Глава 10. Правовые основы формирования электронного правительства в Таджикистане

10.1. Понятие и сущность электронного правительства

Широкое использование современных технологий в государственном управлении сделало неизбежным феномен известный мировой общественности как «электронное правительство». Понятия «электронное правительство» было выдвинуто несколькими авторами. В энциклопедии Википедия отмечено, что «электронное правительство» - это стадия компьютеризации бумажного документооборота, в результате которой появились новые способы правления, дискуссий и принятия важнейших решений, развития коммерции, новые пути общения с народом и новые пути организации разработки информации[1].

В тоже время пункт 6 Главы 1 Концепции формирования электронного правительства Республики Таджикистан, понятие «электронное правительство» приводится таким образом: «новая форма организации деятельности исполнительных органов государственной власти, обеспечивающая за счет широкого применения ИКТ качественно новый уровень оперативности и удобства получения гражданами и организациями общественных услуг, и информации о результатах деятельности исполнительных органов государственной власти"

Понятие "электронного правительства" предполагает наличие следующих аспектов:

1. Информационно-коммуникационные технологии (ИКТ).
2. Внедрение ИКТ в деятельность
3. Цель внедрения ИКТ в деятельность

ИКТ состоит из ряда технологических связей (радио, телевидение, телефон, компьютер, интернет, беспроводные спутниковые технологии и т.д.) и программного обеспечения, которые предназначены для производства, распространения, обработки, защиты и обмена информации.

Процесс развития ИКТ в Республике Таджикистан по данным статистики и анализа положительный. Например, количество сим карт для мобильных телефонов превышает численность населения республики, количество пользователей интернета в РТ превышает 50%.

Второй фактор, реализация ИКТ в процессе деятельности. Процесс ИКТ должен охватить деятельность всех государственных структур, граждан и юридических лиц (коммерческие и некоммерческие организации). К примеру, если налоговый орган принимает отчёт в электронном виде, но предприниматель не умеет пользоваться ИКТ, или наоборот – предприниматель пользуется ИКТ, а

[1] Общая тема, лежащая в основе этих определений, заключается в том, что электронное правительство предполагает автоматизацию или компьютеризацию существующих бумажных процедур, что приведет к новым стилям руководства, новым способам обсуждения и принятия стратегий, новым способам ведения бизнеса, новым способам прислушиваться к мнению граждан. и сообщества, а также новые способы организации и доставки информации.

государственный орган нет, то «электронное правительство» не будет реализовываться должным образом. Если обратить внимание на Концепцию формирования электронного правительства в Республике Таджикистан, то можно заметить, что большой акцент делается на «деятельности исполнительных органов государственной власти". Но это не является завершением или достижением цели, не так важно, что значение «электронного правительства» в данной Концепции приведено именно таким образом, важно то, как широко реализуется электронное правительство, то есть не только в рамках деятельности исполнительных органов государственной власти, но и в рамках других государственных органов. Конечно, не каждую деятельность можно реализовать через ИКТ. Например, можно принять решение в электронном виде и подписать его, но есть действия, которые невозможно совершить в электронном виде (например, ремонт здания со стороны человека, который нанес зданию ущерб). Российские специалисты утверждают, что 70% государственные служб имеют возможность осуществлять свою деятельность через ИКТ. В Таджикистане также некоторые услуги осуществляются в электронном виде (электронные отчеты в налоговые органы, тестирование в центре по тестирования и т.д.).

Третий фактор, цель внедрения ИКТ в процессе деятельности, необходимо понимать как положительную цель. Качество и скорость реализации, отношения сторон должны постоянно улучшаться. В целом, не только ИКТ, но также государство, законы и другие факторы необходимы в процессе развития условия жизни человека. Таким образом реализация ИКТ в деятельности, эта новая ступень улучшения качества и темп развития деятельности субъектов. Это означает, что электронное правительство не является новым государственным органом. Оно является процессом применения ИКТ в деятельности государственных органов и других общественных субъектов. В этом направлении государство имеет возможности и играет важную роль. Необходимо отметить, что электронное правительство не одноразовое явление и не существует как отдельный субъект. Это такое условное понятие, которое охватывает большинство сфер деятельности правительства, общества и человека.

10.2. Цифровое правительство: ключевые принципы и основные отличия от электронного правительства:

Ключевое различие между первоначальными моделями электронного правительства и цифровым правительством заключается в переходе от простого предоставления онлайновых государственных услуг к подходу, ориентированному на использование данных.

В последние годы увеличение объема данных происходило экспоненциально. ООН определяет высококачественные данные как «источник для принятия решений и сырье для отчетности». Управление данными приводит к повышению персонализации услуг и продуктов, коммуникации, совместного использования активов и совместной работы, а также ценообразования на основе данных об использовании.

Особое значение имеет понимание роли, которую данные играют в процессах принятия решений, и влияющих на трансформацию административных процессов, т.е. переход к цифровому правительству.

Ключевые принципы цифрового правительства, отличные от электронного правительства, следующие:

- принятие подхода по созданию «правительства как единого целого», которое является «цифровым по умолчанию»;
- приверженность принципу «цифровой от начала до конца» (digital end-to-end);
- проектирование клиенто-центрических услуг;
- платформонезависимость внедряемых услуг;
- реализация стратегии, основанной на использовании данных;
- содействие использованию открытых данных;
- использование открытых стандартов и программного обеспечения с открытым исходным кодом;
- открытость для инноваций и «подрывных» технологий.

Государственные услуги должны функционировать не в виде предустановленного меню, а на основе итеративного подхода, основанного на использовании данных и позволяющего кастомизировать услуги под конкретного гражданина.

Учитывая ограниченные государственных ресурсы, интеллектуальные прогнозные модели, генерирующие сценарии на основе вероятностей, рассчитанных при использовании анализа данных, могут способствовать принятию решений о более оперативном и точном распределении ресурсов. Такие модели, например, используются правоохранительными органами для прогнозирования преступности. Используя алгоритмы и устройства с геолокацией, которые отслеживают данные о преступлениях в режиме реального времени, полицейские подразделения могут развертывать свои ресурсы в районах, где преступность более вероятна. Предиктивная аналитика данных также используется для отслеживания финансовых преступлений, налогового мошенничества и киберпреступлений.

Имеющийся передовой опыт свидетельствует о том, что, для успешной реализации стратегии цифрового правительства, в качестве фундамента необходимо иметь четыре ключевых элемента:

- единая среда управления данными;
- переосмысление принципа «правительство как платформа»;
- приверженность требованиям кибербезопасности и конфиденциальности;
- культура, открытая для инноваций.

Правительства стран, наиболее продвинутых в области развития и использования цифровых технологий, и некоторые неправительственные организации применяют подход **«правительство как платформа»**, чтобы получить возможность предоставлять инновационные государственные услуги более эффективным и удобным для пользователей способом, что позволяет

правительственным структурам создавать более быстрые и дешевые цифровые услуги для граждан и бизнеса.

Правительство выступает в качестве посредника, координирующего участников, обеспечивая сотрудничество, связывая людей и поставщиков, и, в конечном счете, прогнозируя модели предоставления государственных услуг, которые выйдут за рамки того, что мы можем себе представить сегодня.

Переход к модели «правительство как платформа» — значительный скачок на пути к умному правительству. Смысл заключается в том, чтобы сделать данные и решения, принимаемые правительством, открытыми для использования другими лицами через платформу, доступную для всех.

В рамках данного подхода правительство уходит от роли поставщика услуг, и рассматривается как механизм, способствующий деятельности в публичной сфере. Этот подход поощряет граждан к активному участию в разработке политики и предоставлении цифровых государственных услуг, а власть отвечает за функционирование экосистемы для участия.

Опираясь на передовой опыт частного сектора, «правительство как платформа» осуществляет аутсорсинг для снижения затрат и повышения эффективности. Роль правительства заключается в создании платформы, предоставлении государственных услуг, обслуживании инфраструктуры, а также в посредничестве, регулировании и контроле за ее использованием и процессом предоставления услуг, включая сторонние приложения. Платформа должна обеспечивать эффективную персонализацию государственных услуг и предоставлять пользователям большую гибкость в отношении выбора и персонализации государственных услуг.

Основными компонентами «правительства как платформа» являются:

- **открытые правительственные данные**, которые собираются, обрабатываются и хранятся в согласованном и удобном для использования формате;
- **доступ к данным через открытые программные интерфейсы** приложений;
- набор правил, регулирующих доступ и **использование данных, создаваемых и предоставляемых через платформу**.

Цифровое правительство — это не только технологии, но также и культурный сдвиг. Успех внедрения цифрового правительства и цифровой трансформации напрямую связан с приверженностью руководства изменению культуры общества

10.3. Роль электронного документооборота в формировании электронного правительства

Данное направление является одной из важных частей электронного правительства. Прежде всего этот процесс регулируется Законом Республики Таджикистан «Об электронном документе». Электронный документ — это информация, зафиксированная на машинном носителе, и соответствует

требованиям данного закона. Согласно статье 6 Закона основными требованиями, предъявляемыми к электронным документам, является следующее:
-создаваться, обрабатываться, приниматься, передаваться и храниться с помощью программных и технических средств;
-иметь структуру, установленную законом и содержать реквизиты, позволяющие его идентифицировать;
-быть представленным в форме понятной для восприятия человеком;
Электронный документооборот состоит из трёх этапов:
1). Организация электронного документооборота в каждой структуре, организации и учреждении; **2).** Налаживание двухсторонних электронных взаимоотношений между государственными структурами; **3).** Предоставление государственных услуг со стороны государственных органов посредством электронного документооборота;

Для осуществления этих отношений необходимо проводить организационные работы. Это значит, необходимо переходить с «бумажной формы» на "электронную", а это прежде всего требует знаний, практики и творчества. Для создания системы электронного документооборот внутри каждой организации необходимо прежде всего, разработать и предоставить для принятия примерную инструкцию по электронному документообороту. Так как без объединения в единую систему этого направления, решение проблем не является возможным.

На данный момент согласно примерной Инструкции по делопроизводству в государственных структурах, учреждениях, предприятиях и других организациях, принятой Постановлением Правительства Республики Таджикистан от 28.07.2017 года, №358 утверждена «традиционная» система делопроизводства.
В пунктах 46-51 Инструкции определены требования к документам, изготовляемыми средствами компьютерного оборудования.
В том числе в пунктах 48-51 приводятся следующие:

При отправке документов должны обязательно соблюдаться следующие правила и размеры полей:
- письма должны отправляться в конвертах;
- шрифтом Times New Roman с использованием таджикского алфавита, размеров шрифта 16 на имя Президента Республики Таджикистан и шрифтом 14 Правительству Республики Таджикистан и министерствам, ведомствам;
- пронумерованы, если документ более 1 страницы;
- обычный шрифт без выделения;
- поля бланка: сверху 1,5 см., слева 2,5 см., снизу для формата А4 не менее 4 см, а для формата А5 - не менее 1 см.

Текст документа печатается через один или полтора межстрочных интервала. Первая строка каждого абзаца печатается с красной строки. При необходимых случаях с документами могут быть представлены и электронные версии. Таким образом, переход на электронный документооборот – это то явление, которое мы должны использовать в каждой отрасли.

10.4. Роль электронной подписи в формировании электронного правительства

Необходимо отметить, что электронная подпись в создании электронного правительства играет важную роль. То есть, надёжный оборот электронных документов обеспечивает именно электронная подпись. В реальном мире для заключения письменного договора подпись на бумаге обязательна. (Статья 185, ГК РТ). Именно такое же положение также применяется и в электронном документообороте. Согласно Закону Республики Таджикистан «Об электронном документе» электронная подпись является составной частью электронного документа. Это означает, что без электронной подписи электронные документы не имеют юридической силы. На практике в Таджикистане на данный момент используется электронно-цифровая подпись, в основном в банковской деятельности и подаче налоговой декларации, но в делопроизводстве такая подпись не используется широко. Причина в том, что порядок выдачи и момент реализации таких подписей не имеет массового распространения. Закон Республики Таджикистан «Об электронной цифровой подписи» определяет порядок получения и использования электронной цифровой подписи.

Одновременно, в законодательстве Таджикистана использование электронной цифровой подписи предусмотрено в нескольких нормативно правовых актах, в том числе в: Законе Республики Таджикистан «О электронном документе», статье 74 Хозяйственно-процессуального Кодекса в Республике Таджикистан, статьях 2, 27 Закона Республики Таджикистан «О кредитных историях», статьи 9 Закона Республики Таджикистан «О праве на доступ к информации», статье 14 Закона Республики Таджикистан «Об информатизации», статье 185 Гражданского Кодекса Республики Таджикистан, статье 10 Закон РТ «О казначействе» и других подзаконных актах.

10.5. Биометрическая аутентификация

Биометрические данные. Сведения, которые характеризуют физиологические и биологические особенности субъекта, на основе которых можно установить его личность, определение описывает принадлежность биометрических данных к персональным данным, с учетом биологических и физиологических особенностей[2].

Биометрические данные – это персональные данные, полученные в результате специальной технической обработки, которые касаются физических, физиологических или поведенческих черт физического лица, а также делают возможной однозначную идентификацию этого физического лица или подтверждает ее, например, изображение лица или дактилоскопические данные[3]. Биометрические черты, которые могут быть использованы для проверки,

[2] EGOV. “Открытые НПА.” Открытые НПА, 2022, legalacts.egov.kz/npa/view?id=14023459. Accessed 17 July 2022.

[3] “Tooltips | GDPR-Text.com.” GDPR-Text.com | GDPR Text, Translation and Commentary, gdpr-text.com/ru/english-gdpr-glossary/. Accessed 17 July 2022.

включающей отпечатки пальцев, лицо, голос, радужную оболочку глаза и другие биологические признаки.

Дактилоскопия. Специальная процедура, применяемая в качестве способа идентификации личности по папиллярным узорам пальцев рук (отпечатков пальцев), путем использования типографской краски и бланка дактилоскопической карты либо путем сканирования специальным считывающим программным устройством. Дактилоскопия - широко применяется в биометрических системах контроля доступа, полученные отпечатки, преобразованные в цифровой код, будут храниться зашифрованном виде в базе биометрических данных[4].

Геномная регистрация. Сбор, хранение и использование биологического материала и дезоксирибонуклеиновой кислоты (ДНК) человека в целях идентификации личности. Базы данных геномной информации будет содержать информацию о лицах, осужденных за совершение тяжких или особо тяжких преступлений, неустановленных лицах, биологических родственников без вести пропавших граждан, неопознанных трупов[5].

Процесс автоматизированной проверки и идентификации личности реализуется путем использования различных приложений, который включает возможность предоставления доступа к базам данных, к оплате общественного транспорта, получению государственных услуг, предоставлению персональной информации в аэропортах, при использовании веб-приложений, таких как онлайн-банкинг и онлайн-покупки.

Биометрические данные наиболее распространенно применяются правоохранительными органами в целях обеспечения национальной безопасности, расследования преступлений, предотвращения совершения правонарушений[6]. Наряду с традиционными методами идентификации, применяются способы верификации через биологические характеристики человека на основе физических, биологических или поведенческих особенностей человека.

Полученные отпечатки пальцев вводят в базу биометрических данных. Зачастую цели внедрения единой базы биометрических данных, обусловлены обеспечением пограничного режима и противодействию терроризму, а также для повышения уровня раскрываемости преступлений. В мировой практике биометрические данные служат для обеспечения общественной безопасности, охраны порядка, контроля за миграционными процессами, повышения эффективности работы органов государственных органов.

---

[4] "Обязательная дактилоскопия казахстанцев: зачем она нужна и как это работает?" CABAR.asia, 6 Jan. 2021, cabar.asia/ru/zachem-vvoditsya-obyazatelnaya-daktiloskopiya-kazahstantsev. Accessed 17 July 2022.

[5] "О дактилоскопической и геномной регистрации - ИПС "Әділет."" Adilet.zan.kz, adilet.zan.kz/rus/docs/Z1600000040. Accessed 15 May 2022.

[6] White, David, et al. "Human Factors in Forensic Face Identification." Handbook of Biometrics for Forensic Science, 2017, pp. 195–218, link.springer.com/chapter/10.1007/978-3-319-50673-9_9, 10.1007/978-3-319-50673-9_9. Accessed 11 Nov. 2019.

Практика дактилоскопирования также получила широкое использование при получении документов, удостоверяющих личность, въезде или выезде за границу, при чрезвычайных ситуациях, получении медицинских карт и др.

В соответствии с Постановлением Межпарламентской Ассамблеи государств – участников СНГ «О Глоссарии терминов и понятий, используемых государствами – участниками СНГ в пограничной сфере» биометрическими данными являются сведения, характеризующие физиологические особенности человека, на основе которых можно установить его личность:

- цифровая фотография,
- отпечатки пальцев,
- изображение радужной оболочки глаз и иные биометрические данные;

могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных и в соответствии с национальным законодательством[7].

Соединенные Штаты Америки:

В США отмечено отсутствие федерального регулирования биометрических данных. Несмотря на многочисленные виды использования биометрических данных в Соединенных Штатах, только в штатах Иллинойс и Техас успешно приняты законы о защите биометрических данных[8]. Закон о конфиденциальности биометрической информации штата Иллинойс (BIPA), известный как BIPA, обеспечивает кроме общей защиты биометрических данных возможность подавать частным лицам иски о возмещении ущерба[9]. Генеральная Ассамблея также отметила необходимость защиты биометрических данных, поскольку «полные последствия биометрических технологий не полностью известны»[10]. Законодательство, регулирующее получение и использование биометрии (Capture or Use of Biometric Identifier Act)[11], также аналогичен BIPA, но он не создает частного права на иск для потребителей. Вместо этого CUBI предписывает штраф в размере «не более 25 000 долларов США за каждое нарушение»[12].

---

[7] "Постановление № 47-13 (Постановление Межпарламентской Ассамблеи государств - участников Содружества Независимых Государств от 13 апреля 2018 г. №47-13 "О Глоссарии терминов и понятий, используемых государствами - участниками СНГ в пограничной сфере.")." www.etalonline.by, www.etalonline.by/document/?regnum=n21800044. Accessed 20 July 2022.

[8] U.S. Department of Justice. "Privacy Act of 1974." Justice.gov, 17 July 2015, www.justice.gov/opcl/privacy-act-1974.

[9] "Biometric Information Privacy Act (BIPA)." ACLU of Illinois, 26 Apr. 2021, www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa.

[10] СБОРНИК ПРАКТИЧЕСКИХ РЕКОМЕНДАЦИЙ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом Подготовлен совместно с Институтом биометрии.

[11] The Capture or Use of Biometric Identifiers Act (CUBI). 15 Sept. 2021, caseguard.com/articles/the-capture-or-use-of-biometric-identifiers-act-cubi/. Accessed 15 May 2022.

[12] "Analyses of Section 503.001 - Capture or Use of Biometric Identifier, Tex. Bus. & Com. Code § 503.001 | Casetext." Casetext.com, casetext.com/statute/texas-codes/business-and-commerce-code/title-11-personal-identity-information/subtitle-a-identifying-information/chapter-503-biometric-identifiers/section-503001-capture-or-use-of-biometric-identifier/analysis?citingPage=1&sort=relevance.

Принятый Калифорнийский закон о конфиденциальности потребителей (CCPA)[13] от 2018 года обеспечивает множество мер защиты данных потребителей, включая биометрические данные. CCPA был принят 28 июня 2018 года, и в законопроект уже было внесено много поправок для уточнения его технических аспектов, тем не менее он достаточно обеспечивает средства защиты, аналогичные Общему регламенту Европейского союза по защите данных (GDPR)[14].

Ярким примером является предъявление коллективного иска жителей штата Иллинойс в федеральный суд США Северного округа штата Иллинойс двум американским компаниям, в сумме штрафа 6,8 миллиона долларов о незаконном сборе биометрических данных при покупке в торговых автоматах. Данные торговые автоматы хранили отпечатки пальцев покупателей без получения согласия и надлежащего информирования[15]. Вторым известным случаем в Иллинойсе был иск к компании Facebook в сумме 650 миллионов долларов, за использование функции распознавания лиц и отметки на изображении лиц, без уведомления пользователей, а также за сбор и хранение биометрических данных пользователей[16].

К примеру, Центры Fusion используют инструменты интеллектуального анализа данных для сбора, обработки и обмена персональными данными из государственных и «баз данных частного сектора, Интернета, а также государственных и частных видеокамер». Центр Fusion[17] также имеет доступ к «досье на сотни миллионов людей»[18], а некоторые даже «собирают биометрические данные и используют программное обеспечение для распознавания лиц»[19].

С появлением технологий, которые позволяют собирать больше личной информации о субъектах, включая хранение и изучение онлайн-активности и коммуникаций, становится все труднее оставаться анонимным либо сохранять свою приватность в современном обществе. Несмотря на то, что подавляющее количество личной информации, собранной о субъектах, подвергается различного рода использованию, тем самым позволяя использовать информацию третьим лицам, и знать о субъектах гораздо больше, чем это необходимо[20].

Республика Таджикистан:

---

[13] "California Consumer Privacy Act (CCPA)." Google Cloud, cloud.google.com/security/compliance/ccpa. Accessed 15 May 2022.

[14] "Текст GDPR на русском с комментариями и ссылками | GDPR-Text.com." GDPR-Text.com | GDPR Text, Translation and Commentary, 28 Oct. 2019, gdpr-text.com/ru/.

[15] "В США подан иск к Amazon, Google и Microsoft из-за сбора конфиденциальных сведений." РАПСИ, 15 July 2020, rapsinews.ru/international_news/20200715/306034494.html. Accessed 15 May 2022.

[16] "Власти США ополчились на Facebook за нелегальное распознавание лиц пользователей." CNews.ru, www.cnews.ru/news/top/2022-02-25_vlasti_ssha_opolchilis_na. Accessed 15 May 2022.

[17] Department of Homeland Security. "Fusion Centers." Department of Homeland Security, 19 Sept. 2019, www.dhs.gov/fusion-centers.

[18] "Биометрические персональные данные и технологии идентификации: какие правовые проблемы могут возникнуть?" www.garant.ru, www.garant.ru/news/1460152/. Accessed 15 May 2022.

[19] Considerations for Fusion Center and Emergency Operations Center Coordination Comprehensive Preparedness Guide (CPG) 502. 2010.

[20] *Id.*

Согласно статье 17 Закона Республики Таджикистан от 3 августа 2018 года No1537 «О защите персональных данных» отдельно определены биометрические персональные данные, сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные), и которые используются оператором для установления личности субъекта персональных данных. Могут быть обработаны только при наличии письменного согласия субъекта персональных данных, за исключением случаев, связанных с осуществлением уголовного преследования и правосудия, исполнением судебных актов, а также в случаях, предусмотренных законодательством Республики Таджикистан об обороне, о безопасности, об оперативно-розыскной деятельности, противодействии терроризму, экстремизму, коррупции и легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового поражения, исполнения уголовного наказания, приобретения и прекращения гражданства Республики Таджикистан и о государственной службе[21].

Российская Федерация:

В России с 30 декабря 2021 года действует Единая биометрическая система (ЕБС - далее), которая стала частью инфраструктуры, обеспечивающей взаимодействия информационных систем, используемых для предоставления государственных и муниципальных услуг. Государство ввело единую биометрическую систему (ЕБС), участие в сдаче данных в общую базу ЕБС было добровольным. Защиту биометрических данных предусматривает Федеральный закон "Об информации, информационных технологиях и о защите информации", статья 14.1 в данном Законе определяет понятие и распространяет защиту по части персональных данных, включая биометрические данные. Более того, пункт 2 и 3 статьи 14.1 Федерального закона «Об информации, информационных технологиях и о защите информации» предусматривает ограничения по обработке биометрических данных. Пункт 2 статьи 14.1 предусматривает фиксирование действий при размещениях действий касательно биометрических данных, а пункт 3 распространяет контроль и надзор за действиями касательно обработки, сбора и использования биометрических данных, что гарантирует правовую сохранность данных.

Республика Казахстан:

В настоящее время не существует отдельных законов, защищающих биометрические данные субъектов. Несмотря на то, что Закон о защите персональных данных[22] охватывает регулирование сферы персональных данных в Казахстане и защищает конфиденциальность персональной информации

---

[21] Закон Республики Таджикистан от 3 августа 2018 года № 1537 “О защите персональных данных.”” Информационная система ПАРАГРАФ, online.zakon.kz/Document/?doc_id=39538796&pos=7. Accessed 3 July 2022.

[22] “О персональных данных и их защите - ИПС “Әділет.”” Adilet.zan.kz, adilet.zan.kz/rus/docs/Z1300000094/z13094.htm. Accessed 15 May 2022.

государственных субъектов, однако в частном секторе такой защиты нет, как в нашем государстве, так и в практике зарубежных государств.[23] Кроме того, явное отсутствие более четкого регулирования биометрических данных позволяет правительству обойти некоторые требования Закона о защите персональных данных при помощи операторов сети и нерегулируемого частного сектора[24].

По части защиты персональных данных предусмотрена уголовная и административная ответственность, а также уголовная ответственность за правонарушения, связанные с посягательством на неприкосновенность частной жизни[25].

В Казахстане запланирован повсеместный и обязательный сбор биометрических данных. Сбор будет осуществлен посредством проведения обязательной дактилоскопической регистрации всех граждан, проживающих на территории Казахстана, иностранцев, а также лиц без гражданства. Данное требование распространяется также и на несовершеннолетних лиц (дети в возрасте от 12-ти до 16-ти лет подлежат дактилоскопической регистрации)[26]. Существующее описание принятых мер, будет реализовано в соответствии с Законом «О дактилоскопической и геномной регистрации», который поэтапно вступил в силу[27]. Первый этап вступления в силу произошел 1 января 2021 года, второй этап планируется в 2023 году. Согласно официальным данным МВД РК вопрос об обязательной дактилоскопической регистрации граждан состоится с 2023 года путем организации работы специализированной базы данных АИС БИЛ[28].

В Казахстане последствия пандемии COVID-19 способствовали созданию цифровых решений по удаленной идентификации личности — «Центр обмена идентификационными данными» Национального Банка РК, сервис центра обмена

---

[23] "Biometrics Litigation: An Evolving Landscape | Practical Law." Content.next.westlaw.com, content.next.westlaw.com/practical-law/document/Id18ae0a6f51711e598dc8b09b4f043e0/Biometrics-Litigation-An-Evolving-Landscape?viewType=FullText&transitionType=Default&contextData=(sc.Default). Accessed 15 May 2022.

[24] "Ответственность за нарушение закона о персональных данных." www.garant.ru, www.garant.ru/actual/persona/otvetstvennost/. Accessed 15 May 2022.

[25] "Передача базы телефонных номеров. История одного тендера "Казахтелекома." Радио Азаттык, rus.azattyq.org/a/kazakhstan-numbers-base-transfer-history-of-a-tender-of-kazakhtelecom/31757577.html.

[26] Слотер, Энн-Мэри. "К чему приведёт сбор государством биометрических данных граждан?" Www.forbes.kz, 25 July 2018, forbes.kz/life/observation/kak_gosudarstvo_sobiraet_informatsiyu_o_svoih_grajdanah/. Accessed 15 May 2022.

[27] "О дактилоскопической и геномной регистрации - ИПС "Әділет."" Adilet.zan.kz, adilet.zan.kz/rus/docs/Z1600000040. Accessed 15 May 2022.

[28] АИС БИЛ - Автоматизированная Информационная Система Биометрическая идентификация личности». "Исследование возможных экономических, социальных и правовых последствий закона РК "О дактилоскопический и геномной регистрации." Soros Kazakhstan Foundation, 23 June 2021, www.soros.kz/ru/study-of-the-law-of-the-republic-of-kazakhstan-on-fingerprint-and-genomic-registration/. Accessed 15 May 2022.

идентификационными данными (ЦОИД)[29], а также Digital ID Министерства цифрового развития и аэрокосмической промышленности РК. Сервис центра обмена идентификационными данными (ЦОИД) позволяет банкам второго уровня проводить удаленную идентификацию личности клиентов, открывать банковские счета и вклады, осуществлять кредитование, выпуск платежных карточек и другие операции.

Европейский Союз:

Общий/Генеральный регламент по защите персональных данных GDPR направлен на «защиту всех граждан ЕС от нарушений конфиденциальности данных, ключевые изменения GDPR включают: расширение территориального охвата (экстерриториальная применимость), штрафы, согласие, уведомление о нарушении, право на доступ, право на забвение, переносимость данных, политики конфиденциальности и требование к компаниям назначать сотрудника по защите данных[30].

Сфера действия GDPR распространяется не только на компании, расположенные в Европейском союзе, которые обрабатывают персональные данные субъектов, проживающих в Союзе, но и на компании, расположенные за пределами Европейского Союза, при условии, что они обрабатывают данные субъектов ЕС[31]. GDPR также требует, чтобы предприятия, не расположенные в Пределах Европейского Союза, но которые обрабатывают данные граждан ЕС, назначали представителя в Европейском союзе.

GDPR налагает штрафы на организации, которые не соблюдают требования в размере до четырех процентов от их годового оборота или двадцати миллионов евро. В GDPR использует многоуровневый подход к штрафам, штрафы применяются к контроллерам и процессорам.[32] Требование о согласии, в соответствии с GDPR является повышенным, потому как ожидается, что запрос на согласие будет дан в «понятной и легко доступной форме с целью обработки данных»[33]. Кроме того, согласие возможно будет так же легко отозвать, как и дать его[34].

Что касается прав субъектов данных, GDPR предоставляет право на уведомление о нарушении, право на доступ, право на забвение и право на переносимость данных[35]. Эти права требуют, чтобы все государства-члены должны будут уведомить субъектов и контролеров о нарушении данных в течение семидесяти двух часов[36]. Кроме того, субъекты данных имеют право знать,

---

[29] "Нацбанк: В пилотном режиме запущен сервис центра обмена идентификационными данными." *Деловой портал Капитал.кз*, kapital.kz/tehnology/86517/natsbank-v-pilotnom-rezhime-zapushchen-servis-tsentra-obmena-identifikatsionnymi-dannymi.html. Accessed 14 May 2022.

[30] *Id*. Note 30

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] Id.

«обрабатываются ли касающиеся их персональные данные, где и с какой целью"[37]. Субъекты данных также имеют право на бесплатную копию хранения своих персональных данных в электронном формате[38]. Самое главное, если субъекты данных соответствуют условиям, они «имеют право на то, чтобы контроллер данных удалил его [или] ее данные, прекратил дальнейшее распространение данных и потенциально заставил третьих лиц прекратить обработку данных[39].

Законодательный акт ЕС о защите персональных данных GDPR ориентированный на частно – правовую сферу регулирования данных, исключает из сферы действия закона использование и защиту персональных данных в целях расследования преступлений, общественной безопасности и т.д. Например, в Великобритании существует одна из самых крупных национальных баз ДНК с более чем 5 млн профилей, также это базы биометрических данных Интерпола, либо база биометрических данных пассажиров в аэропортах для контроля миграции. Также, если обычно хранение образцов ДНК не допускается после вынесения окончательного решения по делу, в котором они были использованы, это будет возможным в случае, если человек, которому они принадлежат признан судом виновным в совершении тяжких преступлений против жизни, неприкосновенности и безопасности других лиц.

В частно – правовой сфере GDPR обязывает любую организацию запрашивать согласие пользователя до сбора данных. Те компании, которые не смогут обеспечить безопасность данных, получат внушительные штрафы.

Риски, связанные с утечкой биометрических данных. Использование биометрических данных, может привести к большим рискам. Ограничить список рисков невозможно, потому как цифровизация развивается с большим успехом, из чего следует что право всегда должно соответствовать актуальным требованиям. Наиболее распространенными риском при использовании биометрических данных является продажа и (или) публикация биометрических данных, потому как биометрические данные не могут быть видоизменены.

Законодательство о защите биометрических данных сталкивается с несколькими основными проблемами, с одной стороны, слишком медленно борется со скоростью, с которой они собираются и обрабатываются.

Задачи:

Задача№1. Ахмад во время заключения договора с иностранными партнерами в договоре поставил свою подпись, отсканировал ее и отправил своим иностранным партнерам. Его иностранные партнеры приняли договор, поставили свою подпись, отсканировали и вернули Ахмаду обратно. Спустя некоторое время между ними возник спор. В экономическом суде судья, разбирая данный договор сделал вывод, что договор не соответствует требованиям Закона РТ. «О электронной цифровой подписи». Так как, сканированная подписи не значит, что это электронно

[37] Id.
[38] Id.
[39] Id.

цифровая подпись. Дайте правовую оценку действию сторон, заключению судьи и сканированной подписи.

Задача №2. Самад, как директор, разработал внутренний ведомственный регламент, подтвердил и для его исполнения отправил через электронную почту сотрудникам и структурам организации для ознакомления и исполнения. Спустя время, между руководством и сотрудником хозяйственной части предприятия возник спор. Работник хозяйственной части предприятия отказался от исполнения электронного документа, обосновывая это тем, что он хотя и получил Устав предприятия на электронную почту, но официально не ознакомился и не подписал его. Поэтому выполнение этой задачи ему не обязательно. Выполнение задачи для работника становится обязательным, тогда, когда он ознакомлен и поставил свою подпись. Дайте правовую оценку действиям руководства и Самада?

Тесты:

№1. К какой ветви власти относится электронное правительство, согласно Концепции формирования электронного правительства в РТ?

А) Исполнительная;

Б) Судебная;

В) Законодательная;

Г) Всем.

№2 На каком из этих понятий основывается электронное правительство?

А) Электронное управление;

Б) Электронные деньги;

В) Сервер;

Г) Интернет.

№3. Назовите признаки электронного документооборота?

А) Подготовленные программными и техническими средствами, разработка, отправка, прием и защита;

Б) Имеют признаки, дающие возможность для сравнения;

В) Предоставляется в той форме, которая доступна понятию человека;

Г) Все ответы верны.

№4. Назовите этапы электронного документооборота?

А) Организация электронного документооборота внутри каждой организации, предприятия, органа;

Б) Налаживание двухсторонних электронных отношений между государственными структурами;

В) Оказания государственных услуг населению органами государственной власти через электронный документооборот;

Г) Все ответы верны.

№5. В каких документах электронная подпись не обязательна?

А) В электронных документах, в которых законодательство требует этой подписи;

Б) В электронных документах, которые определены сторонами;

В) Во всех документах;

Г) Все ответы неверные.

Вопросы для письменной работы:

1. Дайте информацию о Концепции формирования электронного правительства в Республике Таджикистан.
2. Опишите Законы, которые непосредственно продвигают формирование электронного правительства в Республике Таджикистан.
3. Из каких реквизитов состоит электронный документ?
4. Проинформируйте об электронной подписи и его видах.
5. Проанализируйте внутриорганизационные инструкции и электронный документооборот.

Вопросы для самотестирования:

1. Что такое электронное правительство?
2. С какой целью создается электронное правительство?
3. Каковы основные признаки электронного правительства?
4. Приведите примеры формирования электронного правительства
5. Какие правовые действия приняты для развития электронного правительства?

Литература:

1. Концепция электронного правительства в Республике Таджикистан от 30 декабря 2011 года./ Юстиция 7.0
2. Типовые инструкции по делопроизводству в государственных органах, учреждениях, предприятиях и иных организациях Республики Таджикистан, утверждаемые Правительством Республики Таджикистан от 28 июля 2017 года, №358/ Юстиция 7.0
3. Меликов У.А Концепция развития информационного законодательства Республики Таджикистан// юридический журнал, 2020, №2. С.19-26.