МЕЖДУНАРОДНО-ПРАВОВОЙ АНАЛИЗ ПРОЕКТА ЗАКОНА РЕСПУБЛИКИ КАЗАХСТАН “О ВНЕСЕНИИ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ В НЕКОТОРЫЕ ЗАКОНОДАТЕЛЬНЫЕ АКТЫ РЕСПУБЛИКИ КАЗАХСТАН ПО ВОПРОСАМ РЕГУЛИРОВАНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ”

Подготовила Ольга Кирилюк
к.ю.н., юрист в сфере международного права
эксперт по вопросам персональных данных, AI, кибербезопасности и цифровых прав человека
спикер международных конференций в Европе, США и Канаде

Прим. – данный проект Закона был подписан Президентом РК 25 июня 2020 г

ОГЛАВЛЕНИЕ

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.

Краткий обзор

Современные цифровые технологии все больше проникают в различные сферы жизни человека, заставляя государства находиться в режиме постоянной адаптации к новым технологическим вызовам. При этом, построение государственной стратегии в сфере цифровых инноваций должно основываться на комплексной оценке рисков и разумном обосновании разрешенных случаев применения технологий, с одновременным предоставлением максимальных гарантий защиты прав человека.

В условиях цифровизации каждый человек становится прозрачным для государства, аккумулирующего огромные объемы персональных данных граждан. При этом сами правительства не всегда открыто заявляют о применении интрузивных цифровых технологий и не объясняют общественности реальные риски.

В связи с все возрастающим использованием видеомониторинга с применением технологии распознавания лиц, биометрической аутентификации, искусственного интеллекта и интернета вещей совершенно объективно возникает вопрос о необходимости их законодательного регулирования. Однако, нормативно урегулировать эту сферу не так просто, поскольку технологии развиваются чрезвычайно быстрыми темпами, что приводит к такой же быстрой потере актуальности законодательными актами. Именно поэтому при разработке последних важно прописывать не конкретные случаи использования технологий, но скорее ключевые принципы и стандарты, которые с высокой вероятностью смогут быть применимы даже к технологиям следующего поколения. Кроме того, трудности разработки национального законодательства в сфере технологий в значительной степени связаны с отсутствием единых международно-правовых стандартов в этой сфере.

Примечательной особенностью проекта закона “О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий” является попытка законодателя совместить в одном документе нормативные нововведения в довольно большое количество законодательных актов, совершенно не связанных друг с другом. Законодательные органы государств постсоветского пространства выработали верный способ лоббирования непопулярных или ограничительных норм путем внесения изменений в уже существующие законы, вместо принятия отдельных нормативно-правовых актов. Это, прежде всего, касается норм, которые могут нести определенные риски для прав человека. Немногие желающие смогут разобраться с объёмным пакетом изменений и дополнений в законодательство, если к тому же они спрятаны за совершенно нейтральным названием проекта закона.

Самое значительное нововведение, предложенные рассматриваемым законопроектом кроется в нормах, направленных на создание национального сегмента Интернета (п. 45-1 ст. 1 и ст. 56-1 Закона “Об информатизации”)[1]. В данном случае речь идет не столько о правовой природе

[1] *Статья 1. Основные понятия, используемые в настоящем Законе*
В настоящем Законе используются следующие основные понятия:
45-1) пространство казахстанского сегмента Интернета - совокупность интернет-ресурсов, размещаемых на аппаратно-программных комплексах, расположенных на территории Республики Казахстан;
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.

и обоснованности предложенных поправок, сколько о том, что с их помощью предпринимается попытка создать свою отдельную, подконтрольную правительству сеть под видом “защиты доменных имен в пространстве казахстанского сегмента Интернета”. На техническом уровне достаточно сложно и затратно полностью изолировать национальный сегмент от глобальной сети, еще более сложно сделать его самодостаточным и обеспечить бесперебойное функционирование. Как правило, сегментацию интернета поддерживают государства с авторитарными режимами, практикующие тотальный мониторинг онлайн активности своих граждан и вводящие существенные ограничения прав человека.

В приведенном обосновании необходимости создания казахстанского сегмента интернета правительство, по существу, не скрывает своих планов локализировать данные и отслеживать онлайн активность граждан, что служит серьёзным тревожным звонком. Прокол HTTPS и технология DNSSEC уже успешно решают ту же задачу, что и предлагаемые сертификаты безопасности национального производства. Существует высокий риск того, что последние будут использованы для перехвата и мониторинга данных соответствующими национальными органами (во всяком случае в отношении Интернет-ресурсов с доменными именами в зоне .KZ и(или) .ҚАЗ, которые должны будут размещаться исключительно на аппаратно-программном комплексе, расположенном на территории Республики Казахстан).[2]

Интернет как глобальная сеть построен на принципах открытости и интероперабельности. Любое вмешательство в его архитектуру считается неприемлемым и потенциально опасным. Здесь вопрос не в том, какие именно сертификаты безопасности собирается использовать правительство, а в том, зачем оно собирается это делать. Данные шаги по законодательному обособлению казахстанского сегмента Интернета аналогичны действиям Российской Федерации по созданию своего локального Рунета. Помимо России созданием национальных сегментов интернета занимаются Китай, Иран и Северная Корея. Такой путь регулирования интернета является сомнительным и опасным, особенно с точки зрения соблюдения международных стандартов в области прав человека. И хотя не существует международно-правовых актов, запрещающих государствам проводить сегментацию интернета, подобные инициативы не находят поддержки международного сообщества. Ведь, как правило, единственным настоящим мотивом государств, стремящихся к созданию обособленного сегмента глобальной сети, является желание тотального контроля над онлайн пространством, включая любые коммуникации и информацию. Национализация интернета, по сути, есть не что иное как попытка ввести всеобъемлющую цензуру, где нет места свободе выражения взглядов и приватности. Внедрение национальных сертификатов будет лишь началом дальнейших ограничений и усиления контроля государства. Учитывая риски, заложенные в предложенные законодательные поправки, направленные на создание национального сегмента интернета, последние должны быть исключены из текста законопроекта. Следует полностью отказаться от такого подхода к регулированию интернета в пользу многостороннего диалога с участием всех заинтересованных сторон (правительства, частного сектора, технического сообщества, гражданского общества).

---

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

[2] Данные опасения связаны с предпринятой властями Казахстана в 2019 году попыткой внедрить национальный сертификат Qaznet Trust Network. Новая инициатива направлена на решение тех же задач путем постепенного распространения требования о наличии национальных сертификатов в национальном сегменте Интернета.

В этом контексте следует обратить особое внимание на необходимость повышения осведомленности общественности в отношении обсуждаемых законодательных инициатив. Кроме того, внедрение новых технологий на государственном уровне должно быть результатом открытых публичных консультаций. Очень важно, чтобы диалог между правительством и общественностью происходил еще на стадии обсуждения законодательных инициатив, оставляя за гражданами возможность влиять на содержание проекта нормативно-правового акта.

Предметом данного анализа являются те нормы законопроекта, которые потенциально могут иметь наибольший эффект на защиту права на приватность и персональных данных. Предложенные законодательные изменения проанализированы в контексте их соответствия международно-правовым стандартам и заложенных в них рисков для прав человека. К каждому разделу приводятся рекомендации для избежания или минимизации предполагаемых рисков.

В целом, вполне обоснованным и целесообразным представляется создание отдельного уполномоченного органа в сфере защиты персональных данных в Республике Казахстан. Наличие такого органа соответствует сложившейся международной практике и служит гарантией обеспечения надлежащего уровня защиты персональных данных на национальном уровне. При этом важно, чтобы создаваемый орган был независимым и самостоятельным. Безусловно, одной статьи закона недостаточно для определения его конкретных функций и полномочий. Поэтому необходимо дополнить законопроект соответствующими нормами, детально регулирующими процедуру создания уполномоченного органа, его деятельность, а также компетенции и полномочия его членов. Кроме того, функция защиты персональных данных как несвойственная органам прокуратуры (но предусмотренная действующим законодательством) должна быть полностью упразднена и передана в новый уполномоченный орган.

Предложенные масштабы внедрения национальной системы видеомониторинга с одновременным использованием технологии распознавания лиц несут в себе огромные риски для прав субъектов данных. Государства, желающие использовать видеомониторинг, должны гарантировать на законодательном уровне полное соответствие предпринимаемых мер международным стандартам и национальным актам в сфере защиты персональных данных, в частности прописать конкретные требования к сбору и обработке данных, максимально ограничить сроки их хранения и постоянно следить, чтобы объем собираемых данных был пропорционален преследуемой цели. Предлагаемая законопроектом поправка не содержит подобных положений. К тому же, в Концепции к проекту закона создание национальной системы видеомониторинга объясняется необходимостью повышения уровня информационной безопасности и урегулирования процедур, связанных с защитой персональных данных. При этом сложно представить, как с такой задачей должна справиться система, предназначенная для сбора биометрических данных, принадлежащих к специальным категориям данных и требующим повышенной защиты. В этой связи было бы целесообразно исключить статью о видеомониторинге из проекта закона до тех пор, пока не будут изучены все риски и преимущества использования этой технологии, проведены общественные консультации и выработан четкий и комплексный подход к этому вопросу.

При создании биометрических баз данных следует уделять особое внимание их надежности и безопасности. Централизованные базы особо уязвимы, поскольку любое несанкционированное вмешательство или технический сбой могут привести к утечке данных, что, в свою очередь, подвергнет неоправданной опасности приватность лиц, которым такие данные принадлежат. Оценка рисков должна проводиться до внедрения и применения любых систем и приложений аутентификации и/или идентификации на основе биометрических данных, при этом конфиденциальность и безопасность должны быть заложены в дизайн таких систем и приложений. В целом же биометрическая аутентификация, предложенная законопроектом, считается одним из самых надежных и достоверных способов идентификации личности. Для избежания незаконного мониторинга на основании предоставленных биометрических данных, субъекты данных должны получить от государства гарантии их исключительно целевого использования.

Что касается искусственного интеллекта (ИИ), то он позволяет значительно оптимизировать некоторые управленческие и образовательные процессы, предоставление услуг, диагностику и лечение заболеваний, как это справедливо отмечено в Концепции к проекту закона. Тем не менее, вызывают обеспокоенность планы законодателя использовать распознавание лиц, отпечатки пальцев и снимок сетчатки глаза как замену для электронной цифровой подписи. В равной степени тревожными являются планы в сфере безопасности, предполагающие применение камер с технологией распознавания лиц, анализ данных из социальных сетей, новостных лент, а также внутренних данных организаций с целью выявления потенциально опасных или требующих внимания действий граждан. Даже такое общее описание свидетельствует больше о намерениях правительства к построению полицейского государства, основанного на тотальном контроле, чем о приверженности соблюдению демократических принципов и наивысших стандартов защиты прав человека. Кроме того, предложенное в проекте закона определение интеллектуального робота сформулировано крайне широко и расплывчато, и вряд ли внесет какую-либо ясность при возникновении реальных правоотношений, связанных с использованием ИИ. При введении любых новых определений в законодательные акты, особенно тех, что связаны с быстро развивающейся сферой технологий, следует руководствоваться практическими ситуациями их применения. Любое новое определение должно привносить юридическую ясность и способствовать формированию четкой правовой базы. К сожалению, в приведенном определении, равно как и в проекте нормы, относящейся к регулированию правоотношений между собственником и владельцем интеллектуального робота, нет четкости и направленности на заполнение конкретных юридических пробелов в аспекте регулирования ИИ.

Нацеленность властей на построение “Интернета всего” может создать значительные риски безопасности критической инфраструктуры страны и значительно снизить ее устойчивость к различного рода кибератакам. Объединение такого большого количества устройств в жизненно важных секторах экономики в случае взлома системы может подорвать жизнедеятельность целых городов и остановить промышленные мощности. К тому же, чем большее влияние на человека оказывает использование устройств, подключенных к Интернету вещей, тем сложнее становится процесс соблюдения приватности и защиты персональных данных. В условиях автоматизации сервисов и услуг в крупных масштабах (умный дом, умные энергосистемы) становятся практически невозможными получение согласия каждого человека на обработку данных, равно как и минимизация собираемых данных.

Среди ключевых рекомендаций, приведенных в анализе, можно выделить следующие:

- При создании уполномоченного органа в сфере защиты персональных данных следует законодательно предусмотреть конкретные требования к его членам, прописать срок их полномочий, процедуру назначения (увольнения), права и обязанности. Также рекомендуется расширить сферу компетенции самого органа и детально прописать его полномочия, гарантируя при этом его независимость и самостоятельность.
- Преимущества применения видеонаблюдения должны в каждом конкретном случае существенно перевешивать риски, связанные со снижением уровня конфиденциальности физических лиц, подпадающих под мониторинг.
- На законодательном уровне должно быть четко прописано что считается достаточным уведомлением о видеомониторинге, какие именно данные могут обрабатываться при применении видеомониторинга, что может служить законным основанием для обработки данных, как долго такие данные могут храниться, кто может получать к ним доступ, необходимость соблюдения конфиденциальности сотрудниками и последствия ее несоблюдения, гарантии предотвращения несанкционированного доступа к персональным данным и их защиты от случайного уничтожения или повреждения, ограничение количества лиц с правом доступа к данным видеокамер, обязательное обучение и повышение квалификации персонала, участие ответственных органов в расследованиях, законные основания для раскрытия данных и т. д.
- Насколько это возможно, обмен данными с камер видеонаблюдения с третьими сторонами, в том числе с другими государственными органами, должен быть запрещен.
- Ответственные государственные органы должны представлять общественности регулярный отчет о случаях использования видеомониторинга и достигнутых результатах, тем самым демонстрируя, что эти технологии не используются дискриминационным, непропорциональным или иным незаконным образом.
- Внедрение систем с использованием биометрических данных должно сопровождаться предоставлением необходимых правовых, процедурных и технических гарантий с целью минимизации вмешательства в личную жизнь. Оценка необходимости и пропорциональности должна проводиться при принятии решений о создании централизованных баз биометрических данных и правил, регулирующих хранение и доступ к ним. Следует избегать создания централизованных систем данных и концентрации всех данных в едином месте. Более надежным считается хранение биометрических данных на смарт-картах или токенах, что способно защитить их от несанкционированного доступа
- Государству следует регулярно пересматривать свои регуляторные политики и нормативные акты в сфере защиты персональных данных, чтобы они оставались актуальными в отношении новых рисков, вызванных быстрым развитием и усовершенствованием биометрических технологий.

Ниже более детально рассмотрены предложенные законодательные изменения и рекомендации касательно их совершенствования.

1. Уполномоченный орган в сфере защиты персональных данных

Предлагаемые изменения в Закон “О персональных данных и их защите”

Статья 27-1. Компетенция уполномоченного органа в сфере защиты персональных данных

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

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

2) разрабатывает правила 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.

2. В отношении персональных данных, ставших известными уполномоченному органу в сфере защиты персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных.

1.1. Международно-правовые акты и стандарты

Надзорные органы, выполняющие свои задачи в условиях полной независимости, являются одним из факторов эффективной защиты физических лиц в отношении обработки данных личного характера.

На сегодняшний день максимальный уровень защиты персональных данных предоставляется Общим регламентом по защите данных (GDPR), принятым в Европейском Союзе (ЕС) и вступившим в силу в мае 2018 года[3]. Акты ЕС в сфере персональных данных являются авторитетным стандартом для обеспечения надлежащего уровня защиты субъектов персональных данных. Соблюдение GDPR обязательно не только для государств-членов ЕС, но и для компаний за пределами ЕС, которые обрабатывают данные граждан ЕС в целях предложения товаров и услуг субъектам данных или мониторинга их поведения, если такое

[3] Общий регламент защиты персональных данных (GDPR) Европейского союза от 27 апреля 2016 года, https://gdpr-text.com/ru/

поведение имеет место в ЕС. Учитывая эти два обстоятельства, а также общую мировую тенденцию на приведение национальных актов в сфере персональных данных в соответствие с GDPR, представляется целесообразным использовать соответствующие положения GDPR в качестве стандартов при разработке изменений в Закон Республики Казахстан "О персональных данных и их защите".

GDPR обязывает государства-члены создать независимый надзорный орган по защите персональных данных (ст. 51 GDPR). При выполнении своих задач и осуществлении своих полномочий члены надзорного органа должны оставаться свободными от любого внешнего вмешательства, а также не должны запрашивать или получать указания со стороны (ст. 52 GDPR). Государство должно обеспечить, чтобы каждый надзорный орган располагал своим собственным персоналом, а также обладал отдельным годовым бюджетом. Процедура назначения членов надзорного органа должна быть максимально прозрачной. Члены могут назначаться парламентом, правительством, главой государства или независимым органом (ст. 53 GDPR). Каждый член надзорного органа должен обладать квалификацией, опытом и знаниями, в том числе в сфере защиты персональных данных, необходимыми для выполнения своих обязанностей и осуществления своих полномочий.

Задача национальных надзорных органов заключается в мониторинге применения законодательства в сфере персональных данных с целью защиты прав физических лиц в отношении обработки их данных. Каждый надзорный орган обязан публиковать годовой отчет о своей деятельности, который может включать, среди прочего, список типов зарегистрированных нарушений и виды предпринятых мер (ст. 59 GDPR).

Еще одним ключевым международно-правовым документом в контексте урегулирования вопросов, связанных с созданием надзорных органов в сфере защиты персональных данных, является модернизированная Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера, разработанная под эгидой Совета Европы и более известная под названием Конвенция 108+[4]. Согласно статье 15 Конвенции надзорные органы обладают следующими полномочиями:

- проведение расследований;
- принятие решений в случаях нарушения положений Конвенции, в частности наложения административных санкций;
- участие в судебном разбирательстве или уведомление компетентных судебных органов о нарушениях положений Конвенции;
- повышение осведомленности контролеров и процессоров о правах субъектов данных и соответствующих обязанностях.

Компетентные надзорные органы должны быть полностью независимы и беспристрастны в своей деятельности. С ними должны проводиться консультации в отношении предложений о любых законодательных или административных мерах, предусматривающих обработку персональных данных. Они также должны обладать механизмом по рассмотрению обращений и жалоб субъектов данных. Как и в случае с GDPR, надзорные органы, создаваемые во исполнение положений Конвенции, должны публиковать периодические отчеты о своей

[4] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Council of Europe, 18 May 2018, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

деятельности. Члены и сотрудники надзорных органов обязаны соблюдать конфиденциальность в отношении информации, к которой они имеют доступ при выполнении своих обязанностей и полномочий. Конвенция предусматривает, что решения надзорных органов могут быть обжалованы в судебном порядке.

В контексте проанализированных выше ключевых международно-правовых актов в сфере защиты персональных данных, вполне обоснованным и целесообразным представляется создание отдельного уполномоченного органа в сфере защиты персональных данных в Республике Казахстан. Наличие такого органа соответствует сложившейся международной практике и служит гарантией обеспечения надлежащего уровня защиты персональных данных на национальном уровне. При этом, критически важно, чтобы такой орган был независимым и самостоятельным. Само намерение создать такой орган уже можно расценивать как позитивный шаг, но, безусловно, одной статьи закона недостаточно для определения конкретных функций и полномочий этого органа. Поэтому необходимо дополнить проект закона соответствующими нормами, детально регулирующими деятельность уполномоченного органа.

Также следует отметить, что функция защиты персональных данных несвойственна органам прокуратуры и должна быть полностью передана в новый уполномоченный орган, в связи с чем следует исключить статью 28 из Закона Республики Казахстан “О персональных данных и их защите”[5].

1.2. Потенциальные риски

Отсутствие компетентного регулятора, равно как и рассредоточенность регуляторных функций между разными государственными органами, не способствует формированию единой правоприменительной практики в сфере защиты персональных данных. Создание уполномоченного органа, напротив, должно привести к усилению контроля за деятельностью лиц, занимающихся сбором и обработкой персональных данных, а также стать гарантией реализации прав и законных интересов субъектами данных. Такие органы несут ответственность за обеспечение соблюдения законов о защите данных на национальном уровне и помогают в толковании этих законов. Ни один закон о персональных данных не может считаться полным, если в нем не предусмотрен надежный механизм обеспечения соблюдения предписанных норм и принципов, который в обязательном порядке включает создание независимого надзорного органа. Даже идеально выписанный закон так и останется декларативным, если надзорный орган не будет наделен необходимыми полномочиями и ресурсами для мониторинга его реализации, проведения расследований и применения санкций в случае нарушения принципов обработки данных и прав субъектов данных.

Примечательно, что роль органов в сфере защиты данных заключается не только в обеспечении соблюдения законов о защите данных и осуществлении надзора, но также в оказании помощи контролерам и процессорам в выполнении их обязанностей. Сотрудничество с уполномоченными регуляторами в сфере защиты данных является важным

[5] Статья 28. Надзор за применением настоящего Закона
1. Органы прокуратуры осуществляют высший надзор за соблюдением законности в сфере персональных данных и их защиты.
2. Акты прокурорского надзора, вынесенные на основании и в порядке, установленных Законом Республики Казахстан “О прокуратуре”, обязательны для всех органов, организаций, должностных лиц и граждан.

шагом на пути к пониманию своих прав и обязанностей со стороны государственных органов, компаний и гражданского общества. Просветительская деятельность играет здесь важную роль, поскольку субъекты данных, как правило, плохо осведомлены о существовании таких органов и сфере их компетенции. Правительства, в свою очередь, должны содействовать работе надзорных органов, объяснять их роль и предоставлять адекватный бюджет для выполнения ими своих обязанностей и полномочий. В противном случае, такие органы так и останутся функционировать лишь на бумаге. Кроме того, правительства сами должны быть заинтересованы в обеспечении защиты и сохранности персональных данных, в частности, когда информация хранится в государственных органах. Любая утечка данных (например, вследствие кибератаки) может подорвать доверие граждан к своему правительству и нанести серьезный ущерб имиджу страны.

1.3. Рекомендации

- При разработке законодательства в сфере защиты персональных данных учитывать все возможные потенциальные риски и злоупотребления в контексте нарушения приватности физических лиц. Для этого процесс создания новых нормативных актов должен быть максимально открытым и инклюзивным, включать стадию публичных консультаций и поощрять вклад всех заинтересованных сторон, особенно гражданского общества.
- При создании уполномоченного органа в сфере защиты персональных данных законодательно предусмотреть:
  - квалификационные требования для назначения в качестве члена надзорного органа;
  - правила и процедуры назначения членов надзорного органа;
  - срок полномочий членов надзорного органа (согласно GDPR – не менее четырех лет);
  - возможность повторного назначения членов надзорного органа;
  - обязанности членов надзорного органа, запреты касательно несовместимых видов деятельности и получения дополнительных выплат в течение срока исполнения полномочий;
  - прекращение полномочий членов надзорного органа;
  - обязательство соблюдения профессиональной тайны членами надзорного органа, как на протяжении, так и после истечения срока их полномочий. В течение срока их полномочий такая обязанность должна применяться в том числе к сообщениям физических лиц о нарушениях их прав.
- Расширить сферу компетенции уполномоченного органа в сфере защиты персональных данных, путем добавления в перечень, предусмотренный статьей 27-1 проекта закона, следующих полномочий (в любом удобном порядке):
  - контролирует и обеспечивает применение настоящего закона и других законодательных актов в сфере защиты персональных данных;
  - консультирует национальные органы власти касательно законодательных и административных мер в сфере защиты прав и свобод человека, касающихся обработки персональных данных;

- содействует повышению осведомленности контролёров и процессоров о возложенных на них обязанностях в соответствии с законодательством в сфере защиты персональных данных;
- утверждает стандартные договорные условия, предусматривающие, в частности продолжительность обработки данных, характер и цель обработки, тип персональных данных, обязанности и права контролера и т. д.;
- составляет и публикует список видов операций по обработке персональных данных, требующих проведения оценки их воздействия на защиту данных;
- поощряет разработку кодексов поведения в сфере обработки персональных данных и утверждает такие кодексы;
- поощряет создание механизмов сертификации, печатей и знаков защиты данных, а также утверждает критерии такой сертификации;
- составляет критерии и проводит аккредитацию органа по осуществлению мониторинга за соблюдением кодексов поведения и органа по сертификации;
- рассматривает жалобы (а не только обращения), поданные субъектами данных;
- проводит расследования касательно соблюдения законодательства в сфере защиты персональных данных;
- содействует информированию общественности о рисках, правилах, гарантиях и правах в отношении обработки персональных данных;
- осуществляет мониторинг законодательных изменений в той части, в которой они влияют на защиту персональных данных, в том числе на развитие информационно-коммуникационных технологий и коммерческих практик.

- Пункт 9 статьи 27-1 проекта закона после слов “осуществляют иные полномочия” дополнить словами “в сфере защиты персональных данных, предусмотренные законами Республики Казахстан, актами Президента Республики Казахстан и Правительства Республики Казахстан”.
- Исключить из компетенции органов прокуратуры функцию высшего надзора за соблюдением законности в сфере персональных данных и их защиты.
- Разграничить компетенцию и полномочия органа в сфере защиты персональных данных путем исключения из перечня, предусмотренного статьей 27-1 проекта закона, пункта 5, который “требует от оператора персональных данных уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных”.
- Дополнить проект закона новой статьей “Полномочия уполномоченного органа в сфере защиты персональных данных” и включить в статью следующие категории полномочий:

1. Полномочия по расследованию
   - требовать от контролёра и процессора предоставления любой информации, необходимой для выполнения задач уполномоченного органа;
   - проводить расследования в форме аудитов защиты данных;

- проводить ревизию сертификатов защиты данных;
- уведомлять контролёра или процессора о предполагаемом нарушении законодательства в сфере защиты персональных данных;
- получать от контролёра или процессора доступ ко всем персональным данным и всей информации, необходимой для выполнения задач уполномоченного органа;
- получать доступ к любым помещениям контролёра или процессора, а также к оборудованию и техническим средствам обработки данных в соответствии с процессуальным законодательством Республики Казахстан.

2. Корректирующие полномочия

- выносить предупреждения контролёру и/или процессору о том, что запланированная обработка данных может нарушать положения законодательства в сфере защиты персональных данных;
- выносить предупреждение контролёру и/или процессору, если обработка данных нарушила положения законодательства в сфере защиты персональных данных;
- требовать от контролёра и/или процессора удовлетворения запроса субъекта данных относительно осуществления его прав согласно законодательства в сфере защиты персональных данных;
- требовать, при необходимости, от контролёра и/или процессора приведения процесса обработки данных в соответствие с положениями законодательства в сфере защиты персональных данных в установленном порядке и в установленный срок;
- требовать, чтобы контролёр сообщил субъекту данных о нарушении безопасности персональных данных;
- наложить временное или окончательное ограничение на обработку данных, включая запрет обработки;
- требовать исправления или уничтожения персональных данных, или ограничения обработки, а также уведомления об указанных действиях получателей, которым были раскрыты персональные данные;
- отозвать сертификат, потребовать от сертификационного органа отзыва сертификата защиты данных, или потребовать, чтобы сертификационный орган не выдавал сертификат, если требования для сертификации не выполняются или перестали выполняться;
- требовать приостановить передачу данных получателю в третьей стране или международной организации.

3. Разрешительные и консультативные полномочия

- консультировать контролёра в порядке предварительной консультации;
- по собственной инициативе или по запросу выдавать национальным органам власти, другим институциям и органам, а также общественности заключения по любому вопросу, связанному с защитой персональных данных;

- выдавать заключение и утверждать проекты кодексов поведения;
- аккредитовать сертификационные органы;
- выдавать сертификаты и утверждать критерии сертификации;
- утверждать стандартные договорные условия по защите данных.

- Включить в текст проекта закона следующие положения:
  - решения, деятельность или бездеятельность уполномоченного органа в сфере защиты персональных данных могут быть обжалованы в судебном порядке;
  - уполномоченный орган обязан уведомить органы судебной власти о факте нарушения законодательства в сфере защиты персональных данных и, в соответствующих случаях, вправе начать судебный процесс или иным образом участвовать в нем в целях обеспечения исполнения положений настоящего Закона и других нормативных актов Республики Казахстан.
  - уполномоченный орган может обладать другими полномочиями, необходимыми для выполнения им возложенных на него функций и обеспечения соблюдения настоящего Закона и других нормативных актов Республики Казахстан в сфере защиты персональных данных.

2. Система национального видеомониторинга (с функцией распознавания лиц)

Предлагаемые дополнения в Закон “Об информатизации”

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:

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.

2.1. Международно-правовые акты и стандарты

Перед запуском любой системы видеонаблюдения следует в первую очередь четко прописать на законодательном уровне каким образом эта система будет функционировать и предполагает ли ее применение сбор, использование или передачу персональных данных третьим сторонам. Большинство современных систем видеонаблюдения собирают изображения людей с целью их дальнейшей идентификации. Правительства, желающие использовать видеомониторинг, должны принять все необходимые меры для обеспечения надлежащего уровня защиты основных прав и свобод человека, в частности предоставить необходимые гарантии защиты персональных данных.

Видеонаблюдение в общественных местах напрямую затрагивает несколько ключевых прав человека, которые защищаются как на международном, так и на национальном уровне, в частности право на неприкосновенность частной жизни, на защиту персональных данных и на свободное передвижение. Так, право на неприкосновенность частной жизни гарантируется статьей 12 Всеобщей декларации прав человека 1948 года, статьей 17 Международного пакта о гражданских и политических правах (МПГПП) 1966 года, статьей 8 Европейской конвенции о правах человека (ЕКПЧ) 1950 года[6] и статьей 7 Хартии основных прав ЕС 2000 года.

Право на защиту персональных данных предусмотрено статьей 8 Хартии основных прав ЕС, статьей 1 GDPR, статьей 9 модернизированной Конвенции Совета Европы о защите частных лиц в отношении автоматизированной обработки данных личного характера 2018 года, а также Руководством Организации экономического сотрудничества и развития (ОЭСР) по защите неприкосновенности частной жизни и трансграничной передаче персональных данных 2013 года.

Кроме того, Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера 1981 года применима к видеонаблюдению даже в тех случаях, когда персональные данные собираются видеокамерами и распространяются в режиме реального времени без создания записи. Видеонаблюдение подпадает под действие Конвенции в той степени, в которой данные, возникающие из звуков и изображений, позволяют идентифицировать лиц при их сопоставлении с другой информацией, в частности с речью, статическими или динамическими изображениями, или другими звуковыми данными.

[6] В значении статьи 8 ЕКПЧ защита персональных данных относится к сфере частной жизни.

Конвенция закрепляет право человека знать о хранении информации о нем и, если необходимо, требовать исправления такой информации[7].

Видеонаблюдение в общественных местах затрагивает также право на свободное передвижение лиц, предусмотренное статьей 13 Всеобщей декларации прав человека, статьей 12 МПГПП, статьей 2 Дополнительного протокола № 4 к ЕКПЧ. Эта свобода касается не только права свободно перемещаться в физическом пространстве, но и права перемещаться без постоянного отслеживания.

Согласно международному праву запрещается произвольное или незаконное вмешательство в личную жизнь (ст. 17 МПГПП). Допустимым считается только то вмешательство, что предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности, или защиты прав и свобод других лиц (ст. 8 ЕКПЧ).

Несмотря на то, что сам факт пребывания в общественном месте предполагает меньшую степень приватности, каждый человек вправе ожидать соблюдения его прав и свобод, в том числе тех, которые связаны с его приватностью и изображением. Сам по себе видеомониторинг далеко не всегда несет угрозу правам человека. Трудности возникают в случаях, когда камеры ведут запись и обработку данных, тем самым создавая незаконное вмешательство в право на неприкосновенность частной жизни, особенно если такие данные были собраны с использованием скрытых методов наблюдения. Еще более неоднозначным является применение видеонаблюдения с встроенной функцией распознавания лиц, что позволяет автоматически и в режиме реального времени идентифицировать человека на основании анализа так называемой лицевой карты, составленной из уникальных черт лица.

Использование биометрических данных, в частности через применение технологии распознавания лиц, влечет за собой повышенный риск для прав субъектов данных. Поэтому крайне важно, чтобы использование таких технологий осуществлялось при должном уважении принципов законности, необходимости, пропорциональности и минимизации данных, изложенных в GDPR.

Видеозапись отдельного человека сама по себе не может рассматриваться как биометрические данные в соответствии со статьей 9 GDPR, если она не была специально технически обработана для идентификации личности. В соответствии с принципом минимизации данных контроллеры должны гарантировать, что данные, извлеченные из цифрового изображения для построения шаблона, не будут чрезмерными и будут содержать только информацию, требуемую для заявленной цели, предотвращая тем самым любую возможность дальнейшей обработки.

В соответствии со статьей 35(1) GDPR контролеры обязаны проводить оценку воздействия планируемых операций обработки на защиту персональных данных в случаях, когда тип обработки данных, в особенности с использованием новых технологий, может привести к высокому риску для прав и свобод физических лиц. Потенциальный риск неправильного использования данных видеомониторинга возрастает в зависимости от масштаба контролируемого пространства и количества людей, посещающих это пространство. В этой

[7] Opinion on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights, Venice Commission, March 2007, https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2007)014-e

связи, в случае систематического видеомониторинга общедоступных мест в крупных масштабах, статья 35(3)(c) GDPR требует проведения оценки его воздействия на защиту персональных данных. А статья 37(1)(b) GDPR предписывает контролерам и процессорам назначать инспектора по защите персональных данных в случаях проведения операций по обработке данных, которые в силу своего характера, объема и/или целей требуют регулярного и систематического мониторинга субъектов данных в больших масштабах.

Цель видеонаблюдения, сводящаяся исключительно к обеспечению безопасности, не является достаточно конкретной в понимании статьи 5(1)(b) GDPR. Более того, видеомониторинг, проводимый без надлежащего уведомления субъектов данных, противоречит принципу законной, справедливой и прозрачной обработки персональных данных в отношении субъекта данных (ст. 5(1)(a) GDPR).

Однако, персональные данные могут обрабатываться посредством видеонаблюдения в соответствии со статьей 6(1)(e) GDPR, если это необходимо для выполнения задачи в общественных интересах или при осуществлении официальных полномочий. Может возникнуть ситуация, когда осуществление официальных полномочий не допускает такой обработки, но существуют и другие законодательные основы, в частности обеспечение здравоохранения и безопасности работников и посетителей, которые могут служить основанием для ограниченной обработки персональных данных. При этом должны соблюдаться права субъектов данных. Государства, желающие использовать видеомониторинг, должны гарантировать на законодательном уровне, что принимаемые меры полностью соответствуют международным стандартам и национальным актам в сфере защиты персональных данных, в частности прописать конкретные требования к сбору и обработке данных, максимально ограничить сроки их хранения и постоянно следить, чтобы объем собираемых данных был пропорционален преследуемой цели.

Согласно европейским стандартам в сфере защиты персональных данных субъекты данных должны быть проинформированы о каждом случае видеонаблюдения за ними. Все места, где ведется видеомониторинг, должны быть помечены специальными информационными знаками. Они должны располагаться примерно на уровне глаз на разумном расстоянии от мест, находящихся под мониторингом, позволяя прохожим своевременно их увидеть и при желании избежать попадания в камеру. Нет необходимости указывать точное местоположение самих камер видеонаблюдения, если информационные знаки позволяют однозначно определить местность, находящуюся под мониторингом. Информационные знаки должны содержать любую информацию, которая может повлиять на решение субъекта данных быть заснятым камерами видеонаблюдения. Такая информация может касаться передачи данных третьим сторонам и периода хранения. Если эта информация отсутствует, субъект данных должен справедливо полагать, что мониторинг проводится исключительно в реальном времени, без какой-либо записи или передачи данных третьим сторонам. Кроме того, сами субъекты данных должны уметь оценивать, какую территорию захватывает камера, чтобы при необходимости адаптировать свое поведение.

Персональные данные не могут храниться дольше, чем это необходимо для целей их обработки (ст. 5(1)(e) GDPR). Государства могут предусмотреть в национальном законодательстве специальные положения о сроках хранения данных видеонаблюдения в случаях, когда обработка необходима для выполнения правового обязательства, возложенного на контролёра, или выполнения задачи в общественных интересах или в рамках осуществления

государственной власти, доверенной контролёру (ст. 6(2) GDPR). Как правило, законными целями видеонаблюдения являются защита собственности или сохранение доказательств. Обычно причиненный ущерб может быть оценен и зафиксирован в течение одного или двух дней. Принимая во внимание принципы, заложенные в статье 5(1)(c) и (e) GDPR, а именно минимизацию данных и ограничение периода хранения, персональные данные в большинстве случаев (например, собранные в целях выявления актов мелкого хулиганства) должны быть удалены через несколько дней. В идеальном случае такое удаление происходит автоматически. Чем длиннее срок хранения данных (особенно более 72 часов), тем больше возникает сомнений в законности и необходимости такого хранения.

В то время как использование видеомониторинга, в том числе оснащённого функцией распознавания лиц, может казаться эффективным средством обеспечения национальной безопасности и общественного правопорядка, правительствам следует прежде всего оценить влияние видеомониторинга на основные права и свободы человека и рассмотреть менее интрузивные альтернативные средства для достижения преследуемой цели.

2.2. Потенциальные риски

В Концепции к проекту закона создание национальной системы видеомониторинга объясняется необходимостью повышения уровня информационной безопасности и урегулирования процедур, связанных с защитой персональных данных. При этом сложно представить, как с такой задачей должна справиться система, предназначенная для сбора биометрических данных, принадлежащих к специальным категориям данных и требующим повышенной защиты. Более того, предполагается, что данные будут собираться в общенациональном масштабе на регулярной основе.

Любые конкретные механизмы реализации предлагаемого нововведения в действующем законодательстве и в проекте закона отсутствуют. В случае принятия законопроекта в настоящем виде, предлагаемая статья либо останется невыполнимой на практике, либо же механизм осуществления видеомониторинга будет прописан в подзаконных правовых актах или актах служебного пользования, что не соответствует принципу транспарентности и в дальнейшем может привести к нарушению прав человека.

Внедрение видеомониторинга в таких масштабах, как предусматривает проект Закона, и, в частности применение технологии распознавания лиц, несут в себе огромные риски. В этой связи было бы целесообразно исключить статью о видеомониторинге из проекта закона до тех пор, пока не будут изучены все риски и преимущества, проведены общественные консультации и выработан четкий и комплексный подход к этому вопросу. Концепция ссылается на опыт Беларуси, ОАЭ, КНР и Великобритании в контексте внедрения централизованных интеллектуальных систем видеонаблюдения и видеоаналитики. Примечательно, что за исключением Великобритании ни одна из этих стран не может считаться образцом демократии, равно как и похвастаться отсутствием нарушений прав человека, в том числе в отношении отсутствия злоупотреблений при использовании цифровых технологий. Та же Великобритания не единожды становилась объектом для критики именно из-за использования полицией систем видеонаблюдения с технологией распознавания лиц.

Следует обратить отдельное внимание на тот факт, что технология распознавания лиц представляет собой особенно интрузивную форму биометрического наблюдения за

человеком, поскольку ее можно использовать дистанционно, без ведома субъекта наблюдения. Избежать слежки практически невозможно, когда такая технология используется в общественных местах. Технология распознавания лиц функционирует на программном обеспечении, которое считывает четкие и специфические черты лица человека для создания подробной биометрической лицевой карты. По аналогии попадание в камеру, оснащенную технологией распознавания лиц, значит то же самое, если бы у человека сняли отпечатки пальцев без его ведома. Отсутствие уведомления о таком видеонаблюдении фактически лишает человека возможности отказаться от вмешательства в его личную жизнь и избежать сбора своих персональных данных. Всеобъятность видеонаблюдения в сочетании с такими технологическими достижениями, как высокое разрешение, увеличение, идентификация и отслеживание, могут легко нарушить баланс между необходимостью использования таких систем и обеспечением конфиденциальности физических лиц.

Кроме того, правительственный видеомониторинг, особенно с применением технологии распознавания лиц с большой вероятностью будет оказывать охлаждающий эффект на реализацию таких прав человека, как свобода выражения взглядов, свобода религии и объединений, право на равное участие в политической и общественной жизни. Зная о том, что невольно можно стать объектом наблюдения, человек будет сознательно прибегать к самоцензуре, чтобы избежать негативных последствий, связанных с его общественной и профессиональной деятельностью, или личными убеждениями. Это вовсе не значит, что человеку на самом деле есть чего бояться, но размытость регулирования, часто сопровождающая проекты по внедрению систем видеомониторинга, создает информационный вакуум и формирует культуру страха. Даже на психологическом уровне понимание человеком того, что он находится под пристальным мониторингом и отсутствие уверенности в том, как его данные могут быть использованы в дальнейшем, заставляют его чувствовать себя как минимум некомфортно.

Отсутствие четких законодательных рамок касательно использования видеомониторинга и технологии распознавания лиц делает возможными потенциальные злоупотребления со стороны различных государственных органов и должностных лиц. Примечательно, что объектами мониторинга становятся не только потенциально опасные члены общества (которые ранее привлекались к уголовной или административной ответственности), но также и люди, которые не совершали или не подозреваются в совершении какого-либо преступления.

Видеонаблюдение и технология распознавания лиц создают вполне реальные риски для прав человека из-за отсутствия прозрачного механизма их использования и высокой чувствительности обрабатываемых данных. Эти технологии дают правительству огромное количество информации, которую оно может использовать для избирательного преследования активистов и несогласных с проводимой политикой, тем самым предупреждая любые протесты и другие способы выражения критики против правящей верхушки.

Полиция и другие органы, которые отвечают за ведение баз данных, собранных с камер видеонаблюдения, концентрируют в своих руках огромные объемы информации и могут отследить практически каждого человека. Если такие данные вовремя не уничтожаются, то можно полностью забыть о праве на приватность. Как правило, внедрение систем видеомониторинга происходит, как и в случае с Казахстаном, под обширным предлогом обеспечения национальной безопасности и правопорядка, но как показали многие

исследования нет никакой связи между всеобъемлющим видеомониторингом и сокращением уровня преступности.[8] Кроме того, до сих пор ни одна система распознавания лиц не дала безошибочных результатов.[9]

Если же внедрение видеомониторинга объективно представляется единственно возможным способом достижения поставленной цели, тогда на законодательном уровне должны быть предусмотрены все необходимые гарантии защиты персональных данных, в частности указаны конкретные цели обработки данных, приведен перечень категорий обрабатываемых данных и прописан четкий период их хранения, а также будут ли эти данные передаваться третьим лицам. Субъекты данных должны быть чётко уведомлены о своих правах, а также проинформированы к каким компетентным органам они могут обращаться за консультацией или с жалобой. Особенно важно избегать централизации всех персональных данных в единых базах и системах с целью предотвращения их утечки, несанкционированного доступа и повышения уровня защищенности и устойчивости к атакам самих данных.

2.3. Рекомендации

- Внедрение системы видеомониторинга, в особенности со встроенной функцией распознавания лиц, должно преследовать четкую цель и быть направлено на решение реальной, существенной и актуальной проблемы. Законным основанием могут служить поддающиеся проверке конкретные случаи массовых преступлений или существенные угрозы безопасности.
- Любые целенаправленные меры видеомониторинга, в том числе в общественных местах, должны быть необходимыми и пропорциональными для достижения законной цели.
- До внедрения системы видеомониторинга должны быть рассмотрены другие, менее интрузивные способы достижения тех же целей. И только в случаях, когда они окажутся значительно менее эффективными или практически невыполнимыми, следует переходить к обсуждению целесообразности и законности применения видеомониторинга.
- Преимущества применения видеонаблюдения должны в каждом конкретном случае существенно перевешивать риски, связанные со снижением уровня конфиденциальности физических лиц, подпадающих под мониторинг. Сокращение операционных расходов (например, за счет сокращения штата полицейских) само по себе не может считаться достаточным основанием для ограничения приватности.
- Потенциальные последствия видеонаблюдения, в частности в виде охлаждающего эффекта на реализацию прав человека, не должны перевешивать потенциальную пользу от использования этой технологии. В связи с этим, до начала внедрения системы распознавания лиц в общественных местах ответственным органам власти необходимо

[8] Noam Biale, ‘What Criminologists and Others Studying Cameras Have Found’, ACLU, https://www.aclu.org/sites/default/files/images/asset_upload_file708_35775.pdf; Paul Bischoff, ‘Surveillance camera statistics: which cities have the most CCTV cameras?’, Comparitech, August 15, 2019, https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/#The_20_most-surveilled_cities_in_the_world

[9] Study finds massive errors in facial recognition tech, Bangkok Post, December 20, 2019, https://www.bangkokpost.com/tech/1820554/study-finds-massive-errors-in-facial-recognition-tech

провести оценку рисков для прав человека и убедиться, что технология прошла проверку на необходимость и пропорциональность.

- Внедрению системы видеомониторинга, в особенности со встроенной функцией распознавания лиц, должны предшествовать общественные консультации, призванные не только информировать общественность о потенциальных нововведениях, но и гарантировать обратную связь. К участию в консультациях должны быть приглашены все заинтересованные стороны.
- На законодательном уровне должно быть четко прописано что считается достаточным уведомлением о видеомониторинге, какие именно данные могут обрабатываться при применении видеомониторинга, что может служить законным основанием для обработки данных, как долго такие данные могут храниться, кто может получать к ним доступ, необходимость соблюдения конфиденциальности сотрудниками и последствия ее несоблюдения, гарантии предотвращения несанкционированного доступа к персональным данным и их защиты от случайного уничтожения или повреждения, ограничение количества лиц с правом доступа к данным видеокамер, обязательное обучение и повышение квалификации персонала, участие ответственных органов в расследованиях, законные основания для раскрытия данных и т. д.
- Камеры следует использовать только для решения конкретно определенных проблем безопасности, сводя к минимуму сбор ненужных данных (принцип минимизации данных). Такой подход не только уменьшает вторжение в частную жизнь, но также помогает обеспечить более целенаправленное и эффективное использование видеонаблюдения.
- Право каждого на информацию в случае видеомониторинга должно удовлетворяться путем размещения уведомления или знаков, информирующих людей об установленных камерах. Такие знаки являются обязательными, поскольку субъекты данных должны быть осведомлены о факте мониторинга, его назначении, продолжительности хранения отснятого материала и ответственных органах.
- Любое внедрение системы видеомониторинга должно сопровождаться технологическими и административными мерами предосторожности для снижения вероятности неправомерного доступа к системе и злоупотреблений при работе с данными.
- Отслеживание и идентификация отдельных лиц на основании данных, полученных системой видеонаблюдения, допустимы только на основании судебного ордера.
- Насколько это возможно, обмен данными с камер видеонаблюдения с третьими сторонами, в том числе с другими государственными органами, должен быть запрещен.
- Все без исключения физические лица, подпадающие под видеомониторинг, должны пользоваться одинаковым уровнем защиты на основании принципа недискриминации.
- Необходимые средства правовой защиты должны быть доступны всем, кто пострадал от неправомерного использования или злоупотребления системами общественного видеонаблюдения.
- Надлежащая просветительская работа должна проводиться для информирования людей о том, как могут применяться законы, какие данные о них могут собираться и как эти данные будут храниться.

- Для избежания злоупотреблений со стороны государственных органов, следует предусмотреть адекватные гарантии и ввести эффективный контроль за испытаниями, приобретением и использованием технологий видеомониторинга.
- Ответственные государственные органы должны представлять общественности регулярный отчет о случаях использования видеомониторинга и достигнутых результатах, тем самым демонстрируя, что эти технологии не используются дискриминационным, непропорциональным или иным незаконным образом.
- Сфера применения видеомониторинга должна ограничиваться лишь теми местами, которые непосредственно связаны с проблемой, на решение которой направлен видеомониторинг (в противовес постоянному общенациональному мониторингу).
- Дополнительная сенсорная информация, такая как звук, не должна записываться, кроме случаев, когда она напрямую необходима для решения заявленной проблемы.
- Записанные данные, которые не были использованы, должны быть стерты согласно утверждённому графику. Срок хранения должен быть ограничен количеством времени, практически необходимым для обнаружения или сообщения об инциденте, произошедшем в контролируемом пространстве.
- Одновременно с запуском системы видеомониторинга правительство должно создать независимый орган контроля, с участием в нем всех заинтересованных сторон (представителей государства, частного сектора, гражданского общества, исследовательских институтов), для осуществления контроля за использованием технологии, оценки достигнутых результатов, детализации рисков и выгод, выявления пробелов в существующей государственной политике и правовом регулировании и т. д.
- Правительство должно вкладывать средства в программы цифровой грамотности, способствующие гражданам в улучшении понимания того, как технологии воздействуют на их жизнь.

3. Биометрическая аутентификация

Предлагаемая поправка в Закон “Об информатизации”

Статья 1. Основные понятия, используемые в настоящем Законе

46-1) биометрическая аутентификация - комплекс мер, идентифицирующих личность на основании физиологических и биологических неизменных признаков.

46-2) верификация биометрических данных - аутентификация новых биометрических данных физического лица с ранее полученными биометрическими данными идентифицирующего физического лица.

Статья 27. Веб-портал и шлюз “электронного правительства”

…

3. 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.*

3.1. Международно-правовые акты и стандарты

На сегодняшний день не существует отдельных международно-правовых актов обязательной силы, посвященных вопросам работы с биометрическими данными. Пока не будут разработаны отдельные правила к этой категории данных применяются общие положения о защите персональных данных. Всеобщая декларация прав человека и МПГПП начинаются со слов о том, что “признание достоинства, присущего всем членам человеческой семьи, и равных и неотъемлемых прав их является основой свободы, справедливости и всеобщего мира”. Злоупотребления в сфере использования биометрических данных могут привести к серьезным рискам для прав человека и нарушить баланс, предписанный основными международно-правовыми актами в этой сфере. В частности, злоупотребление полученными биометрическими данными может привести к нарушению презумпции невиновности и права на справедливое судебное разбирательство.

Первым международным документом, затронувшим вопросы безопасности биометрических данных, стала Конвенция Совета Европы о защите частных лиц в отношении автоматизированной обработки данных личного характера 1981 года (Конвенция 108) и модернизированная в 2018 году (Конвенция 108+). Статья 6 Конвенции 108+ предусматривает, что обработка биометрических данных, позволяющих однозначно идентифицировать человека, допускается только в том случае, если соответствующие гарантии закреплены в законе (в дополнение к тем, что предусмотрены в Конвенции). Такие гарантии должны защищать от рисков, которые может представлять обработка чувствительных данных для интересов, прав и основных свобод субъекта данных, в частности, риска дискриминации.

GDPR определяет биометрические данные как персональные данные, полученные в результате специальной технической обработки, которые касаются физических, физиологических или поведенческих черт физического лица и позволяют однозначно идентифицировать или подтвердить личность (напр., изображение лица или дактилоскопические данные). Статья 9 GDPR запрещает обработку биометрических данных с целью однозначной идентификации физического лица, допуская лишь ограниченное количество исключений из этого правила (напр., четкое согласие субъекта данных, в сфере трудоустройства и социального обеспечения, в отношении публичных данных, из соображений важного общественного интереса). Кроме того, биометрические данные относятся к специальной категории (более чувствительных) персональных данных, нуждающихся в большей защите и требующих проведения оценки рисков, связанных с их обработкой.

Прямое упоминание биометрических данных в тексте обязательного к применению европейского регионального документа является значительным шагом вперед в контексте их защиты.

Право субъектов данных быть информированными означает, как минимум, что они должны получать информацию относительно цели обработки биометрических данных, типа данных, которые будут собираться и использоваться, и (если применимо) информацию об использовании данных для автоматического принятия решений.

3.2. Потенциальные риски

Создание массовых баз биометрических данных вызывает серьезную обеспокоенность в контексте защиты прав человека. Такие данные особенно чувствительны, поскольку они неразрывно связаны с конкретной личностью и ее жизнью, а злоупотребление ими может привести к серьезным нарушениям. Безопасность хранения данных играет чрезвычайно важную роль. Например, последствия от хищения биометрических данных, мошенничество или финансовые потери могут быть невосполнимыми. Биометрические данные человека уникальны и неизменны, и если взломанный пароль доступа можно легко восстановить, то совершенно невозможно изменить похищенные биометрические идентификаторы личности. По сути, украденная биометрия будет считаться украденной навсегда. Человек уже не сможет использовать свои данные для аутентификации своей же личности. Некая обеспокоенность возникает из этических и социальных соображений, в частности в аспекте защищенности частной информации и физической неприкосновенности лиц.

Существенные риски конфиденциальности данных возникают в случаях хранения биометрических данных в централизованных базах, поскольку любое несанкционированное вмешательство или технический сбой могут привести к утечке данных, что, в свою очередь, подвергнет неоправданной опасности приватность лиц, которым такие данные принадлежат. Локальное хранение биометрических данных (например, на чипе биометрического паспорта) позволяет использовать их для аутентификации физического лица (удостоверения, что человек является тем, за кого он себя выдает), но предотвращает их использование в гораздо более интрузивном процессе идентификации (установления личности человека, когда она неизвестна). Сам факт хранения биометрических данных в централизованной системе идентификации может привести к последующей разработке новых обоснований для их использования и расширению доступа к ним органов власти. Также очень важно, чтобы к биометрическим данным при их сборе применялись надежные алгоритмы и сертифицированные технологии шифрования, что позволит предотвратить несанкционированный доступ и будет служить дополнительной гарантией защищенности данных. Сбои в системе могут привести к ошибочной аутентификации личности.

Кроме того, биометрические данные могут использоваться для целей, отличных от тех, для которых они были собраны, включая незаконное отслеживание и мониторинг отдельных лиц. Учитывая эти риски, особое внимание следует уделить вопросам необходимости и пропорциональности при сборе биометрических данных, а также закрепить на законодательном уровне надлежащие правовые и процедурные гарантии. Зачастую во имя национальной безопасности и борьбы с терроризмом государства стремятся предоставить правоохранительным органам и органам безопасности доступ к базам данных, изначально не предназначавшимся для целей борьбы с терроризмом, предотвращения или расследования преступлений. Риски, связанные с несанкционированным доступом к биометрическим данным, также ставят под вопрос эффективность мер по их обработке и использованию, особенно когда такие нарушения своевременно не сообщаются независимым надзорным органам и лицам, чьи законные интересы могли пострадать.

Оценка рисков должна проводиться до внедрения и применения любых систем и приложений аутентификации и/или идентификации на основе биометрических данных, при этом конфиденциальность и безопасность должны быть заложены в дизайн таких систем и приложений.

В целом же биометрическая подпись считается одним из наиболее надежных и достоверных, а также наиболее современных способов аутентификации личности. Некоторые планшеты для забора подписи позволяют не просто захватить цифровое изображение ручной подписи, но также могут собирать информацию, связанную с процессом ее создания – давление, приложенное к кончику стилуса, места, где стилус опускается на страницу и отрывается от нее, форма и закруглённость букв и т. д. Кроме того, могут собираться и другие метаданные, такие как дата и время проставления подписи, местоположение, идентификатор устройства. Самым веским доводом в пользу биометрической подписи считается тот факт, что сами подписи могут быть имитированы, но способ их написания – нет, что позволяет добиться максимально точной аутентификации личности.

3.3. Рекомендации

- Обработка биометрических данных, включая сбор, анализ, хранение и передачу, должна быть предусмотрена законом и ограничена достижением четкой и наглядно необходимой законной цели. Этот закон должен быть достаточно четким и точным, чтобы физические лица могли предвидеть случаи и особенности его применения, а также степень вмешательства в их личную жизнь.
- Внедрение систем с использованием биометрических данных должно сопровождаться предоставлением необходимых правовых, процедурных и технических гарантий с целью минимизации вмешательства в личную жизнь. Оценка необходимости и пропорциональности должна проводиться при принятии решений о создании централизованных баз биометрических данных и правил, регулирующих хранение и доступ к ним. Следует избегать создания централизованных систем данных и концентрации всех данных в едином месте. Более надежным считается хранение биометрических данных на смарт-картах или токенах, что способно защитить их от несанкционированного доступа.
- Создание национальной системы биометрической идентификации само по себе не является законной целью сбора биометрических данных в больших масштабах. В этой связи вызывает тревогу упоминание в Концепции к проекту закона опыта Индии в реализации биометрического проекта Aadhaar, который вызвал серьезную обеспокоенность международных правозащитных организаций.
- На законодательном уровне должны быть предусмотрены основания для обработки биометрических данных, возможность субъектов данных оспаривать в судебном порядке законность запроса на сбор биометрических данных, гарантии безопасности и конфиденциальности данных, срок хранения и порядок удаления биометрических данных из баз данных, независимый механизм для мониторинга процесса сбора и использования биометрических данных, гарантии предотвращения злоупотреблений и обеспечения доступа субъектов данных к эффективным средствам правовой защиты. Следует также четко определить кто несет ответственность и обязательства на разных стадиях разработки, внедрения и обслуживания биометрических систем, а также какими могут быть непредвиденные последствия в краткосрочной, среднесрочной и долгосрочной перспективе.
- Недопустимо неизбирательное хранение персональных данных, включая биометрические данные, поскольку оно не соответствует принципам пропорциональности и необходимости.

В обязательном порядке должны быть установлены временные рамки функционирования системы, а политика хранения данных доступна для общественного ознакомления.

- Государству следует регулярно пересматривать свои регуляторные политики и нормативные акты в сфере защиты персональных данных, чтобы они оставались актуальными в отношении новых рисков, вызванных быстрым развитием и усовершенствованием биометрических технологий. С этой целью могут создаваться специальные консультативные органы с многосторонним и межсекторальным представительством, уполномоченные на разработку рекомендаций касательно этического использования биометрических технологий и регулярное информирование правительства о развитии новых технологий и допустимости их применения.
- В основу любых систем и приложений, функционирующих на основании биометрических данных, должен быть заложен принцип защиты и уважения прав человека. Это также предполагает наличие эффективных средств правовой защиты, доступных физическим лицам, а также независимого уполномоченного органа с функцией контроля за соблюдением государственными органами и частными компаниями законодательства в сфере зашиты персональных данных.
- Для обеспечения безопасности данных рекомендуется хранить отдельно биометрические и корреспондирующие им биографические данные, при этом связи между ними могут быть созданы с использованием технологий шифрования.
- Перед внедрением систем, основанных на биометрических данных, следует проводить оценку их влияния на права человека.
- Персонал, работающий с базами биометрических данных, должен иметь необходимые квалификации и навыки, а также проходить регулярное обучение. Кроме того, должны соблюдаться строгие меры безопасности по предоставлению доступа к таким базам.
- Должен быть разработан механизм немедленного оповещения субъектов данных о любых случаях утечки или нарушения целостности хранимых биометрических данных.
- Должна применяться и регулярно пересматриваться система управления рисками, позволяющая оценить эффективность систем, функционирующих на основании биометрических данных. Это также необходимо в силу уязвимости биометрических систем и их предрасположенности к разного рода умышленным атакам.
- Правительствам следует принимать во внимание тот факт, что любая биометрическая система требует больших капиталовложений и высококвалифицированного персонала. Чем больше объемы обрабатываемых данных, тем больше человеческих ресурсов потребуется, поскольку автоматизированные системы в любом случае требуют человеческого вмешательства на последних стадиях анализа и принятия решения во избежание использования ложных позитивных результатов, сгенерированных системой, как основы для соответствующих решений.

4. **Использование искусственного интеллекта**

Предлагаемая поправка в Закон “О цифровизации”

Подпункт 74) п. 1

“74) интеллектуальный робот - автоматизированное устройство, совершающее определенное действие или бездействие с учетом воспринятой и распознанной внешней среды”.

Предлагаемая поправка в Закон “Об информатизации”

“Статья 18-1. Права и обязанности собственника и владельца интеллектуального робота.

Правоотношения между собственником и владельцем интеллектуального робота регулируются гражданским законодательством РК”.

Концепция к проекту закона

Искусственный интеллект

…

Финансовая сфера

Нейронные сети, в части распознавания изображения, могут быть применены как замена для ЭЦП, то есть при оказании услуг использовать лицо как подпись на получение услуг или как передача своих данных третьим лицам. А также можно рассмотреть применение технологии биометрического анализа человека (отпечатки пальцев, снимок сетчатки глаза). Отпечатки пальцев вместо ЭЦП. Это позволит снизить мошеннические операции и снизить временные издержки на установление личности. Подобную методику применили в Индии, система Aadhaar ИИ возможно применить в аналитике обезличенных пользовательских данных в банковской сфере, для выявления потенциального риска и выдачу рекомендации сотрудникам финансового института.

…

Сфера безопасности

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.

ИИ позволит аккумулировать большой поток информации из социальных сетей, новостных лент, а также внутренних данных организаций и выявлять потенциально опасных или требующих внимания действий населения.

…

4.1. Международно-правовые акты и стандарты

Всевозрастающее использование искусственного интеллекта и автоматизация решений ставит перед правительствами новые регуляторные задачи, решение которых требует принятия во внимание в том числе этических соображений. На сегодняшний день существует достаточно большое количество деклараций, рекомендаций и этических кодексов поведения в сфере искусственного интеллекта (ИИ). При этом, создать универсальные нормы, способные детально урегулировать эту высокотехнологичную и быстро развивающуюся область пока не удалось. Сложность этой сферы сводится не только к ее относительной “молодости”, но в значительной степени объясняется непредсказуемостью ее развития даже в краткосрочной перспективе.

Самая большая трудность в регулировании правоотношений, осложненных использованием ИИ, заключается в отсутствии единого нормативного определения ИИ. Кроме того, требуют нормативного урегулирования вопросы правосубъектности ИИ, ответственности и распределения рисков за вред, причиненный автоматизированными системами ИИ, авторского права на объекты, созданные ИИ без вмешательства человека, патентования алгоритмов и т. д.

Общий регламент по защите данных (GDPR) применяется к ИИ только в том, что касается персональных данных. Документ закрепляет принципы обработки персональных данных – принцип законности, справедливости и транспарентности (ст. 6). При этом, субъект данных имеет право не подвергаться решению, которое основано исключительно на автоматизированной обработке. Исключение составляют лишь три случая, когда такое решение: необходимо для заключения и исполнения договора; разрешено законодательством, содержащим надлежащие меры защиты прав, свобод и законных интересов субъекта данных; основывается на четком согласии субъекта данных. При этом за субъектом данных сохраняются, как минимум, право требовать человеческого вмешательства со стороны контролёра, право выражать свою позицию, а также оспаривать автоматически сгенерированное решение (ст. 22). Кроме того, если обработка персональных данных, в особенности с использованием новых технологий, может привести к высокому риску для прав и свобод физических лиц, контролёр перед началом такой обработки должен провести оценку потенциальных рисков для защиты персональных данных (ст. 35).

Поскольку регламент вступил в силу лишь в мае 2018 года, многие практические моменты его применения еще не до конца изучены. Время покажет насколько эффективна предписанная защита в контексте постоянно возрастающих рисков, связанных с развитием ИИ. Тем не менее, на сегодняшний день GDPR может по праву считаться одним из самых успешных примеров нормативного регулирования вопросов защиты персональных данных, в том числе их обработки системами, основанными на ИИ.

Руководящие принципы в отношении искусственного интеллекта и защиты данных[10], принятые Консультативным комитетом Конвенции 108, содержат перечень базовых мер и рекомендаций, адресованных правительствам, разработчикам, производителям и поставщикам услуг ИИ и направлены на обеспечение надлежащего уровня защиты прав человека, в частности защиты персональных данных. Согласно документу разработка ИИ, основанная на обработке персональных данных, должна соответствовать принципам, прописанным в Конвенции 108+, в частности законности, справедливости, спецификации цели, пропорциональности обработки данных, встроенной конфиденциальности (*by design*) и конфиденциальности по умолчанию (*by default*), ответственности и демонстрации соответствия, транспарентности, безопасности данных и управления рисками. Предписывается также необходимость принятия всех соответствующих мер по предотвращению и снижению рисков ИИ в отношении прав человека. Правительствам рекомендуется разработать кодексы поведения в сфере ИИ и соответствующие сертификационные механизмы. Автономия человека в процессах принятия решений не должна подменяться чрезмерной зависимостью от решений, предложенных ИИ. Кроме того,

[10] Guidelines on Artificial Intelligence and Data Protection, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), 25 January 2019, https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

правительства должны инвестировать ресурсы в цифровую грамотность и образование с целью повышения осведомленности об ИИ и последствиях его применения.

В Руководящих принципах защиты лиц в связи с обработкой персональных данных в мире больших данных, изданных Консультативным комитетом Конвенции 108, приводятся конкретные примеры минимизации рисков для субъектов персональных данных в том, что касается возможных погрешностей при анализе данных, недооценки правовых, социальных и этических последствий использования больших данных при принятии решений, а также маргинализации эффективного и информированного участия людей в этих процессах[11].

В Рекомендации о защите данных о здоровье Комитет Министров Совета Европы советует государствам-членам инкорпорировать в их национальное законодательство и правоприменительную практику следующие принципы: прозрачность, законность и справедливость обработки данных; ограничение сбора данных конкретными и законными целями; необходимость и пропорциональность обработки данных по отношению к законной цели; согласие субъекта данных на обработку данных; адекватность, актуальность и умеренность данных по отношению к заявленным целям; надлежащие меры безопасности для обеспечения сохранности данных и предотвращения несанкционированного доступа. В Рекомендации также описываются законные основания для обработки данных о здоровье (напр., профилактические медицинские цели и медицинская диагностика, общественное здравоохранение, общественный интерес в сфере урегулирования претензий по социальному обеспечению и медицинскому страхованию и т. д.). Специальное внимание в документе уделяется данным о внутриутробных детях, генетическим данным, связанным со здоровьем, а также обмену данными в целях предоставления медицинского обслуживания. Отдельные разделы посвящены правам субъектов данных, медицинским исследованиям и сбору данных о здоровье с помощью мобильных устройств[12].

В ноябре 2019 года Комитет экспертов по правозащитным аспектам автоматизированной обработки данных и различных форм искусственного интеллекта (MSI-AUT), созданный в рамках Совета Европы, опубликовал проект рекомендаций о влиянии алгоритмических систем на права человека[13]. В документе приводится определение алгоритмических систем как приложений, которые часто используя методы математической оптимизации, выполняют одну или несколько задач, таких как сбор, объединение, очистка, сортировка, классификация и анализ данных, а также выбор, приоритизацию, предоставление рекомендаций и принятие решений. Функционируя на основании одного или нескольких алгоритмов для выполнения заданных требований в конкретных условиях их применения, алгоритмические системы автоматизируют действия таким образом, чтобы создавать масштабируемые адаптивные услуги в реальном времени. В проекте рекомендаций четко указывается на необходимость своевременной, на этапе предложения о разработке, оценки рисков использования алгоритмической системы по отношению к правам человека (праву на справедливое судебное

[11] Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 23 January 2017, https://rm.coe.int/16806ebe7a

[12] Recommendation CM/Rec (2019)2 of the Committee of Ministers to member States on the protection of health-related data, 27 March 2019, https://www.apda.ad/sites/default/files/2019-03/CM_Rec%282019%292E_EN.pdf

[13] Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, November 2019, https://rm.coe.int/draft-recommendation-of-the-committee-of-ministers-to-states-on-the-hu/168095eecf

разбирательство, неприкосновенность частной жизни и защиту персональных данных, свободу мысли, совести и религии, свободу выражения взглядов, свободу собраний и т. д.).

В документе отдельно упоминаются случаи полной или частичной зависимости функций, традиционно выполняемых государственными органами (напр., в транспортной или телекоммуникационной сфере), от алгоритмических систем, поставляемых частными компаниями. Любой отказ поставщиков от предоставления оборудования и его обслуживания может привести к снижению качества и/или эффективности таких услуг либо к полнейшему их приостановлению. Государства, в свою очередь, должны обеспечить непрерывность предоставления таких услуг независимо от их коммерческой жизнеспособности, особенно в тех случаях, когда субъекты частного сектора доминируют на рынке и диктуют свои правила поведения. Это примечание может быть особенно актуально для Казахстана в контексте развёртывания городской системы видеонаблюдения Sergek и анонсированного применения технологии FacePay для оплаты проезда в общественном транспорте.

Согласно проекту рекомендаций, процесс разработки любых регуляторных политик и законодательства в сфере алгоритмических систем должен быть прозрачным, понятным и инклюзивным. Государствам предписывается регулярно консультироваться со всеми соответствующими заинтересованными сторонами и теми субъектами, чьи интересы потенциально могут быть затронуты в случае принятия нормативных изменений. Алгоритмические системы должны подвергаться регулярной оценке их влияния на права человека. Государства наравне с другими стейкхолдерами (частный сектор, гражданское общество) должны проводить соответствующую просветительскую деятельность с целью повышения грамотности населения в контексте использования алгоритмических систем.

Государства должны гарантировать, что любое проектирование, разработка и применение алгоритмических систем предоставляют людям возможность заранее получать информацию об обработке их данных (включая понимание ее целей и возможных последствий) и механизмы контроля за использованием их данных. Кроме того, во исполнение своих обязательств согласно Европейской конвенции о защите прав человека, государства должны предоставить в распоряжение граждан эффективные средства правовой защиты в случае нарушения их прав в связи с использованием алгоритмических систем.

Проект рекомендаций MSI-AUT содержит обязательства не только государств, но и частных компаний, что очень важно в контексте обеспечения комплексного подхода к защите прав человека в контексте использования алгоритмических систем. Несмотря на то, что на данный момент документ еще находится на стадии разработки и не был официально утвержден, есть все основания полагать, что он будет принят. Уже сейчас документ можно использовать в качестве инструкции при разработке национального законодательства в сфере ИИ. Заложенные в текст рекомендаций принципы являются универсальными по своей природе и могут быть применены безотносительно к региону и стране.

Хартия этических принципов использования искусственного интеллекта в судебных системах, разработанная Европейской комиссией по эффективности правосудия (ЕКЭП) Совета Европы, стала первым европейским документом в этой сфере. Среди пяти ключевых принципов – уважение основных прав; недискриминация; качество и безопасность; прозрачность, беспристрастность и справедливость; пользовательский контроль. Хартия также содержит

исследование с конкретными примерами использования ИИ в судебных системах, в частности в приложениях, обрабатывающих судебные решения и данные[14].

В сентябре 2019 года Комитет министров Совета Европы принял решение создать Специальный комитет по искусственному интеллекту (CAHAI), уполномоченный рассмотреть возможности разработки правовых рамок в отношении ИИ на основании проведения многосторонних консультаций[15]. Первое пленарное заседание комитета состоялось в ноябре 2019 года и было в основном посвящено организационным вопросам его деятельности[16]. Вторая встреча должна была состояться вначале марта, но была отложена из-за кризиса, вызванного COVID-19.

Не оставила ИИ без своего внимания и Европейская Комиссия, в рамках которой была создана Группа экспертов высокого уровня по вопросам ИИ и подготовлено исследование, в котором, среди прочего, были представлены рекомендации органам, занимающимся разработкой регуляторной политики на национальном уровне и в рамках ЕС. Любой регуляторной инициативе должен предшествовать анализ рисков, связанных с использованием ИИ. При этом, чем выше риски, тем жестче должен быть подход к регулированию. Следует избегать излишне предписывающего регулирования, вместо этого отдать предпочтение регулированию, основанному на принципах, регулярном мониторинге и контроле за исполнением. Участие в разработке соответствующих регуляторных политик в сфере ИИ должны принимать все заинтересованные стороны. Помимо этого, рекомендуется регулярно проводить оценку существующего законодательства на предмет предоставления адекватного уровня защиты прав человека в контексте использования ИИ, а также необходимости принятия новых регуляторных актов для своевременного ответа на вновь возникшие риски[17].

Вопросы, связанные с разработкой и использованием ИИ, также активно изучаются в рамках Организации экономического сотрудничества и развития (ОЭСР). В феврале 2019 года Экспертная группа по искусственному интеллекту, в состав которой вошли более 50 представителей из 20 стран мира, Европейской Комиссии, ЮНЕСКО, частных компаний, передовых мировых исследовательских центров и университетов – Института инженеров по электротехнике и электронике, Массачусетского института технологий, Центра исследований интернета и общества имени Беркмана Кляйна Гарвардского университета и Французского института исследований в области компьютерных наук и автоматизации, опубликовала Рекомендации касательно ИИ, утвержденные государствами-членами ОЭСР в мае 2019 года и более известные как Принципы ОЭСР в сфере ИИ[18]. Наличие такого разностороннего представительства в составе участников экспертной группы свидетельствует о том, что глобальное влияние ИИ на все страны и регионы мира требует формирования глобального

[14] European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment, European Commission for the Efficiency of Justice (CEPEJ), 3-4 December 2018, https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

[15] Ad hoc Committee on Artificial Intelligence (CAHAI) - Terms of reference, 11 September 2019, CoE Committee of Ministers, Council of Europe Portal, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016809737a1

[16] Abridged Meeting Report, Ad Hoc Committee on Artificial Intelligence (CAHAI), 18-20 November 2019, https://rm.coe.int/cahai-2019-07-abridged-report-1st-plenary-meeeting-eng/168099029b

[17] Policy and Investment Recommendations for Trustworthy AI, Independent High-Level Expert Group on Artificial Intelligence, European Commission, 26 June 2019, https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence

[18] Recommendation of the Council on Artificial Intelligence, Organisation for Economic Cooperation and Development, 22 May 2019, https://one.oecd.org/document/C/MIN(2019)3/FINAL/en/pdf

консенсуса и универсальных подходов к регулированию этой стремительно развивающейся сферы.

В рекомендациях приводятся основные определения (система ИИ, жизненный цикл системы ИИ, знания, субъекты и стейкхолдеры ИИ), а также содержатся принципы ответственного управления заслуживающим доверия ИИ (инклюзивный рост и устойчивое развитие, ориентированность на человеческие ценности, справедливость, прозрачность и понятность, надежность и безопасность, подотчетность) и рекомендуемые приоритеты для формирования национальной политики (инвестирование в исследования и разработки в области ИИ, содействие созданию благоприятной цифровой экосистемы и регуляторной среды для ИИ, наращивание человеческого потенциала и подготовка к преобразованию рынка труда) и международного сотрудничества в сфере заслуживающего доверия ИИ.

Содержащиеся в Рекомендации принципы стали первыми международными стандартами в сфере ИИ, согласованными на межправительственном уровне. Помимо государств-членов ОЭСР, к Принципам присоединились также Аргентина, Бразилия, Колумбия, Коста-Рика, Перу и Румыния. Рекомендации ОЭСР не имеют обязательной юридической силы, но, как правило, используются правительствами в качестве международных стандартов при разработке соответствующего национального законодательства[19]. Универсальность разработанных принципов позволяет использовать их в качестве базы для формирования регуляторных политик и принятия нормативных актов по вопросам ИИ по всему миру.

Принципы в сфере ИИ, разработанные ОЭСР, легли в основу одноименного документа, принятого странами “Большой двадцатки” (G20) в июне 2019 года. Страны-члены G20 договорились о развитии человекоориентированного ИИ с одновременным соблюдением всех существующих гарантий приватности и защиты персональных данных[20].

4.2. Потенциальные риски

Главные риски, связанные с использованием ИИ, касаются соблюдения норм, направленных на защиту основных прав и свобод человека (в особенности права на приватность, защиту персональных данных и недискриминации) и предоставления надлежащих гарантий безопасности и эффективных средств правовой защиты. Эти риски могут возникать из-за недостатков в дизайне систем искусственного интеллекта (в том числе в отношении человеческого контроля), выхода из-под контроля, умышленного использования в преступных целях или из-за отсутствия возможности исправления обнаруженных недостатков в алгоритмах анализа данных (например, система обучается с использованием исключительно или преимущественно данных, полученных от мужчин, что приводит к неоптимальным результатам в отношении женщин – предвзятость на основании пола). Технологии на базе ИИ (напр., распознавание лиц) очень часто нарушают границы частной жизни человека и подвергают людей мониторингу в режиме реального времени, как правило, без надлежащего уведомления о ведении такого мониторинга. Всегда существует потенциальный риск того, что ИИ будет использован государственными органами или частными структурами для массовой слежки. ИИ анализирует большие объемы данных и выявляет связи между ними, что может быть использовано для отслеживания и деанонимизации данных о физических лицах, тем

[19] OECD Principles on AI, Organisation for Economic Cooperation and Development, https://www.oecd.org/going-digital/ai/principles/
[20] G20 AI Principles, Annex, 8-9 June 2019, https://www.mofa.go.jp/mofaj/files/000486596.pdf

самым создавая новые риски в контексте защиты персональных данных (даже в отношении наборов данных, которые сами по себе не включают персональные данные). Невозможно также полностью исключить риск принятия ИИ необъективных решений на основании анализа больших данных.

Технологии ИИ могут вызывать появление новых рисков в отношении безопасности пользователей, когда они встроены в продукты и услуги. Например, в результате ошибки в технологии распознавания объектов автомобиль автономного управления может ошибочно идентифицировать объект на дороге и спровоцировать аварию с травмами и материальным ущербом. Эти риски могут быть вызваны недостатками в дизайне технологии ИИ, проблемами с доступностью и качеством данных или с другими недостатками, вытекающими из машинного обучения. Некоторые риски не уникальны для продуктов и услуг на основании ИИ, но именно использование ИИ может увеличить или усугубить эти риски. Отсутствие четких законодательных положений по безопасности ИИ, направленных на устранение этих рисков, может создавать юридическую неопределенность для предприятий, которые продают свои продукты с использованием ИИ. Органы контроля и правоохранительные органы могут оказаться в ситуации, когда необходимо немедленно устранить риск или воспрепятствовать его возникновению, но у них будут отсутствовать полномочия действовать или необходимые технические возможности. Таким образом, правовая неопределенность может снизить общий уровень безопасности и подорвать конкурентоспособность компаний.

Постоянный рост количества “умных” устройств, подключенных к интернету, значительно повышает их уязвимость к различного рода кибератакам. Поэтому критически важно, чтобы развитие технологий шифрования и кибербезопасности происходило в том же темпе, что и развитие ИИ.

Отсутствие унифицированного регулирования ИИ, как на международном, так и на региональном уровне, а также предрасположенность систем ИИ к оптимизации заложенных в них процессов и принятию автономных решений приводит к существенным сложностям в установлении правосубъектности и привлечению к ответственности в случаях причинения вреда. Предложенное в проекте закона определение интеллектуального робота как “автоматизированного устройства, совершающего определенное действие или бездействие с учетом воспринятой и распознанной внешней среды” сформулировано крайне широко и расплывчато, и вряд ли внесет какую-либо ясность при возникновении реальных правоотношений, связанных с использованием ИИ. При введении любых новых определений в законодательные акты, особенно тех, что связаны с быстро развивающейся сферой технологий, следует руководствоваться практическими ситуациями их применения. Любое новое определение должно привносить юридическую ясность и способствовать формированию четкой правовой базы. К сожалению, в предложенном определении, равно как и в проекте нормы, относящейся к регулированию правоотношений между собственником и владельцем интеллектуального робота, нет четкости и направленности на заполнение конкретных юридических пробелов в аспекте регулирования ИИ.

Особенное внимание следует уделить защите персональных данных при их использовании и анализе системами, основанными на ИИ. Субъекты персональных данных должны быть уведомлены о любом случае утечки их данных вследствие сбоев систем ИИ. В основу таких систем должен быть заложен принцип защиты персональных данных.

Безусловно ИИ позволяет значительно оптимизировать некоторые управленческие и образовательные процессы, предоставление услуг, диагностику и лечение заболеваний, как это справедливо отмечено в Концепции к проекту закона. Тем не менее, вызывают обеспокоенность планы законодателя использовать распознавание лиц, отпечатки пальцев и снимок сетчатки глаза как замену для ЭЦП. В предыдущем разделе уже были проанализированы риски в отношении прав человека, связанные с биометрической аутентификацией. При этом, совершенно необязательно собирать биометрические данные, которые не являются необходимыми для предоставления услуги. Так, в случае с подписью, специальное оборудование позволяет запечатлеть не только электронный снимок подписи человека, но и сам процесс ее нанесения для дальнейшей аутентификации.

В равной степени тревожными являются планы в сфере безопасности, предполагающие применение камер с технологией распознавания лиц, анализ данных из социальных сетей, новостных лент, а также внутренних данных организаций с целью выявления потенциально опасных или требующих внимания действий граждан. Даже такое общее описание свидетельствует больше о намерениях правительства к построению полицейского государства, основанного на тотальном контроле, чем о приверженности соблюдению демократических принципов и наивысших стандартов защиты прав человека.

ИИ в сочетании с большими объемами публично доступных персональных данных (напр., из социальных сетей) способен делать достаточно подробные выводы о людях, проводя их категоризацию, что, в свою очередь, может существенно усилить существующие формы дискриминации, сегрегации и маргинализации общества. На основании анализа цифровых отпечатков людей может осуществляться их профайлинг, что в дальнейшем может оказать самое непосредственное влияние на их жизнь (напр., для принятия решений о благонадежности граждан, их праве на получение ипотеки или услуг в области здравоохранения).

Особенно подвержены рискам, связанным с использованием ИИ, лица, которые в силу своего возраста или низкого уровня цифровой грамотности могут быть не осведомлены об опасностях эксплуатации персональных данных. В зону риска также попадают дети, лица, принадлежащие к маргинализованным общинам, а также активные пользователи интернета, которые оставляют особенно большой цифровой отпечаток.

4.3. Рекомендации

- Правительство должно обеспечить создание правовой основы для использования ИИ в различных секторах промышленности и сферах жизни человека, а также гарантировать безопасность продуктов и услуг на основе ИИ, желательно на уровне дизайна систем ИИ. Кроме того, должны быть предусмотрены четкие критерии установления вины и процедура эффективного устранения ущерба в случаях его нанесения ИИ без человеческого вмешательства.
- Проанализировать и оценить существующее законодательство в сфере персональных данных с точки зрения наличия достаточных гарантий для соблюдения права на уважение частной жизни и защиту личных данных при использовании систем ИИ. При выявлении пробелов в регулировании внести необходимые изменения в законодательство.

- Оценка рисков должна проводиться перед выпуском продукта на рынок, при внесении изменений в дизайн продукта, а также периодически для анализа автономного поведения ИИ на протяжении всего срока использования продукта.
- Следует прописать конкретные требования к прозрачности и надежности алгоритмов, а также условие присутствия человеческого надзора, что особенно важно для дальнейшего исполнения сгенерированных ИИ решений и укрепления доверия к использованию этих технологий.
- Запретить разработку, внедрение и использование автономных систем ИИ, функционирующих без контроля человека.
- Правительству следует инициировать открытые и инклюзивные публичные консультации с целью формирования позиции касательно того, где проходит грань между допустимым использованием данных, полученных на основании анализа, проделанного ИИ, и недопустимым манипулированием на основании сгенерированных данных (например, профайлинг населения по принципу благонадежности в целях получения социальной помощи или кредитов).
- Правительства должны уделять надлежащее внимание и предоставлять необходимые ресурсы для развития цифровой грамотности населения и повышения осведомленности общественности о том, когда и как применяются системы ИИ (особенно при оказании государственных услуг), сколько данных генерируется и обрабатывается персональными устройствами, сетями и платформами с помощью специально натренированных алгоритмических процессов.
- Обеспечить соблюдение открытых стандартов закупок и прозрачные процедуры использования систем ИИ.
- Создать независимый и эффективный механизм контроля за соблюдением прав человека в системах ИИ с достаточными полномочиями и знаниями в этой сфере.
- Избегать профайлинга лиц, принадлежащих к определенным группам, при использовании систем ИИ.

5. Интернет вещей

Рекомендации по развитию технологии в Казахстане из Концепции к проекту закона:

1. Государственным организациям рекомендуется выработать единые стандарты развития технологии…

2. Предлагаем рассмотреть вопросы содействия локализации производства датчиков и сенсоров казахстанского производства …

… Есть смысл задаться вопросом по внедрению смарт систем в малых городах по принципу автоматизации и создания экосистемы первоочередных услуг для населения, так как проблема автоматизации услуг остается. Это позволит местным исполнительным органам видеть картину происходящего в режиме реального времени, и соответственно реагировать и принимать соответствующие меры.

…

4. Местным исполнительным органам при построении структуры "Smart city" необходимо учитывать направление создания единой инфраструктуры. В настоящее время нет единых стандартов развития "Smart city".

…

Предлагается рассмотреть построение структуры исходя из общепринятых для каждого города услуг для автоматизации и создание экосистемы "Интернета вещей".

…

При построении структуры "Интернет вещей", следует учесть, что все города и "Промышленный интернет вещей" можно будет интегрировать в одну уникальную сеть - "Интернета всего".

Нацеленность на построение "Интернета всего" может создать значительные риски безопасности критической инфраструктуры страны и значительно снизить ее устойчивость к различного рода кибератакам. Объединение такого большого количества устройств в жизненно важных секторах экономики в случае взлома системы может подорвать жизнедеятельность целых городов и остановить промышленные мощности. В случае автоматизации и диджитализации сферы услуг, очень важным становится обеспечение непрерывности и доступности услуг на основе Интернета вещей, а также внедрение механизмов безопасности, препятствующих возникновению эксплуатационных сбоев и перебоев в работе. Например, централизованные системы более уязвимы и подвержены атакам, поскольку даже выведение из строя одного элемента может заблокировать деятельность всей системы. В связи с этим еще на стадии разработки систем на основе Интернета вещей следует закладывать в их дизайн принципы информационной безопасности, конфиденциальности и защиты персональных данных.

Чем большее влияние на человека оказывает использование устройств, подключенных к Интернету вещей, тем сложнее становится процесс соблюдения приватности и защиты персональных данных. В условиях автоматизации сервисов и услуг в крупных масштабах (умный дом, умные энергосистемы) становятся практически невозможными получение согласия каждого человека на обработку данных, равно как и минимизация собираемых данных. Увеличение объемов собираемых данных может вызвать проблемы с аутентификацией и спровоцировать кризис доверия к устройствам Интернета вещей. Кроме того, информация об одном человеке, собранная из нескольких объектов, подключенных к Интернету вещей, делает этого человека значительно легче идентифицируемым и, следовательно, уязвимым.

Еще один риск заключается в том, что данные, которые были собраны с одной целью, могут быть использованы также и в других целях, несовместимых с соблюдением прав человека, а также переданы третьим лицам. Также существует высокий риск того, что люди добровольно и сами того не осознавая будут предоставлять свои данные и становиться объектом постоянного мониторинга в обмен на удобство и быстроту сервисов и услуг, основанных на Интернете вещей. Помимо этого, созависимость устройств, подключенных к Интернету вещей, будет негативно сказываться на возможности потребителей изменить поставщика услуг Интернета вещей, что фактически ограничивает контроль человека над своими данными и его право свободно выбирать поставщиков услуг. Автоматизированные решения, принимаемые Интернетом вещей, со временем будут создавать у человека ощущение потери контроля над своей жизнью.

При разработке регуляторных политик и правового регулирования в сфере Интернета вещей следует ориентироваться на два основных принципа: во-первых, использование Интернета вещей не должно нарушать неприкосновенность и достоинство человека, а также права человека на частную жизнь и защиту персональных данных; во-вторых, физические лица должны иметь возможность контроля над своими данными, созданными или обработанными на основе Интернета вещей.

Кроме того, при внедрении технологии Интернета вещей правительствам следует уделить должное внимание вопросам технических стандартов и технической совместимости устройств, необходимости лицензирования отдельных устройств, наличия достаточного радиочастотного спектра и IP-адресов.

Любое внедрение современных высоких технологий в государственную практику требует тщательного предварительного изучения контекста, природы предлагаемых технологических решений, их необходимости, пропорциональности, ориентированности на права человека, сопутствующих рисков, а также наличия альтернативных, менее интрузивных и более безопасных для частной жизни человека решений.