. Имеют место факты, когда некоторые виды чувствительной информации (данные видеонаблюдения, сведения о передвижении на транспорте и т.п.) не могут быть отнесены к категории «персональных данных», т.к. не соответствуют определению, установленному законодательством.

В целях повышения уровня информационной безопасности и урегулирования процессов защиты персональных данных в сфере обработки видеоинформации представляется целесообразным реализовать **комплекс правовых, организационных и технических мер по созданию национальной системы видеомониторинга**.

Также в Концепции говорится: «Технологию ИИ на основе больших данных возможно применить правоохранительным органам, **различные камеры** на дорогах и в зданиях позволяют **проводить высокоточную аналитику и оповещать о подозрительных действиях злоумышленников органы безопасности, для превентивных мер**».

В Заключении [26] научной экономической экспертизы Проекта было отмечено, что законопроектом предусматривается расширение компетенций Государственной технической службы в части обеспечения функционирования Национальной системы видеомониторинга. Согласно законопроекту, данная система будет состоять из системы видеонаблюдения центральных государственных и местных исполнительных органов, системы видеонаблюдения объектов, уязвимых в террористическом отношении, системы видеонаблюдения общественной, городской и дорожной безопасности. На сегодняшний день, по информации государственного органа-разработчика данная система не функционирует. Помимо этого, не разработаны правила функционирования Национальной системы видеомониторинга.

Создание Национальной системы видеомониторинга, поддержка функционирования может потребовать средств государственного бюджета. Однако государственным органом-разработчиком не проведена оценка влияния данной нормы на параметры государственного бюджета. Государственному органу-разработчику необходимо провести расчеты затрат согласной вводимой норме.

В Экспертном заключении Национальной палаты предпринимателей Республики Казахстан «Атамекен» также говорилось, что передача данных систем видеонаблюдения финансовых учреждений Национальной системе видеомониторинга нарушает банковскую тайну, страховую тайну, тайну вкладов и ведет к нарушению функционирования финансовой системы.

Однако вышеуказанные замечания экспертов не повлияли на содержание рассматриваемой нормы в Проекте.

Поскольку пользователями Национальной системы видеомониторинга являются **специальные государственные органы и органы внутренних дел**, важно сразу отметить следующие нормы Закона РК «О персональных данных и их защите».

В соответствии с ними, **биометрические данные** - это персональные данные, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на основе которых **можно установить его личность**.

[26] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=33400415

Само по себе видеоизображение не является носителем персональных данных, так как не способно служить для однозначной идентификации личности, если на видеозаписи присутствует лишь изображение некоего человека. Таким образом, **при отсутствии процедуры идентификации личности**, видеоизображения граждан не могут считаться биометрическими персональными данными. Но если в системе используется **система распознавания лиц**, в которой изображению присваивается идентификатор, можно было бы применить нормы закона.

Однако, согласно статье 3 Закона РК «О персональных данных и их защите», его **действие не распространяется** на отношения, возникающие при сборе, обработке и защите персональных данных в ходе разведывательной, контрразведывательной, оперативно-розыскной деятельности, а также осуществлении охранных мероприятий по обеспечению безопасности охраняемых лиц и объектов в пределах, установленных законами Республики Казахстан. А к специальным государственным органам относятся **органы национальной безопасности, уполномоченный орган в сфере внешней разведки, Служба государственной охраны Республики Казахстан**[27]. Таким образом, нормы Закона РК «О персональных данных и их защите», включая согласие субъектов и прочие меры по защите персональных данных, на их деятельность, связанную с использованием Национальной системы видеомониторинга, распространяться не будут вообще.

Что касается **органов внутренних дел**, то они относятся к правоохранительным органам, которые могут осуществлять **сбор, обработку персональных данных без согласия субъекта или его законного представителя** (статья 9 Закона РК «О персональных данных и их защите»).

При этом представляется, что функционирование Национальной системы видеомониторинга возможно только при условии, что это не противоречит базовым, прописанным в Конституции правам граждан (в частности, на неприкосновенность частной жизни).

Право неприкосновенности частной жизни – понятие более широкое, чем категория «персональные данные». В статье 17 Международного пакта о гражданских и политических правах (МПГПП)[28] формулировка этого права обозначена так: «*Никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств*». МПГПП был ратифицирован Республикой Казахстан[29], вступил в силу для РК 24 апреля 2006 года и имеет приоритет перед её законами (пункт 3 статьи 4 Конституции РК[30]).

---

[27] Статья 3 Закона Республики Казахстан от 13 февраля 2012 года № 552-IV «О специальных государственных органах Республики Казахстан»
ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=31123483

[28] См.: Международный пакт о гражданских и политических правах. Принят резолюцией 2200 А (XXI) Генеральной Ассамблеи от 16 декабря 1966 года. Вступил в силу 23 марта 1976 года // Сайт Организации Объединённых Наций. URL: http://www.un.org/russian/documen/ convents/pactpol.htm.

[29] Закон Республики Казахстан №91-III от 28 ноября 2005 года «О ратификации Международного пакта о гражданских и политических правах»// ИС «Параграф» URL:
https://online.zakon.kz/Document/?doc_id=30035423

[30] См.: Конституция Республики Казахстан. Принята на республиканском референдуме 30 августа 1995 г. / ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=1005029

В статье 18 Конституции РК говорится[31]: «*1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства. Ограничения этого права допускаются только в случаях и в порядке, прямо установленных законом*». Конституция не исключает допустимость ограничения этого права в соответствии с п. 1 ст. 39.

В **Послании Конституционного Совета Республики Казахстан от 9 июня 2017 года № 09-2/5 «О состоянии конституционной законности в Республике Казахстан»** в очередной раз отмечалось, что: «Необходимо также **законодательное раскрытие понятия «неприкосновенность частной жизни»**, на что неоднократно обращали внимание правоохранительные и специальные государственные органы (Послание Конституционного Совета от 12 июня 2012 года № 09-3/1)» [32].

В ряде нормативных постановлений Конституционный совет указывал, что закон, ограничивающий конституционные права и свободы человека и гражданина, должен соответствовать требованиям юридической точности и предсказуемости последствий, то есть его нормы должны быть сформулированы с достаточной степенью четкости и основаны на понятных критериях, позволяющих со всей определенностью отличать правомерное поведение от противоправного, исключая возможность произвольной интерпретации положений закона (от 27 февраля 2008 года № 2, от 11 февраля 2009 года № 1, от 7 декабря 2011 года № 5, от 11 июня 2014 года № 2 и другие).

Думается, что представленные формулировки по функционированию Национальной системы видеомониторинга не в полной мере соответствуют принципам ясности, точности, конкретности, определённости, соразмерности, законности ограничений права частной жизни, определенным **Сиракузскими принципами толкования ограничений и отступлений от положений Международного пакта о гражданских и политических правах**[33].

В ст. 144 Гражданского кодекса Республики Казахстан (далее - ГК РК) (Общая часть)[34] говорится, что **раскрытие тайны личной жизни** возможно лишь в случаях, установленных законодательными актами. Право на личную тайну является естественным правом человека, принадлежит каждому в силу рождения и относится к нематериальным благам, направленным на неприкосновенность внутреннего мира человека и его интересов. Внутренний мир человека характеризует его частную жизнь[35]. Таким образом, под личной тайной понимается право индивида определять своё поведение в обществе, самостоятельно регулировать режим информации и требовать от иных лиц соблюдения этих прав.

В статье 145 ГК РК также закреплено **право на собственное изображение**: «Никто не имеет право использовать изображение какого-либо лица без его согласия».

---

[31] См.: Экспертный обзор по исполнению государственными органами Республики Казахстан Национального плана РК в области прав человека на 2009-2012 г.г. Раздел: Право на частную жизнь и защиту персональных данных за период 2009-2012 гг. (Лоскутов И.Ю.) // Сайт «Zakon.kz». URL: https://pravo.zakon.kz/4460665-jekspertnyjj-obzor-po-ispolneniju.html

[32] 33764294

[33] См.: Сиракузские принципы толкования ограничений и отступлений от положений Международного пакта о гражданских и политических правах. Документ ООН E/CN.4/1985/4, Приложение (1985) // ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=30449593

[34] См.: Гражданский кодекс Республики Казахстан (Общая часть). Принят Верховным Советом Республики Казахстан 27 декабря 1994 года ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=1006061

[35] См. Научно-практический комментарий к Конституции Республики Казахстан (Конституционный совет Республики Казахстан, 2010 г.) // ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=31064937

Важен учет этих норм, поскольку Национальная система видеомониторинга будет осуществлять сбор, обработку и хранения видеоизображений, а кодексы (в том числе ГК РК) в юридической иерархии имеют приоритет на обычными законами, каким, например, является Закон Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан»[36].

А ГК РК в отношении использования изображения без согласия не делает никаких исключений, наподобие тех, что есть в ч. 1 ст. 152.2 Гражданского кодекса РФ. В ней указано, что согласие на получение и использование изображения гражданина не требуется, когда наблюдение ведётся в государственных или общественных интересах, в общедоступных местах и на публичных мероприятиях («за исключением случаев, когда такое изображение является основным объектом использования)[37]. В Казахстане схожие нормы недавно приняты лишь в отношении СМИ, но на уровне закона и не в отношении специальных или правоохранительных органов.

Отсутствие соответствующих национальных норм заставляет нас обратиться к международному опыту, т.к. необходимо изучить практику применения технологий в других странах и выработать безопасные регламенты обработки видеоинформации.

Так, на сегодня, Европейский союз рассматривает возможность запрета технологии распознавания лиц в общественных местах на срок до пяти лет, чтоб дать время выработать способы предотвращения злоупотреблений, связанных с использованием основанных на этой технологии систем[38]. Калифорния стала первым штатом в США, где ввели запрет на использование технологий распознавания лиц полицейскими и другими правоохранительными органами. Власти отметили, что они могут рассмотреть снятие запрета после того, как технологию можно будет контролировать[39].

В тоже время, КНР, наоборот, предлагает Казахстану шире внедрять данные технологии. **Все действующие уже в Казахстане видеокамеры вместе с более современными могут быть объединены в единую систему для поддержания общественной безопасности,** сообщил вице-президент по общественной безопасности компании Huawei Надим Абдулрахим 5 апреля 2019 года на «День Huawei»**[40]**. «Для этого мы создали видеооблако. Во всех городах у вас уже есть действующие системы видеонаблюдения в аэропортах, на дорогах, в торгово-развлекательных центрах, местах скопления народа и так далее. Все эти действующие системы были развернуты в течение многих лет, значительные инвестиции были направлены, поэтому их нужно использовать, но их нужно использовать для нужд многих органов государственной власти, внутренних дел, национальной безопасности, дорожной полиции и так далее. Есть много различных органов, отвечающих за поддержание порядка и что для них нужно, какой функционал? Чтобы они могли смотреть это видео, проигрывать это видео, им необходимо, чтобы у них был доступ к этой базе видеоматериалов, и они также должны обладать функционалом аналитики», - сказал он. «Например, (можно получить) госномера автомобилей, идентификацию по лицам. Вся эта информация находится у нас в базах данных для того, чтобы в последующем ее можно было анализировать», - сказал **Абдулрахим**. «В частности, по каждой попавшей в кадр автомашине фиксируется марка, цвет и госномер. Если же лица человека, попавшего в кадр видеокамеры пока нет в базе данных, то будут использованы внешние параметры, которые также пригодятся в будущем при его

[36] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=31106860
[37] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=30396612
[38] https://www.rbc.ru/politics/17/01/2020/5e21dee19a794767254d9c10
[39] https://hightech.fm/2019/10/19/california-face
[40] https://kursiv.kz/news/kompanii/2019-04/kitay-gotov-podelitsya-tekhnologiyami-videoslezheniya-s-kazakhstanom

поиске.... «Потом если мы будем искать какого-то человека, который носит красный свитер, мы сможем найти этого человека по меткам метаданных. Эта информация будет храниться у нас не только в виде видео, но и в виде потока метаданных. Когда мы проводим анализ потом, мы проводим анализ меток метаданных для того, чтобы найти что нам необходимо по транспортным средствам, полу, людям, возрасту, по тому, что они носят и так далее», - сказал представитель компании. Абдулрахим отметил, что система способна также сама определить часто появляющихся в определенных местах людей и отнести их к «праздношатающимся».

В докладе «**Право на приватность в цифровую эпоху**» Верховного комиссара ООН по правам человека от 16 июля 2014 года[41] говорится:

– международное право предусматривает универсальные основы и механизмы для соблюдения права на неприкосновенность частной жизни;

– однако, как выяснилось, во многих странах не разработано адекватное национальное законодательство, надлежащие процессуальные гарантии и механизмы эффективного надзора, что приводит к **произвольному или незаконному вмешательству** в право на частную жизнь;

– при рассмотрении проблем, связанных с обеспечением права на неприкосновенность частной жизни, необходимо обратить особое внимание на два фактора:

(1) постоянное совершенствование технологий и появление новых возможностей слежки;

(2) **отсутствие прозрачности** в деятельности правительств, связанной с политикой наблюдения, что затрудняет усилия по оценке этой деятельности и её согласованию с международными принципами обеспечения прав человека.

Также следует упомянуть, что Специальный докладчик Организации Объединённых Наций (ООН) по вопросу о поощрении и защите права на свободу мнений и их свободное выражение, Представитель Организации по безопасности и сотрудничеству в Европе (ОБСЕ) по вопросам свободы СМИ, Специальный докладчик Организации американских государств (ОАГ) по вопросам свободы выражения мнения и Специальный докладчик по вопросам свободы выражения мнения и доступа к информации Африканской комиссии по правам человека и народов (АКПЧ) еще в 2015 году[42] отмечали следующее:

a. … **скрытая слежка может проводиться только ограниченно и целенаправленно**, таким образом, чтобы соблюдался соответствующий баланс между необходимостью, с одной стороны, обеспечить соблюдение закона и поддержания безопасности, а с другой стороны, обеспечить право на свободу выражения мнения и неприкосновенность частной жизни. Нецелевая или «массовая» слежка по своей сути непропорциональна и является нарушением прав на неприкосновенность частной жизни и свободу выражения мнения.

b. Подобным образом, требования хранить или практика хранения персональных данных **на неизбирательной основе в целях обеспечения соблюдения закона или поддержания безопасности не являются легитимными**. Персональные данные могут храниться для целей обеспечения соблюдения закона или поддержания безопасности только на ограниченной и целевой основе и таким образом, чтобы был соблюдён соответствующий баланс между необходимостью обеспечения соблюдения закона и

[41] См.: Итоговый доклад Верховного комиссара ООН по правам человека Н. Пиллэй «Право на приватность в цифровую эпоху», 16 июля 2014 года // Сайт Управления Верховного комиссара ООН по правам человека. URL: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/ Session27/Documents/A.HRC.27.37_en.pdf

[42] Совместная декларация о свободе выражения мнения и реагировании на ситуации конфликта (Рига, 4 мая 2015 года)// ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=34622054

поддержания безопасности и правами на свободу выражения мнения и неприкосновенность частной жизни.

c. Государства должны всегда обеспечивать **полную прозрачность** в вопросах, касающихся систем скрытой слежки, включая соответствующие правовые и политические основания.

d. Должен иметь место адекватный **независимый надзор за системами скрытой слежки**, в том числе за органами власти, непосредственно занимающимися проведением слежки.

В **Резолюции Генеральной Ассамблеи Организация Объединенных Наций от 14 ноября 2018 года № A/C.3/73/L.49/Rev.1** «Право на неприкосновенность частной жизни в цифровую эпоху»[43] *вновь подтверждается* право человека на неприкосновенность частной жизни, в соответствии с которым никто не должен подвергаться произвольному или противоправному вмешательству в его или ее личную и семейную жизнь и произвольным или противоправным посягательствам на неприкосновенность жилища или тайну корреспонденции, а также предусмотренное законом право на защиту от такого вмешательства или таких посягательств и признавая, что осуществление права на неприкосновенность частной жизни имеет большое значение для реализации права свободно выражать свои мнения и беспрепятственно придерживаться своих убеждений и права на свободу мирных собраний и свободу ассоциации и является одной из основ демократического общества. В ней также *отмечается,* что, хотя использование метаданных может иметь свои преимущества, некоторые виды метаданных, при их агрегировании, могут раскрывать информацию личного характера, которая может быть не менее чувствительной, чем содержание сообщений, и может давать представление о поведении, социальных связях, индивидуальных предпочтениях и личности человека.

Подчеркивается, что: государства должны выполнять международные обязательства в области прав человека, касающиеся права на неприкосновенность частной жизни, при перехвате частных цифровых сообщений и/или сборе персональных данных, а также в случаях, когда они делятся собранными данными или иным образом предоставляют доступ к ним, в частности на основании соглашений об обмене информацией и разведывательными данными, или когда они требуют раскрытия персональных данных третьими сторонами, включая частные компании,

Отмечая активизацию сбора чувствительной биометрической информации, получаемой от частных лиц, и подчеркивая, что государства должны соблюдать свои обязательства по правам человека и коммерческие структуры должны уважать право на неприкосновенность частной жизни, право на наивысший достижимый уровень физического и психического здоровья и другие права человека при сборе, обработке, передаче и хранении биометрической информации, и в этих целях, в частности, рассматривать вопрос о принятии норм и гарантий, касающихся защиты данных, ГА ОНН *приветствует* добровольно принимаемые коммерческими структурами меры по информированию своих клиентов о тех правилах, которым они следуют в отношении запросов государственных органов, касающихся предоставления доступа к данным и информации о клиентах, *будучи глубоко обеспокоена* тем, что слежение за сообщениями и/или их перехват, включая экстерриториальное слежение за сообщениями и/или их перехват, а также сбор персональных данных, особенно в массовом масштабе, могут иметь негативные последствия для осуществления и реализации прав человека:

1. вновь подтверждает право на неприкосновенность частной жизни, в соответствии с которым никто не должен подвергаться произвольному или противоправному вмешательству в его или ее частную и семейную жизнь и произвольным или

[43] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=36838318

противоправным посягательствам на неприкосновенность жилища или тайну корреспонденции, а также право на защиту со стороны закона от такого вмешательства или таких посягательств, как это предусмотрено в статье 12 Всеобщей декларации прав человека и статье 17 Международного пакта о гражданских и политических правах;

…

3. подтверждает, что права, которые люди имеют в офлайновой среде, включая право на неприкосновенность частной жизни, должны защищаться и в онлайновой среде;

4. напоминает, что государства должны обеспечить, чтобы при любом ограничении права на неприкосновенность частной жизни принимались во внимание законность, необходимость и соразмерность такого ограничения;

6. *призывает* все государства:

c) регулярно пересматривать свои процедуры, практику и законодательство, касающиеся слежения за сообщениями, их перехвата и сбора персональных данных, включая массовое слежение, перехват и сбор, в целях защиты права на неприкосновенность частной жизни путем обеспечения полного и эффективного выполнения всех своих обязательств по международному праву в области прав человека;

f) рассмотреть вопрос о разработке или продолжении и обеспечении выполнения, в сотрудничестве со всеми соответствующими заинтересованными сторонами, включая гражданское общество, надлежащего законодательства, предусматривающего эффективные санкции и соответствующие средства правовой защиты, для защиты лиц от нарушений и ущемлений права на неприкосновенность частной жизни, заключающихся в **противоправном и произвольном сборе, обработке, хранении или использовании персональных данных частными лицами, правительствами, коммерческими структурами и частными организациями**.

В GDPR под термином «**биометрические данные**» понимаются персональные данные, возникающие в результате особой технической обработки, касающиеся физических, физиологических или поведенческих характеристик физического лица, которые предусматривают или подтверждают уникальную идентификацию указанного физического лица, например, изображение лица человека или дактилоскопические данные.

Согласно статье 9 регламента, **обработка биометрических данных для однозначной идентификации физического лица должна быть запрещена**. Эта норма не применяется в ряде случаев, в т.ч. если: «(g) обработка необходима по причинам **особого общественного интереса** на основании законодательства, которое должно быть **пропорционально** преследуемой цели, должно **соответствовать сущности права** на защиту данных и предусматривать **приемлемые и конкретные меры** для защиты основных прав и интересов субъекта данных;»[44].

В **Декларации Комитета министров Совета Европы от 22 апреля 2020 года** отмечается, что законы, позволяющие государствам собирать, использовать и хранить персональные данные, должны строго соответствовать праву на неприкосновенность частной жизни, защищенному как национальными конституционными положениями, так и прецедентным правом Европейского суда по правам человека и Суда Европейского союза, а действия, предпринимаемые органами государственной власти, должны подлежать **независимому надзору**[45].

[44] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=39559334

[45] https://www.kommersant.ru/doc/4332762

Согласно действующему Приказу исполняющего обязанности Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 10 июля 2019 года № 152/НҚ «Об утверждении **Методических рекомендаций к построению «умных» городов»**[46], в систему видеомониторинга города должны входить:

1) системы видеонаблюдения в местах массового скопления людей;
2) внутри дворовые системы видеонаблюдения;
3) системы уличного видеонаблюдения (остановки, пешеходные переходы, тротуары);
4) системы видеонаблюдения в государственных учреждениях (школы, поликлиники, больницы, ЦОНы);
5) системы видеонаблюдения коммерческих организаций (магазины, гостиницы, ломбарды);
6) системы видеофиксации нарушений ПДД и видеонаблюдения на дорогах;
7) системы видеонаблюдения в общественных транспортных средствах.

Внедряемые системы **должны интегрироваться в Национальную систему видеомониторинга** (НСВМ) на уровне МИО (Местный исполнительный орган) и должны обеспечивать непрерывную передачу видеопотока в Центр оперативного управления.

Система видеомониторинга на уровне МИО должна быть централизованной и обеспечивать резервирование, иметь возможность подключения удаленных пользователей и возможность масштабируемости.

Системы, внедряемые в централизованную систему видеомониторинга должны иметь открытый платформо-независимый API для интеграции с внешними системами для объединения всех камер, датчиков и сенсоров, тревожных кнопок, терминалов экстренного вызова и выполнять установленные требования Уполномоченных органов.

Технологические требования к камерам устанавливаются в Единых технических требованиях к системам видеонаблюдения Уполномоченным/курирующим Государственным органом. Требования к видеоаналитике устанавливаются курирующим Уполномоченными/курирующим Государственным органом в рамках построения Национальной системы видеомониторинга».

Отметим также, что Постановлением Правительства Республики Казахстан от 6 декабря 2019 года № 908 «О реализации Закона Республики Казахстан «О республиканском бюджете на 2020 - 2022 годы»[47] предусмотрено выделить на развитие автоматизированной информационной системы Министерства внутренних дел Республики Казахстан «**Биометрическая идентификация личности**» на 2020 год 12 124 179 тыс. тенге и на 2021 год 2 062 692 тыс. тенге.

Судя по этим нормам, создание Национальной системы видеомониторинга уже идет и без законодательного обеспечения.

При этом, в **Концепции информационной безопасности Республики Казахстан до 2016 года**[48] констатировалось, что проверки состояния защищенности государственных баз данных, включенных в состав «электронного правительства», указывают на отсутствие адекватного правового, организационного и технического режима защиты персональных

[46] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=36679134
[47] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=36362178
[48] См.: Указ Президента Республики Казахстан №174 от 14 ноября 2011 года // ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=31086318

данных граждан. За это время не поступало сведений о том, что данный вопрос полностью закрыт, более того, всплыл на поверхность целый ряд новых инцидентов информационной безопасности в государственных органах.

Предложения:

Согласно пункту 5 Правил организации законопроектной работы в уполномоченных органах Республики Казахстан, утвержденных постановлением Правительства Республики Казахстан от 29 декабря 2016 года № 907[49], изложение аргументов, свидетельствующих о необходимости принятия законодательного акта, должно быть конкретным, обстоятельно устанавливающим связь негативных явлений и процессов с недостаточно эффективным действующим законодательством. В качестве аргументации необходимо приводить примеры из правоприменительной практики с указанием краткой фабулы имевшихся ситуаций, выводы и предложения.

Однако, в Проекте не приводится никаких аргументов из правоприменительной практики, устанавливающих связь негативных явлений и процессов с отсутствием Национальной системы видеомониторинга. В связи с чем необходимо четко обозначить цели ее создания, а также соответствие этих целей конституционному праву на неприкосновенность частной жизни, праву на собственное изображение.

Для приведения казахстанского законодательства в соответствие с международными стандартами в области защиты права на частную жизнь, необходимо также дать адекватные ответы на вопросы: будет ли храниться собираемая информация только для достижения определенных целей или неопределенный срок?

Необходимо подтверждение, что это не механизм тотальной слежки с технологией распознавания лиц с интегрированной базой персональных и биометрических данных граждан.

А для этого нужен общественный контроль хотя бы со стороны независимого органа по защите персональных данных.

На основании изложенного, предлагается установить определенный срок для введения рассматриваемой нормы, чтоб дать время выработать необходимые правовые механизмы предотвращения возможных злоупотреблений, связанных с использованием Национальной системы видеомониторинга.

4. Применение сертификатов безопасности интернет-ресурсами

«Статья 56-1. Защита доменных имен в пространстве казахстанского сегмента Интернета.

1. Интернет-ресурс с зарегистрированным доменным именем.KZ и (или).ҚАЗ размещается на **аппаратно-программном комплексе**, который расположен на **территории Республики Казахстан**.

2. Использование доменных имен.KZ и (или).ҚАЗ в пространстве казахстанского сегмента Интернета при **передаче данных интернет-ресурсами** осуществляется с **применением сертификатов безопасности**.»;

В **Концепции Проекта** говорится следующее: «Законопроектом вводится норма, согласно которой интернет-ресурс с зарегистрированным доменным именем.KZ и (или).ҚАЗ должен размещаться на аппаратно-программном комплексе, который расположен на территории Республики Казахстан. Согласно данным государственного органа-

[49] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=39753504

разработчика реализация данной нормы позволит органам внутренних дел устанавливать личность человека, который разместил запрещенную информацию на интернет-ресурсах с зарегистрированным доменным именем. При этом использование доменных имен.KZ и (или).ҚАЗ в пространстве казахстанского сегмента Интернета при передаче данных интернет-ресурсами должно осуществляться с применением сертификатов безопасности. Согласно данным государственного органа-разработчика использование сертификата безопасности позволит **передавать данные по защищенному соединению** между браузером и сервером интернет-ресурса в зашифрованном виде в целях **предотвращения возможного хищения конфиденциальных данных** (персональные данные пользователей, пароли от интернет-ресурсов, платежная информация и т.д.)».

В **Сравнительной таблице** к правительственному Проекту выдвигается такое же обоснование: «Использование сертификата безопасности позволит передавать данные по защищенному соединению между браузером и сервером интернет-ресурса в зашифрованном виде в целях предотвращения возможного хищения конфиденциальных данных (персональные данные пользователей, пароли от интернет-ресурсов, платежная информация и т.д.). Сертификаты безопасности **выпускаются специализированными организациями - удостоверяющими центрами**. Удостоверяющие центры предлагают сертификаты безопасности, как на безвозмездной основе, так и на возмездной. Кроме того, размещение аппаратно-программных комплексов на территории Казахстана позволит активно использовать отечественные центры обработки данных, которые в настоящее время простаивают. Также, поможет органам внутренних дел устанавливать личность человека, который разместил запрещенную информацию на интернет-ресурсах с зарегистрированным доменным именем. Принятие предложенных мер позволит обеспечить развитие безопасного казахстанского сегмента Интернет, а также повысить рейтинг Казахстана в Индексе электронной торговли».

При рассмотрении Проекта в Мажилисе в анализируемой норме слова «на **аппаратно-программном комплексе**, который расположен на территории Республики Казахстан» были заменены словами «в **пространстве казахстанского сегмента Интернета**». И теперь пункт 1 статьи 56-1 представлен в такой редакции: «Интернет-ресурс с зарегистрированным доменным именем.KZ и (или).ҚАЗ размещается в пространстве казахстанского сегмента Интернета».

Поправка является логичной, поскольку, согласно Проекту, **пространство казахстанского сегмента Интернета** - это совокупность интернет-ресурсов, размещаемых на **аппаратно-программных комплексах**, расположенных на территории Республики Казахстан.

По сути же, в Правилах регистрации, пользования и распределения доменных имен в пространстве казахстанского сегмента Интернета[50] давно закреплено требование о том, что **обязательным условием к серверному оборудованию является его физическое место нахождения на территории Республики Казахстан**. Теперь эта норма вынесена на уровень закона.

Однако, действующее определение **аппаратно-программного комплекса** охватывает **совокупность программного обеспечения и технических средств**, совместно применяемых для решения задач определенного типа. Вероятно, теперь уполномоченные государственные органы собираются отслеживать и нахождение программного обеспечения на территории Республики Казахстан. Но как это будет реализовано на практике, пока сложно представить. В недавней истории уже был прецедент, когда РГП «Государственной технической службой» Комитета национальной безопасности

[50] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=35205534

Республики Казахстан был установлен факт нахождения информационно-коммуникационной инфраструктуры (охватывает в т.ч. и аппаратно-программный комплекс) сетевого издания «Ratel.kz» за пределами Республики Казахстан на основании чего, свидетельство о постановке на учет сетевого издания решением уполномоченного органа было признано утратившим силу. Это послужило основанием для судебного спора[51], где из-за нечеткости вышеуказанных формулировок, представители издания не смоги отстоять свою позицию, что не нарушали требование о территориальности.

Что касается применения сертификатов безопасности при передаче данных казахстанскими интернет-ресурсами, то делается это очевидно в реализацию норм Постановления Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении **Концепции кибербезопасности («Киберщит Казахстан»)»**[52], согласно которым доля использования **отечественных сертификатов безопасности** при шифрованной передачи данных Интернет-ресурсами с доменом.KZ и.ҚАЗ в 2018 году составит 20%, в 2019 году - 40%, в 2020 году - 60%, в 2021 году - 80%, в 2022 году - 100%.

Ранее власти пытались провести кампанию по установке казахстанского сертификата безопасности пользователям[53]. 6 августа 2019 года Комитет национальной безопасности РК объявил об успешном завершении тестирования применения сертификата безопасности. Президент РК Касым-Жомарт Токаев сообщил, что проверка действенности сертификата безопасности проводилась по его поручению в **рамках программа «Киберщит»**. Он заверил в защищенности информационного пространства РК, высоком уровне технической оснащенности и в том, что неудобств пользователям РК нет.

Теперь, возможно, бремя использования сертификата переносится на владельцев казахстанских сайтов. Если это повлечет технические трудности для их пользователей, не думается, что это будет способствовать развитию казахстанского сегмента Интернета.

Нужно отметить нечеткость формулировки Проекта – непонятно, **о каких именно сертификатах безопасности идет речь**? Если речь только о том, чтобы казахстанские интернет-ресурсы использовали зашифрованное соединение в принципе, то это хорошая новость для их пользователей в плане безопасности.

Но, возможно, и что имеются в виду сугубо казахстанские сертификаты, выдаваемые через Государственную техническую службу КНБ РК. Ведь именно о них говорится в Концепции кибербезопасности («Киберщит Казахстан»)». Кроме того, работа протоколов, поддерживающих шифрование с применением сертификата безопасности, вполне может подпадать под программное обеспечение, которое должно находиться на территории РК.

В настоящее время, в **Законе Республики Казахстан от 5 июля 2004 года № 567-II «О связи»**[54] имеется понятие «удостоверяющий центр информационной безопасности - юридическое лицо, определяемое Комитетом национальной безопасности Республики Казахстан, **выдающее сертификаты безопасности в электронной форме**». Имеется **Приказ Председателя Комитета национальной безопасности Республики Казахстан от 27 марта 2018 года № 23/нс «Об утверждении Правил выдачи и применения сертификата безопасности»**[55].

---

[51] Решение районного суда № 2 Ауэзовского района города Алматы от 13 июля 2018 года № 2-3847/2018 ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=39662466

[52] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=39754354

[53] Хронология событий по адресу: https://air.org.kz/certificatesecuritykz/

[54] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=1049207

[55] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=36700709

Таким образом, казахстанские операторы связи уже осуществляют пропуск трафика с использованием протоколов, поддерживающих шифрование с применением сертификата безопасности в соответствии с подпунктом 4) пункта 3-1 статьи 26 Закона Республики Казахстан от 5 июля 2004 года № 567 «О связи». Применение сертификата безопасности осуществляется операторами связи в целях ограничения распространения по сети телекоммуникаций информации, запрещенной вступившим в законную силу решением суда или законами Республики Казахстан.

Отсюда возникает вопрос в актуальности и целесообразности применения отечественных сертификатов безопасности казахстанскими интернет-ресурсами. Ведь получается, что операторы связи не смогли с помощью сертификата ограничить распространение по сети телекоммуникаций информации, запрещенной вступившим в законную силу решением суда или законами Республики Казахстан.

А теперь, поскольку речь идет о казахстанских доменах, ничто не мешает сомнительным сайтам мигрировать на другие домены, если их будет эта норма реально обременять.

Предложения:

Согласно пункту 7 статьи 23 Закона Республики Казахстан от 6 апреля 2016 года № 480-V «О правовых актах»[56]: «При необходимости уточнения терминов и определений, используемых в нормативном правовом акте, в нем помещается статья (пункт), разъясняющая (разъясняющий) их смысл». В данном случае видится необходимым четкое толкование в Проекте, о каких именно сертификатах безопасности идет речь. Что это такое и для каких целей они будут применяться.

Необходимо также четкое объяснение того, как именно и в каком составе должен размещаться аппаратно-программный комплексе на территории Республики Казахстан для интернет-ресурсов с зарегистрированным доменным именем.KZ и (или).ҚАЗ. Произвольное толкование данной нормы может служить коррупциогенным факторов, а также давать возможность для произвольного прекращения деятельности интернет-ресурсов, что подтверждают имеющиеся прецеденты.

[56] ИС «Параграф» URL: https://online.zakon.kz/Document/?doc_id=37312788