Академия правоохранительных органов
при Генеральной прокуратуре Республики Казахстан

УДК 342.4

На правах рукописи

АМИРОВ АЛМАС МУРАТОВИЧ

Прокурорский надзор за соблюдением законности в сфере персональных данных и их защиты

8D04201 – Юриспруденция
(код направления 8D123 – Общественная безопасность)

Диссертация на соискание степени
доктора философии (PhD)

Научные консультанты
доктор юридических наук,
профессор
Е.Н. Бегалиев,

доктор юридических наук,
доцент
Д.В. Воронков,
кандидат юридических наук,
доцент
(ассоциированный профессор)
А.В. Сырбу

Республика Казахстан
Косшы, 2025

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящей диссертации применяют следующие термины с соответствующими определениями:

Building Information Model – технология информационного моделирования, информационная модель здания или информационное моделирование зданий

Face ID – метод аутентификации, представляющий собой сканирование объемно-пространственной формы лиц человека

IP‑адрес – уникальный адрес, идентифицирующий устройство в сети Интернет или локальной сети

Open Source INTelligence – разведывательная дисциплина и комплекс мероприятий, инструментов и методов для получения и анализа информации из открытых источников

Radio Frequency IDentification – метод автоматической идентификации объекта, построенный на считывании радиосигнала

Radio Frequency IDentification – метод автоматической идентификации объекта, построенный на считывании радиосигнала

Subscriber Identification Module – идентификационный электронный модуль абонента в виде микросхемы, которая вставляется в мобильное устройство для подключения к сети оператора

Short Message Service – уникальный код, который направляется на мобильный телефон субъекта персональных данных для подтверждения определенных действий, в том числе для согласия на доступ к его персональным данным

Virtual private network – виртуальная частная сеть, которая с помощью сети Интернет создает частное сетевое подключение между устройствами

3D	– 3 dimensional – три измерения
BIM	– Building Information Model
GDPR	– General Data Protection Regulation/Генеральный регламент по защите данных
IP‑адрес	– Internet Protocol
OSINT	– Open Source INTelligence
RFID	– Radio Frequency IDentification
SIM–карта	– Subscriber Identification Module
SMS-код	– Short Message Service
VPN	– Virtual private network
АДИС	– Автоматизированная дактилоскопическая информационная система
АИС СУ	– Автоматизированная информационная система «Специальные учеты»
АППК	– Административный процедурно-процессуальный кодекс Республики Казахстан

ВИЧ – Вирус иммунодефицита человека, поражающего иммунную систему человека
г. – город
гр. – гражданин
ГПК – Гражданский процессуальный кодекс Республики Казахстан
ДНК – Дезоксирибонуклеиновая кислота
др. – другие
ЕРАП – Единый реестр административных производств
ЕРДР – Единый реестр досудебных расследований
ЕС – Европейский Союз
ЕСПЧ – Европейский суд по правам человека
ИИН – индивидуальный идентификационный номер
КоАП – Кодекс об административных правонарушениях
КПСиСУ – Комитет по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстана
КУИ – Книга учета информации
МВД – Министерство внутренних дел
млн. – миллион
млрд. – миллиард
НАО – Некоммерческое акционерное общество
ООН – Организация объединенных наций
ОРД – оперативно-розыскная деятельность
ОЭСР – Организация экономического сотрудничества и развития
п. – пункт
пп. – подпункт
СМИ – средство массовой информации
СНГ – Содружество независимых государства
ст. – статья
ст.ст. – статьи
США – Соединенные штаты Америки
т.д. – так далее
т.п. – тому подобное
т.ч. – том числе
ЦАРКА – Центр анализа и расследования кибератак
СИО ПСО – Система информационного обмена правоохранительных, специальных государственных и иных органов
ЭЦП – электронная цифровая подпись

ВВЕДЕНИЕ

Актуальность темы исследования. Государства и коммерческие структуры, начиная от гигантов отраслей до небольших предприятий, стремятся собирать, хранить и анализировать как можно больше сведений. Исследователи прогнозируют, что в 2025 году общий объем глобального хранилища данных превысит 200 зеттабайт, а ущерб от киберпреступлений достигнет 10,5 триллионов долларов США [1].

Собираемая информация представляет значительный интерес для злоумышленников, которые, используя различные методы, совершают атаки на ресурсы и базы данных. Компания Cybersecurity Ventures считает, что к 2031 году программы-вымогатели каждые 2 секунды будут атаковать правительства, предприятия, потребителей и устройства, а ущерб от них каждый год будет превышать 265 миллиардов долларов США [2].

Значительную часть собираемой и хранимой информации составляют персональные данные граждан, с помощью которых государства улучшают процессы государственного регулирования, а коммерческие структуры прогнозируют потребности и регулируют рынок.

Массовый сбор персональных данных позволяет перевести в электронный и более удобный для граждан формат государственные и бизнес услуги, но также увеличивает риски утечки персональной информации значительно повышаются. Ненадлежащее внимание к организации сбора и обработки персональных данных может способствовать необоснованному доступу к ним большого количества лиц, в том числе тех, которые будут использовать данную возможность в противоправных целях.

В Казахстане защита персональных данных гарантируется государством. В целях обеспечения их безопасности проводится значительная работа. Между тем, нередко фиксируются массовые утечки персональных данных, а сами граждане выражают обеспокоенность и неуверенность в защищенности своих сведений. К примеру, в феврале 2024 года опубликована информация, что хакеры около двух лет имели полный доступ к критической инфраструктуре крупнейших казахстанских операторов связи, в том числе и к персональным данным клиентов. Объем полученной ими информации составляет около трех терабайтов [3].

29.07.2024 года Центром анализа и расследования кибератак (ЦАРКА) сообщено об утечке полной базы данных крупнейшего в Казахстане сервиса по навигации с аудиторией более 10 миллионов пользователей, транспортно-логистической компании, популярной букмекерской компании, приложения по доставке еды, а также базы данных студентов и абитуриентов одного из университетов [4]. Ранее сообщалось о ряде других утечек с баз данных, в том числе утечке более 11 миллионов платежной и другой информации граждан Казахстана.

По данным Министерства внутренних дел Республики Казахстан за последние 5 лет число киберпреступлений возросло почти в 3 раза.

Большинство из них составляют интернет-мошенничества, для совершения которых зачастую используются похищенные персональные данные. Каждый 3 опрошенный гражданин сталкивался с такими проявлениями. Между тем, по фактам нарушений законодательства о персональных данных и их защите при обращении граждан в суд в порядке частного обвинения в 80% случаев дела прекращаются. Уголовные дела, возбужденные органами уголовного преследования, прекращаются более чем в 60% случаев.

Защита персональных данных является комплексом мер, включающих технические, правовые, организационные и организационно-технические мероприятия, направленные на обеспечение безопасности информации, относящейся к конкретному физическому лицу или позволяющей идентифицировать его. Эти меры также охватывают защиту прав, свобод и основных интересов людей в контексте обработки и использования их персональных данных, особенно в условиях, связанных с применением информационно-коммуникационных технологий для упрощения процесса обработки информации. Главная цель такой защиты – гарантировать использование персональных данных только в соответствии с их предназначением.

В защите персональных данных задействованы многие государственные органы, в том числе органы прокуратуры. Для их надлежащей работы важно правильное разграничение целей, задач и полномочий, выработка эффективной методики по защите персональных данных, в том числе и прокурорского надзора за соблюдением законности в сфере персональных данных и их защиты.

Степень научной разработанности (научная новизна). Проблемы сбора, обработки, правового регулирования и иных вопросов, связанных с персональными данными, информационной защитой, а также неприкосновенностью частной жизни рассматривались в работах С.В. Адаховской, С.А. Акилова, Г.А. Алибаевой, И.С. Алихаджиевой, Ж. Ахамбаева, Ж. Ахметовой, М. Бисалиева, В.В. Вабищевич, М.А. Важоровой, К.А. Гаджиевой, М.Б. Добробаба, М.О. Дудко, А.В. Ендольцевой, Ю.В. Ендольцевой, С.К. Жетписова, С.А. Жижис, К.С. Захилько, В.П. Иванского, Н.К. Имангалиева, О.Д. Исмагиловой, Л.К. Каирбаевой, С.А. Коморова, Б.М. Максутова, В.А. Новикова, Т.Д. Оганесяна, Э.М. Омурчиевой, Н.И. Петрыкиной, В.В. Писарева, А.Н. Прокопенко, А.А. Пухова, В.Д. Рузановой, Е.Н. Рязановой, М.Е. Соколовой, Ф. Сырлыбаевой, А.В. Сычевой, Ю.С. Телиной, Л.А. Темиржановой, Н.В. Унижаева, К.Р. Хаджи, Э.Т. Халиуллиной, К. Шакирова и других.

Из зарубежных авторов следует отметить таких ученых, как Дж. Абэ, А. Айдыноглу, Ю. Барт, Г. Бхардвадж, И. Вираван, В. Гарг, М. Графенштейн, С. Гу, Р. Дукато, А. Иоанну, Дж. Йельмо, П.К. Каннан, А. Де Кейзер, Р. Карвалью, Т. Клосовский, С. Куач, М. Куковини, К. Лабади, К. Легнер, А. Лима, Ю. Лу, З. Лю, С.К. Лю, Д. Мангку, Й. Мартин, К. Мартин, З. Матвеевой, С. Миллер, Б. Миттельштадт, Х. Муратидис, В. Обиагву, Э.

Озкан, М. Онен, Р. Палматье, К. Прете, Р. Риверо, С.Г. Робинсон, А. Румин, Г. Сингх, С.В. Сингх, Ф. Скьяво, М. Смит, Ю. Сон, Дж. Соуза, Н. Соуза, Г. Стивенс, И. Суастика, З. Сунь, П. Тайчон, Г. Татару, С. Татару, И. Тусядия, С. Уивен, Н. Фибрианти, А. Холиш, М. Шахинол, Н. Юлиартини, В. Юстицкис, Т. Якоби и других.

Вопросы, связанные с осуществлением прокурорского надзора, принципами и правовыми средствами прокурорского надзора, а также осуществлением прокурорского надзора в различных сферах, рассматривались в работах Е.Т. Абеуова, Н.М. Абдирова, А.С. Анненковой, А.Л. Аристархова, А.Б. Ахметовой, С.А. Бессчасного, К.С. Баканова, С.Д. Бекишевой, А.В. Бородиной, А.И. Британова, Н.Д. Бут, Ю.Е. Винокурова, О.В. Воронина, Е.А. Габышевой, Д.И. Ережипалиева, Е.Р. Ергашева, С.К. Журсимбаева, С.И. Захарцева, Е.А. Иванченко, К.В. Камачатова, О.К. Канатбека, Ю.О. Карпышевой, Е.С. Кемали, Н.О. Кирюшкиной, Р.М. Махьяновой, М.Л. Огурцовой, Л.В. Потаповой, Р.В. Пузикова, Т.А. Сулейманова, Б.Х. Толеубековой, Т.Б. Хведелидзе, К.В. Цепелева, М.М. Челпановой, Д.В. Шабарова, С.В. Шпорт, В.В. Яцуценко и других.

Отдельные аспекты цифровизации, применения современных технологий для идентификации и аутентификации лиц, в том числе в рамках расследования различных преступлений, вопросы биометрических персональных данных, обработки персональных данных с помощью искусственного интеллекта отражены в трудах представителей цифровых наук, уголовного процесса и криминалистики: А.А. Арямова, А.А. Баймаханова, Д.В. Бахтеева, С.Н. Бачурина, Е.Н. Бегалиева, Ю.В. Грачевой, С.А. Гречаного, Н.О. Дулатбекова, С.К. Идрышевой, Г.С. Кодашевой, А.И. Лукьянчикова, А.М. Нурмагамбетова, В.Н. Пахомова, Р.К. Сарпекова, В.В. Синкевич, А.В. Сырбу, Ж.У. Тлембаевой и других.

Однако проблемой таких исследований является недостаточное освящение отдельных аспектов осуществления прокурорского надзора в сфере персональных данных и их защиты, роли прокуратуры в вопросах защиты персональных данных, в особенности после внесения фундаментальных изменений в законодательства о прокуратуре, а также придания закону о прокуратуре конституционного статуса. Роль органов прокуратуры в работе по защите персональных данных практически не исследовалась.

В этой связи следует отметить, что, несмотря на наличие существенного интереса учёных к проведению исследований в данной сфере, всё ещё остаётся ряд неизученных вопросов, которые требуют системного и основательного подхода.

Целью исследования является совершенствование организационно-правовых и практических средств, методов и особенностей защиты персональных данных, в том числе прокурорского надзора за соблюдением законности в сфере персональных данных и их защиты.

Задачи исследования:

- предложить авторские дефиниции, охватывающие предметную область защиты персональных данных;

- разработать внутреннюю систему принципов прокурорского надзора в сфере защиты персональных данных;

- внести предложения по совершенствованию действующего законодательства в сфере защиты персональных данных;

- выработать методические предложения и практические рекомендации по организации и проведению проверок в сфере защиты персональных данных;

- проанализировать и предложить современные научно-технические средства и информационные системы, обеспечивающие защиту персональных данных;

- сформулировать элементный состав правовых средств прокурора в сфере защиты персональных данных.

Объектом исследования являются средства, методы и особенности защиты персональных данных, в том числе организации прокурорского надзора за соблюдением законности в сфере персональных данных и их защите.

Предметом исследования являются методологические исследования теории прокурорского надзора, а также защиты персональных данных.

Теоретическую основу научно-исследовательской работы составляют научные статьи и исследования отечественных и зарубежных ученых, которые посвятили свои труды вопросам защиты персональных данных, прокурорскому надзору, а также более узким проблемам, связанным с данными вопросами.

Методологической основой данного исследования является система методов гносеологического и диалектического анализа, синтеза, дедукции и индукции, а также других общетеоретических и специально-юридических методов, которые в совокупности позволили раскрыть основные вопросы осуществления прокурорского надзора в сфере персональных данных и их защиты. В работе также используются метод правовой типологии, анкетирования, логические схемы анализа, обобщения, сравнения и сопоставления полученной информации. При помощи эффективного соединения указанных методов научного исследования удалось обосновать наиболее подходящие подходы к организации прокурорского надзора в сфере персональных данных и их защиты Представленное научное исследование проводилось также на основании пропорциональной сублимации методов эмпирического анализа и теоретического исследования соответствующей проблематики.

Кроме того, использованы психологический, аксиоматический методы, проведена беседа и обсуждение проблем по рассматриваемому вопросу с сотрудниками Генеральной прокуратуры, а также Службы защиты персональных данных Грузии и Департамента полиции г. Тбилиси (Грузия).

Использование формально-логического метода позволило уточнить понятийный аппарат, относящийся к персональным данным и их защите. Путем системно-структурного анализа проведена комплексная оценка организационной практики осуществления прокурорского надзора в сфере

персональных данных и их защиты. Применение сравнительно-правового анализа позволило выявить основные направления дальнейшего развития законодательства в области персональных данных и их защиты, а также организации прокурорского надзора в этой сфере, в том числе с применением современных технологий.

Приемы юридической техники использовались при подготовке авторских дефиниций, охватывающих предметную область защиты персональных данных. Социологический метод применялся в ходе анкетирования 127 граждан по вопросам, связанным с персональными данными. Метод наблюдения заключался в визуальном восприятии и оценке непосредственной работы сотрудников органов прокуратуры по защите персональных данных. Все указанные методы научного познания обеспечили выполнение требований комплексного подхода к диссертационному исследованию.

Нормативную базу исследования составили: Конституция Республики Казахстан, Уголовный и Уголовно-процессуальный кодекс Республики Казахстан, конституционные законы Республики Казахстан, международные пакты и Конвенции, законы, а также нормативные правовые акты Генеральной прокуратуры Республики Казахстан, Министерства внутренних дел Республики Казахстан, а также другие нормативно-правовые акты, регулирующие вопросы прокурорского надзора и защиты персональных данных.

Эмпирическую основу данного исследования составили доступные в электронном виде статистические данные Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстана (далее – КПСиСУ) в период времени с 2013 года по 2024 год. В диссертации анализируются результаты анкетирования респондентов – 127 лиц, из которых 104 обладали средним и высоким уровнем познаний в сфере юриспруденции (Приложение А).

Кроме этого, использованы материалы судебной и следственной практики, государственные программы, доклады, аналитические обзоры, справки, а также иные материалы о деятельности государственных, правоохранительных органов и органов прокуратуры Республики Казахстан, зарубежных государств и международных организаций.

Методология написания данной работы основывается на осуществлении исследования в три взаимосвязанных этапа.

Первый этап включил сбор и систематизацию теоретической базы исследования, её фундаментальное изучение с целью дальнейшего изыскания неразрешённых проблем в исследуемой теме, формирования научно-теоретического обоснования актуальности представленной темы исследования. На данном этапе написания научной работы также была сформулирована методология исследования, определена система методов, что позволило в наибольшей мере раскрыть тему, произвести анализ проблемы осуществления прокурорского надзора в сфере персональных данных и их защиты. Важное значение на данном этапе имела постановка целей и задач исследования.

На следующем этапе произведён аналитический обзор информации о текущей ситуации и перспективах соблюдения законности в сфере персональных данных и их защиты, а также изучение передовой опыт защиты персональных данных. Также на втором этапе исследования значительное внимание уделено исследованию принципов, правовых средств и инструментов прокурорского надзора в сфере персональных данных и их защиты. Такой подход позволил более системно и основательно подойти к решению проблемы повышения эффективности методики осуществления прокурорского надзора в сфере персональных данных и их защиты.

На заключительном этапе представленной научно-исследовательской работы систематизированы результаты проведённого анализа, что позволило достичь поставленных цели и задач исследования. На основании такого обобщения полученных результатов исследования, были сформулированы практические рекомендации, направленные на повышение эффективности прокурорского надзора в рассматриваемой сфере. Кроме того, удалось удостовериться в том, что сформулированные в ходе написания работы выводы и предложения могут быть использованы для дальнейшего развития научных исследований защиты персональных данных и прокурорского надзора, а также для повышения практических навыков работы государственных служащих, сотрудников правоохранительных органов, судей и других категорий лиц, задействованных в вопросах защиты персональных данных.

Положения, выносимые на защиту:

1. Предложены следующие авторские дефиниции:

- «персональные данные» – сведения, совокупность информации, прямо или косвенно относящиеся к определенному или определяемому физическому лицу, являющемуся субъектом (носителем) персональных данных;

- «специальные персональные данные» – особо личные сведения, сбор, обработка и распространение которых могут повлечь чувствительные последствия для субъекта данных, в том числе данные о судимости, расовом или национальном происхождении, родовой принадлежности, политических взглядах, религиозных и других убеждениях, данные о состоянии здоровья и интимной жизни, смене пола и пр.;

- «биометрические данные» – персональные данные, которые позволяют установить личность субъекта персональных данных на основе характеризующих его физиологических, биологических признаков и поведенческих особенностей (цифровая фотография, отпечатки пальцев и (или) кистей рук, изображение радужной оболочки глаз, рисунок вен, геометрия ушных раковин, сигналы мозга, почерк, походка, динамика нажатия клавиш и другие биометрические персональные данные) (Приложение Б).

2. Исходя из обширного разнообразия междисциплинарных и отраслевых основополагающих начал, охватывающих исследуемую совокупность, в качестве ключевого принципа прокурорского надзора в сфере защиты персональных данных определено принятие исчерпывающих мер по обеспечению законности, защите и восстановлению нарушенных прав и свобод

человека и гражданина, охраняемых законом интересов юридических лиц, общества и государства в сфере персональных данных и их защиты.

3. Преследуя цель совершенствования действующего законодательства Республики Казахстан по вопросам, отнесенным к защите персональных данных, считаем целесообразными следующие изменения:

- перевод частей 1 и 2 статьи 147 Уголовного кодекса Республики Казахстан в категорию дел частно-публичного обвинения, ввиду того, что на сегодня они относятся к категории дел частного обвинения, которые не предполагают проведение досудебного расследования, а также возлагают обязанности по сбору и предоставлению суду доказательств на частных обвинителей, что в условиях отсутствия их доступа к служебной документации, информационным системам, компьютерной или иной технике обвиняемого лица в большинстве случаев лишает возможности представления суду доказательств, подтверждающих несоблюдение мер по защите персональных данных, а также незаконный сбора и (или) обработку (за исключением распространения) персональных данных, что в итоге влечет оправдание лиц даже по реальным фактах нарушения законодательства о персональных данных и их защите;

- в статью 147 Уголовного кодекса Республики Казахстан добавить примечание: «Примечание. В настоящей статье под существенным вредом правам и законным интересам лиц в результате несоблюдения мер по защите и незаконной обработки персональных данных следует понимать нарушение права на защиту персональных данных, чем потерпевшему лицу причинен имущественный и (или) неимущественный ущерб»;

- ввести уголовную ответственность за распространение или угрозу распространения, без согласия лица, фото и (или) видеоизображений его обнаженного тела и (или) половых органов;

- внести изменения и дополнения в нормативные постановления Верховного Суда Республики Казахстан №1 от 11.05.2007 года, №4 от 11.05.2007 года, №6 от 11.04.2002 года, №6 от 23.06.2006 года, №3 от 14.05.1998 года и №7 от 28.12.2009 года, согласно которым преступления, предусмотренные ст.ст. 105, 123, 132, 134, 144, 194, 298, 299, 308, 312, 415, 422 Уголовного кодекса Республики Казахстан, могут совершаться под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких (Приложения Б, В).

4. Обоснованы алгоритмы и механизмы проведения предметных проверок, направленных на соблюдение законности в сфере применения законодательства о персональных данных и их защите, по следующим приоритетным направлениям: в деятельности уполномоченного органа в сфере защиты персональных данных; в деятельности государственных органов и их должностных лиц по вопросам соблюдения законодательства о персональных данных и их защите; в деятельности местных исполнительных органов по

вопросам реализации их компетенции; в деятельности собственников и операторов баз, содержащих персональные данные; в деятельности правоохранительных, специальных и иных государственных органов относительно законности получения пользователями сведений из СИО ПСО, ЕРДР, ЕРАП и других информационных систем; в иных случаях, в том числе по поручениям Президента и Генерального Прокурора Республики Казахстан.

5. Для повышения максимальной защищенности баз персональных данных, с целью исключения фактов несанкционированного применения компьютеров, лицами, не имеющими соответствующего права их использования, а также фиксации сведений о пользователе и его действиях, апробирована и внедрена авторская разработка, в формате полезной модели, «Компьютерная мышь со встроенным RFID – датчиком» (Патент №8815 от 02.02.2024 года) (Приложение Г).

6. Обоснована авторская концепция правовых средств прокурора в сфере защиты персональных данных, содержание которых включает в себя следующие структурные элементы, объединенные по групповому признаку: правовые средства прокурорского надзора по выявлению нарушений закона; правовые средства прокурорского надзора по восстановлению нарушений законности; правовые средства прокурорского надзора по привлечению к ответственности виновных лиц; правовые средства прокурора по координации, межведомственному взаимодействию; правовые средства по реализации иных полномочий прокурора.

7. Путем изменения и дополнения Кодекса «О браке (супружестве) и семье» целесообразно введение обязательного медицинского обследования лиц, планирующих вступление в брак, а также обмена между ними персональными данными и внедрение для этих целей Паспорта персональных данных в бумажном и электронном виде, интегрированном с сервисами электронного правительства, который будет содержать сведения о наличии/отсутствии судимости, ВИЧ-статусе, врожденных и приобретенных заболеваниях, способных повлиять на потомство, наличии предыдущих браков, детей и обязательств перед ними, непогашенной задолженности, образовании, наличии недвижимого имущества, долей в юридических лицах и др. (Приложение Д).

Теоретическая и практическая значимость исследования.

Основу методологического подхода в представленной научно-исследовательской работе составляют пропорциональное соединение общетеоретических и специально-юридических методов исследования, при помощи которых были раскрыты правовые основы прокурорского надзора за соблюдением законности в сфере персональных данных и их защите.

Главными результатами, достигнутыми в ходе написания этого труда, следует считать: разработку авторских дефиниций; внутренней системы принципов, правовых средств прокурора и методических рекомендаций по организации прокурорского надзора в сфере защиты персональных данных (Приложение Е); проведение анализа современных и предложение новых научно-технических средств по защите персональных данных.

Результаты данного научного исследования, а также сформулированные выводы, имеют большое практическое и научно-теоретическое значение, как для сотрудников органов прокуратуры, принимающих непосредственное участие в надзорной деятельности, так и для других органов, задействованных в защите персональных данных граждан. Как следствие, произведённый в данной работе научно-правовой анализ позволит существенно повысить эффективность прокурорского надзора за соблюдением законности в сфере персональных данных и их защите.

Апробация и внедрение результатов исследования.

Результаты диссертационного исследования отражены в выступлениях, научных статьях на конференциях международного и республиканского уровней, в качестве рекомендаций по совершенствованию действующего законодательства по данной проблеме.

Выводы и предложения, сформулированные в процессе исследования, могут быть использованы:

а) для углубления и расширения научных представлений по реализации прокурорского надзора за соблюдением законности в сфере персональных данных и их защите;

б) в правотворчестве при совершенствовании соответствующих норм законодательства о персональных данных и их защите;

в) в учебно-образовательном процессе, при подготовке магистерских и докторских работ, проведении научных исследований по указанной проблеме.

Основные положения и результаты, содержащиеся в диссертации, обсуждались на заседании кафедр Академии правоохранительных органов при Генеральной Прокуратуре Республики Казахстан, а также нашли отражение в 9 опубликованных статьях по исследуемой проблематике. В их числе 4 публикации в журналах, рекомендованных Комитетом по обеспечению качества в сфере науки и высшего образования Министерства науки и высшего образования Республики Казахстан; 3 – в сборниках по материалам международных – научно-практических конференций; 1 – патент на полезную модель; 2 – в журналах, входящих в базу данных Scopus.

Был издан Терминологический словарь терминов в сфере защиты персональных данных.

Выводы и по результатам настоящего исследования получены акты внедрения в следующих организациях:

1. Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан.

2. Генеральной прокуратуре Республики Казахстан.

3. «Digital Rights Center Qazaqstan».

4. Академии правосудия при Высшем Судебном Совете Республики Казахстан.

Практическая ценность диссертации подтверждается актами внедрения вышеуказанных организаций (Приложение Ж).

Структура диссертации.

Структура и объем диссертации обусловлены характером изучаемых вопросов, уровнем разработанности темы исследования, логической последовательностью излагаемых аспектов. Диссертация состоит из введения, трех разделов, включающих семь подразделов, заключения, списка использованных источников и приложений. Диссертационное исследование выполнено в объеме, который соответствует требованиям, предъявляемым Комитетом по обеспечению качества в сфере науки и высшего образования Министерства науки и высшего образования Республики Казахстан.

1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРОКУРОРСКОГО НАДЗОРА ЗА СОБЛЮДЕНИЕМ ЗАКОННОСТИ В СФЕРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИХ ЗАЩИТЕ

1.1 Современное состояние и перспективы соблюдения законности в сфере персональных данных и их защите

В современных условиях развития информационно-коммуникационных технологий невозможно обеспечить полную анонимность. Различные данные, такие как время передачи информации, объем информации, используемый протокол, формат и т.д. могут быть фиксированы. Поэтому при обеспечении защиты и конфиденциальности передачи и получения персональной информации необходимо учитывать соображения о целесообразности и необходимости обеспечения общественной и государственной безопасности. Человек является частью социума, в связи с чем оборот некоторых персональных данных может осуществляться вне зависимости от его желания.

Защита персональных данных не означает полное ограничение доступа к этим данным. Важным аспектом является организация правильной процедуры получения и использования персональной информации, которая предусматривает информирование субъектов данных о целях использования их персональных данных и предоставление доступа к информации о накопленных сведениях. Конфиденциальность информации означает обеспечение защиты доступа к персональным данным. Персональные данные являются достаточно сложным объектом, поскольку они сами могут быть предметом противоправного посягательства, а также незаконные действия могут совершаться с их использованием. При этом с помощью персональных данных ущерб может причиняться, как субъекту, к которому они относятся, так и третьим лицам, не имеющим к нему никакого отношения.

Достаточно высокий уровень внимания защите приватности и личных данных обосновывается постоянным ростом цифровизации в мире, которая предполагает массированный сбор информации, в том числе персонального характера, а также тем, что неправомерным сбором и обработкой персональных данных нередко грубо нарушаются конституционные права граждан.

Из отчетов специализирующейся на кибербезопасности компании Positive Technologies за 2023 год и первое полугодие 2024 года следует, что во всем мире точное количество атак, в результате которых злоумышленники добились успеха, неизвестно, поскольку скомпрометированные организации не заинтересованы в обнародовании таких данных ввиду возможных репутационных и финансовых последствий. При этом число успешных кибератак в мире все же остается высоким, а более половины из них приводят к утечке конфиденциальных данных. Более трети всех похищенных у организаций сведений относятся к персональным данным. В даркнете из общего количества объявлений о продаже или передаче всех типов данных персональные данные составляют 83%.

По оценкам компании в 2017-2022 годах во всем мире произошла утечка более 75,2 млрд. единиц платежной информации и персональных данных.

Похищение данных влечет существенные финансовые убытки для коммерческих организаций. К примеру, в 2024 году последствия кибератаки на крупнейшую в США компанию в области медицинского страхования «U.», а также последовавших коллективных исков от пострадавших лиц вылились в убытки для компании, превышающие 2 млрд. долларов США. Подобных примеров немало и в других государствах. При этом нередко результатом кибератак является банкротство компаний. Также зачастую финансовые потери несет и государство. Например, функционировавший несколько лет бесплатный VPN-сервис «9.» оказался крупной бот-сетью, которая осуществляла сбор данных пользователей и использовала их в мошеннической схеме для получения выплат по безработице, чем Правительству США причинён ущерб на почти 6 млрд. долларов США.

Из отчетов компании Positive Technologies также можно выделить, что утечки нередко происходят в деятельности операторов связи. Так, в начале 2024 года в Индии произошла крупная утечка данных 750 млн. пользователей операторов связи.

Особо следует отметить, что в 12-13% случаев утечки происходят из государственных органов и данная отрасль фактически является самой уязвимой. Например, во Франции произошла утечка данных 43 млн. человек, которые за последние 20 лет регистрировались в качестве безработных [5].

Для Казахстана данный вопрос также актуален, поскольку в стране отмечается высокий уровень цифровизации и пользователей интернета.

Согласно ежегодному отчету «Digital 2023: Global Overview Report», который опубликован совместно сервисом «Datareportal», агентством «We Are Social» и аналитической платформой «Meltwater», на начало 2023 года число пользователей интернета в мире составило почти 4,8 млрд. Отчет содержит сведения отдельно по различным государствам, в том числе и касательно Казахстана. Из этого отчета следует, что на начало 2023 года в Казахстане насчитывалось 17,8 млн. интернет-пользователей, 11,9 млн. пользователей социальных сетей и было активно 25,5 млн. сотовых мобильных подключений, что свидетельствует о постоянном использовании интернета большей частью населения нашей страны [6]. Безусловно, большинство из них на постоянной основе осуществляет обработку своих персональных данных в сети Интернет и социальных сетях, что подвергает такую информацию риску.

Огромный массив информации аккумулируется в результате активной цифровизации различных сфер, связанных как с длительностью государства, так и бизнеса. В рейтинге ООН Global E-Government Development Index на 2022 год по развитию электронного правительства Республика Казахстан занимает 28 место из 193 стран [7]. В Центральной Азии Казахстан является ведущей страной по развитию электронного правительства [8].

Казахстанский портал «Электронного правительства» Egov.kz запущен в 2006 году в рамках реализации Указа Президента Республики Казахстан от

10.11.2004 года №1471 «О государственной программе формирования «электронного правительства» в Республике Казахстан на 2005-2007 годы», как информационный ресурс относительно государственных услуг [9]. В дальнейшим портал трансформировался, у граждан появилась возможность с его помощью получать государственные услуги в электронном формате без взаимодействия с государственными органами. В настоящее время из более 1300 видов государственных услуг 90% автоматизированы на портале. За первое полугодие 2024 года казахстанцы получили более 20 миллионов государственных услуг через портал eGov и его мобильную версию. Всего за период действия портала гражданам оказано более 450 миллионов государственных услуг, а через мобильное приложение 66 миллионов услуг [10]. 04.03.2020 года в ходе совещания по цифровизации Казахстана продемонстрирована информационно-аналитическая система Smart Data Ukimet, в рамках которой интегрированы порядка 100 информационных баз государственных органов, содержащих значительный объем информации, в том числе персональных данных. Также в Казахстане действует проект Smart Bridge, направленный на упрощение процессов интеграции информационных систем между государственными структурами и частным бизнесом. По данным АО «Национальные информационные технологии» с 2020 года проведено почти 4 тысячи интеграций [11]. Данные интеграции с одной стороны нередко значительно упрощают жизнь граждан, лишая их необходимости прохождения сложных бюрократических процедур, но с другой стороны они же ставят персональные данные граждан под угрозу, как в части возможного похищения, так и в виде необоснованного доступа к ним третьих лиц.

Все базы персональных данных находятся под серьезной угрозой взлома и похищения сведений. На постоянной основе злоумышленники путем кибератак, взломов, разработки и распространения вредоносного программного обеспечения, вирусов, фишинга и других противоправных действий пытаются незаконно завладеть личными сведениями граждан. По оценкам специалистов в области информационной безопасности в Республике Казахстан в 2018–2020 годах с баз данных государственных органов и негосударственных организаций, осуществляющих сбор и обработку персональных данных, произошла утечка более 11 млн. записей личной и платежной информации пользователей. Однако, никакой официальной информации в этой направлении в свободном доступе не имеется и можно с уверенностью утверждать, что объемы похищенных сведений гораздо выше. Сколько еще имелось подобных случаев остается неизвестным.

В 2020 году Центром анализа и расследования кибератак (ЦАРКА) изучена защищенность веб-ресурсов государственных организаций Республики Казахстан. В результате из 91 исследованного веб-ресурса в 12 выявлены уязвимости, в 6 обнаружены факты утечек, в 29 незащищенность электронной почты, а также другие негативные факторы, дающие возможность для успешных кибератак злоумышленников [12].

Проведенное анкетирование 127 лиц, из которых 104 обладали средним и высоким уровнем познаний в сфере юриспруденции, показало, что только 4% считают уровень защищенности персональных данных в Казахстане достаточным, 13,4% считают, что защищены только отдельные виды данных, 14,2% полагают, что персональные данные не защищены вообще, а 54,3% убеждены в недостаточности уровня защищенности. 98,3% опрошенных лиц опасаются утечки своих данных (Приложение И).

С 2018 года в Казахстане функционирует Национальный координационный центр информационной безопасности, обеспечивший защиту информационных ресурсов государственных органов и критически важной информационной инфраструктуры Республики от кибератак и киберинцидентов. В 2022 году удалось отразить порядка 28 млн. атак.

Также функционирует отраслевой центр информационной безопасности, осуществляющий анализ, оценку, прогнозирование и профилактику угроз кибербезопасности финансового рынка и финансовых организаций в Казахстане. За 2021 год центром зафиксировано и отработано более 75 тысяч событий информационной безопасности в банках второго уровня, в том числе 61 тысячи кибератак.

В 2021 году внедрена система «контроль доступа к персональным данным», которая предусматривает комплекс мер по обеспечению защиты персональных данных.

Согласно официальным сведения Государственной технической службы с начала 2023 года отражено 163,4 млн. кибератак на ресурсы государственных органов [13], что подтверждает интерес злоумышленников к данным казахстанцев. Таким образом, в целом, определенная работа по защите государственных информационных ресурсов от хакерских атак уполномоченными государственными органами и организациями проводится, принимаются иные меры, но утечки персональных данных продолжаются.

Многие из похищенных таким образом сведений в дальнейшем используются для необоснованного вмешательства в частную жизнь граждан, похищения персональных данных и в иных противоправных целях. Анализ отечественного законодательства и судебно-следственной практики показывает, что персональные данные могут быть использованы для совершения многих преступлений, включая клевету, оскорбление, вымогательство, разглашение тайны усыновления (удочерения), незаконное нарушение тайны переписки, тайны предоставления микрокредита, коллекторской деятельности тайны, врачебной тайны и многие другие. При этом точной статистики совершения таких преступлений с использованием именно персональных данных не имеется, поскольку такой учет не ведется.

На сегодня одной из самых серьезных проблем является использование персональных данных граждан для совершения интернет-мошенничества и других киберпреступлений. По оценкам компании Javelin Strategy & Research в США от мошенничества с персональными данными в 2021 году пострадали 42 миллиона американцев, а ущерб составил 52 миллиарда долларов США [14]. По

данным КПСиСУ количество интернет-мошенничеств в период с 2018 по 2022 годы выросло с 517 до 20,6 тысяч фактов. Полагаем, что статистика не отражает реальной ситуации. В 2023 году зарегистрировано 21,8 тысяч таких уголовных правонарушений и в 2024 году тенденция роста подобных преступлений сохранилась. Интернет-мошенничества составляют практически половину (48,6%) от всех совершенных мошенничеств в стране и за последние 2 года ущерб от таких противоправных деяний составил более 30 млрд. тенге. Уровень раскрытия таких киберпреступлений не превышает 15%. Н.К. Имангалиев отмечает, что расследование такой категории дел осложнено тем, что значительная часть из них совершается с территории других государств, для совершения преступлений используются прокси–серверы и «сайты-однодневки», а также имеются проблемы взаимодействия с банками и администрацией интернет-сайтов, социальных сетей и мессенджеров [15].

В целом, по данным Министерства внутренних дел Республики Казахстан за последние 5 лет число киберпреступлений в нашей стране выросло почти в 3 раза. При этом абсолютное большинство всех киберпреступлений составляют интернет-мошенничества.

Институтом общественной политики в 2023 году проведено социологическое исследование, респондентами в котором выступили 8 тысяч казахстанцев. Исходя из результатов данного исследования каждый 3 опрошенный сталкивался с попытками интернет-мошенничества, а 31,4% респондентов относят проблему кибермошенничества к числу наиболее острых в стране и считают необходимым уделить ей первоочередное внимание [16].

Проведенное анкетирование 127 лиц, из которых 104 обладали средним и высоким уровнем познаний в сфере юриспруденции, показало, что адрес 26,8% опрошенных редко поступают звонки от лиц, представлявшихся сотрудниками банков или государственных органов, из разговора с которыми становилось понятно о наличии у них персональных данных, 39,4% такие звонки поступают часто, 8,7% очень часто, еще 12,6% опрошенных лиц такие звонки не поступали, но они слышали о таких фактах (Приложение И).

В целом, мировые тенденции, а также анализ текущей ситуации позволяют сделать вывод, что в ближайшей перспективе не исключается значительный рост уровня интернет-преступности. При этом можно выделить ряд факторов, одним из которых является расширение применения искусственного интеллекта.

В октябре 2023 года, К.К. Токаев, выступая на форуме Digital Bridge, поручил принять стратегический документ, определяющий задачи и инструменты развития искусственного интеллекта. 24.07.2024 года постановлением Правительством Республики Казахстан №592 утверждена «Концепция развития искусственного интеллекта на 2024-2029 годы». Изучение данного документа свидетельствует о значительном расширении применения данной технологии. Также Концепция предусматривает принципы реализации развития искусственного интеллекта, к которым относятся безопасность и конфиденциальность. Принцип конфиденциальности дополняет

безопасность, отдельно акцентируя внимание на необходимости обеспечить защиту персональных данных, частной жизни человека и других охраняемых законом тайн [17].

При этом нельзя не отметить, что уже сейчас возможности искусственного интеллекта активно применяются для совершения киберпреступлений. С расширением технологии их станет еще больше.

Компанией Onfido в 2024 году опубликован Отчет о мошенничестве с личными данными, из которого следует, что в мире в 31 раз увеличилось число мошенничеств с использованием дипфейков, то есть видео и аудио файлов, генерированных с использованием искусственного интеллекта. По оценкам специалистов Onfido 2024 год станет годом дипфейков, поскольку количество цифровых атак увеличивается [18]. Данная тенденция отчетливо ощущается и в Казахстане, где в последнее время имело место немало сгенерированных нейросетями видео известных личностей и высокопоставленных чиновников, в которых они призывали осуществлять инвестиции в те или иные платформы, не имеющие какого-либо отношения к государству.

М.Б. Добробаба считает, что дипфейк-технологии несут угрозу не только правам человека, но и в целом для государства, а в ближайшей перспективе могут стать угрозой национальной безопасности [19].

Следует отметить, что утечка и похищение персональных данных не всегда осуществляются только хакерами. Безусловно, в определенной степени на неконтролируемый сбор персональных данных влияет слабая кибергигиена самих граждан, пользователей сети Интернет и различных цифровых продуктов. Также можно выделить «человеческих фактор», а также умышленную передачу чужих сведений, в том числе в противоправных целях. При этом последним двум направлениям уделяется меньше всего внимания, тогда как на сегодня в Казахстане более 1,3 тысяч государственных услуг оказываются онлайн, функционирует около 100 государственных баз данных, серьезным ресурсом является «Smart Data Ukimet». Доступ к государственным базам данных имеют не меньше 200 тысяч человек, к числу которых относятся государственные служащие, сотрудники правоохранительных и специальных органов, работники государственных учреждений, НАО «Правительство для граждан», частные судебные исполнители, нотариусы и многие другие лица.

К примеру, в 2019 году в г. Алматы по пункту 3 части 2 статьи 211 Уголовного кодекса Республики Казахстан осуждена инспектор центра обслуживания населения А. за незаконную передачу своей знакомой персональных данных третьего лица, с использованием которых в дальнейшем на него оформлены кредиты на покупку дорогостоящей техники [20].

Ожидается, что количество государственных услуг и баз данных будет увеличиваться. Соответственно, будут расти количество накапливаемой на них информации и персональных данных, а также риски их утери.

Стремительно растет количество негосударственных баз данных, осуществляющих сбор личных данных граждан. Их точное число неизвестно.

Обеспечить эффективный контроль за всеми лицами, использующими государственные и негосударственные базы данных, содержащих персональные данные, крайне проблематично.

Необходимо отметить, что в Плане действий по реализации Концепции развития искусственного интеллекта 2024-2029 годы предусмотрены мероприятия по обеспечению доступа бизнеса к государственным данным.

А.В. Ендольцева и Ю.В. Ендольцева отмечают важность принятия технических, организационных и правовых превентивных мер в целях противодействия бесконтрольному распространению персональных данных и их незаконному использованию [21].

Таким образом, текущая ситуация в мире и Казахстане свидетельствует о высоком риске утечки персональных данных, непрекращающихся попытках злоумышленников похитить данные с информационных систем, баз данных, в особенности относящихся к государственным органам. Выбранная Республикой Казахстан траектория активной цифровизации практически всех сфер общественных отношений приносит как положительные результаты, так и повышает угрозу утечки персональных данных. Во избежание негативных последствий, а также учитывая запланированное Республикой Казахстан активно использование возможностей искусственного интеллекта, сбора больших данных, интеграции государственных сервисов с информационными системами бизнеса, в целях защиты персональных данных требуется принятие комплекса технических, организационных, правовых и иных мер.

Эффективная защита персональных данных невозможно в отсутствии действенного законодательства либо в условиях его несовершенства.

В Республике Казахстан права на защиту частной жизни и персональных данных впервые были закреплены в принятой в 1993 году Конституции Республики Казахстан (утратила силу). В Конституции Республики Казахстан 1995 года (действующая) сохранилась неприкосновенность частной жизни, однако положения о запрете вмешательства в нее не были заложены. При этом к частной жизни добавились личная и семейная тайны, которые также стали неприкосновенными. В свою очередь, требования относительно порядка использования информации личного характера (сбора, хранения, использования и распространения) из числа конституционных положений были исключены (статья 18) [22, 23].

Более подробно определение понятиям «неприкосновенность частной жизни», «личная и семейная тайны» дано в научно-практическом комментарии к Конституции, изданном Конституционным Советом в 2018 году. В частности, указывается, что неприкосновенность частной жизни, личная и семейная тайна, защита чести и достоинства человека относятся к числу определяющих факторов конституционно-правового статуса человека и гражданина в Республике Казахстан. Они охраняются законодательством, но в то же время допускается ограничение этих прав в установленных Конституциях случаях. Личная и семейная тайны являются частью частной жизни и содержат сведения о деликатных и интимных сторонах жизни человека, которые он считает

нежелательными к разглашению. Личная тайна предполагает право индивида на самостоятельное регулирование режима информации и требование его соблюдения. Семейной тайной признает право лиц, связанных кровными и(или) родственными узами на сокрытие фактов, определяющих поведение членов семьи. При этом в семье может быть общая семейная тайна, а также личная тайна отдельного члена семьи [24].

Нельзя не отметить, что согласно пункту 2 статьи 20 Конституции Республики Казахстан каждый имеет право свободно получать и распространять информацию любым, не запрещенным законом способом. Данная норма вступает в некоторое противоречие и создает конкуренцию норм с правом на неприкосновенность частной жизни, личную и семейную тайну. Такая проблема характерна для многих государств, поскольку права на неприкосновенность частной жизни и свободу информации являются равновесными, а баланс между защитой частной жизни и свободой слова зачастую регулируется судебной практикой и законами.

В 1999 году Межпарламентской Ассамблей государств-участников СНГ принят Модельный закон «О персональных данных».

Однако, только 21.05.2013 года в Казахстане принят Закон Республики Казахстан «О персональных данных и их защите» [25]. Для сравнения, в Российской Федерации Федеральный закон «О персональных данных» был принят еще в 2006 году. Немного ранее, а именно в 2001 году от имени Российской Федерации подписана, а в 2005 году ратифицирована Конвенция о защите физических лиц при автоматизированной обработке персональных данных 1981 года [26]. Еще раньше, а именно 08.10.2002 года Закон «О персональных данных» был принят в Республике Армения. В 2015 году этот правовой акт утратил силу и был принят новый Закон «О защите личных данных» [27]. Следует отметить, что указанную Конвенцию 1981 года ратифицировали многие неевропейские государства (всего более 50), в числе которых следует выделить Армению, Азербайджан, Грузию, Молдову и Беларусь [28]. К сожалению, следует констатировать тот факт, что Республика Казахстан к указанной Конвенции до настоящего времени не присоединилась [29].

Исходя из Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023-2029 год, утвержденной постановлением Правительства Республики Казахстан №269 от 28.03.2023 года, Казахстаном в ближайшее время будут рассмотрены вопросы присоединения к данной Конвенции, что даст право расследовать нарушения прав наших граждан в сфере защиты персональных данных, совершаемых операторами стран, присоединившихся к Конвенции [30].

Из международных договоров, к которым присоединилась Республика Казахстан, можно отметить ратифицирование в апреле 2022 года Соглашения о взаимной правовой помощи по административным вопросам в сфере обмена персональными данными. Сторонами данного Соглашения являются участники Содружества Независимых государства (СНГ) [31].

Н.И. Петрыкина указывает, что «институт персональных данных образуют следующие группы правовых норм:

Нормы, закрепляющие понятие, виды, конфиденциальность персональных данных. Это весьма обширный блок норм, составляющих основу всего института. В него входят нормы, закрепляющие определение персональных данных; устанавливающие их разграничение по видам и, соответственно, режимам оборота и охраны, а также закрепляющие и реализующие такое важнейшее свойство персональных данных, как конфиденциальность.

Нормы, закрепляющие правовой статус субъектов отношений, связанных с оборотом персональных данных (субъект персональных данных, оператор, пользователь, государство, третьи лица). Данными нормами регулируются права, обязанности и правосубъектность всех участников отношений по сбору и обработке персональных данных.

Нормы, регулирующие обработку персональных данных, составляют важнейший элемент рассматриваемого института и опосредуют правомерное использование персональных данных в личных, общественных и государственных целях.

Нормы, регулирующие контрольно-надзорные отношения, составляют важный блок отношений и опосредуют деятельность уполномоченных органов исполнительной и судебной власти, других государственных органов по контролю и надзору за соблюдением законности в сфере сбора и обработки персональных данных.

Наконец, нормы об ответственности закрепляют основания, порядок применения и виды юридической ответственности за правонарушения в сфере персональных данных и их защиты» [32].

В принятом в 2013 году Законе Республики Казахстан «О персональных данных и их защите» с учетом его последующей доработки все указанные группы правовых норм нашли свое отражение. При этом следует понимать, что институт защиты персональных данных в Казахстане является относительно молодым институтом, поэтому законодательство в этой сфере находится в процессе постоянной трансформации, дополнения и изменения. При этом немало исследователей выступают с критикой законодательства Казахстана в сфере защиты персональных данных.

К примеру, С.А. Акилов считает, что «в универсальном международно-правовом соглашении в сфере защиты персональных данных при трансграничной передаче информации необходимо определить такие важные аспекты как: сфера охвата и возможные исключения; субъектный состав; основные определения (данные; субъект данных; пользователь данных и т.д.); основные принципы; случаи ограничения права доступа; конфиденциальность и безопасность; права субъекта данных; обработка данных и критерии законной обработки; санкция и административная или судебная защита» [33].

В соответствии с пунктом 2 статьи 1 Закона Республики Казахстан «О персональных данных и их защите» под персональными данными

понимаются зафиксированные на электронном, бумажном и (или) ином материальном носителе сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных. Под субъектом персональных данных (пункт 16 статьи 1 Закона) понимается физическое лицо, к которому относятся персональные данные.

Специалисты «Digital rights center», сравнив дефиниций понятия «персональные данные» в разных странах, пришли к выводы, что хоть и не редко они отличаются, но, как правило, подразумевают сведения, на основании или с помощью которых можно определить, идентифицировать или установить личность лица, являющегося субъектом этих данных [34]. Значимым отличием зарубежных правовых норм от дефиниции, определенной казахстанским законодательством, является отсутствие требований о фиксации персональных данных на каком-либо носителе. Данный подход зарубежных стран в значительной степени выглядит обоснованным, поскольку многие виды персональных данных, в особенности чувствительного характера, такие как, например, сведения о религиозных и политических убеждениях, особенностях сексуального поведения в большинстве случаев не зафиксированы на каком-либо информационном носителе, что может вызвать проблемы при необходимости их защиты.

В.П. Иванский при проведении сравнения европейского законодательства особо отметил тщательную проработку термина «персональные данные» и смежных с ним понятий в финском законодательстве. Помимо самого термина «персональные данные» законодательство предусматривает дефиниции таких понятий, как «файл персональных данных», «файл редакционных данных», «персональные кредитные данные» и «матрикула». Под «матрикулой» понимается любой предназначенный для публикации файл персональных данных, в котором физическое лицо упоминается во взаимодействии с определенными сведениями, такими как статус, профессия, образование, членство в какой-либо организации, экономическая или гражданская деятельность и прочими сведениями [35].

Действительно, в странах Европы, Новой Зеландии, Японии, Южной Корее, Бразилии и многих других государствах под персональными данными понимается любая информация, относящаяся к физическому лицу, которая может быть использована для его идентификации. Из стран СНГ схожий подход избрали Азербайджан, Армения, Белоруссия, Молдова, Россия и Таджикистан. В свою очередь, Казахстан, Кыргызстан, Узбекистан и Туркменистан законодательно закрепили положения о необходимости фиксации такой информации на каком-либо носителе.

Таким образом, изучение законодательного подхода различных государств к определению понятия «персональные данные» показало, что в большинстве случаев под таким сведениями понимается любая информация, которая связана или может идентифицировать субъекта персональных данных. В Казахстане под персональными данными понимается информация, которая зафиксированная на электронном, бумажном и (или) ином материальном

носителе, что сужает понятие и может вызвать определенные сложности на практике.

М.О. Дудко, проанализировав современные подходы к правовому закреплению понятия «персональные данные», пришла к выводу, что «в большинстве государств преобладает достаточно расширительное толкование данного термина, а само определение носит максимально абстрактный характер». При этом автор также отмечает, что ряд государств выбрали подход узконаправленного, специализированного определения понятия «персональные данные», зависящего от сферы применения того или иного правого акта, где закреплено это понятие. Еще одна группа государств избрала смешанный тип определения персональных данных, а именно несмотря на достаточно широкую трактовку термина существует примерный перечень идентификаторов, которые уточняет дефиницию, чем вносят некоторую ясность и определенность. При этом ученые расходятся во мнении о правильности того или иного подхода [36].

В. Писарев, описывая американский подход к регулированию оборота персональных данных, отмечает его отличие от европейского, поскольку в США оно осуществляется на уровне отдельных штатов и отраслей (финансы, страхование, банковская сфера и т.д.). При этом один наиболее масштабных сфер правового регулирования является потребительский сектор. В различных штатах приняты законы о защите конфиденциальности потребителей. Эти законы наделяют потребителей правом знать каким образом используются их персональные данные. Имеются и другие законы, которые определяют порядок обработки персональных данных, вопросы информационной защиты. Автор исследования приводит опыт штата Нью-Йорк, где центральной фигурой, наделенной контрольно-надзорными функциями, обладает Генеральный прокурор штата, на которого возложены функции взаимодействия с лицами и организациями, осуществляющими обработку данных, а также внесение исков по резонансным случаям нарушения прав потребителей в сфере конфиденциальности [37].

Э.М. Омурчиева считает, что «определение «персональные данные» нуждается в доработке, поскольку персональные данные представляют собой не только сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе, но и в целом любую информацию, которая позволяет прямо или косвенно определить идентичность физического лица по разнообразным категориям, как это усматривается в тексте GDPR» [38].

К.А. Гаджиева по итогам исследования правовых актов стран Евразийского экономического союза в сфере защиты персональных данных выделила имеющиеся сходства и различия, а также отметила, что дефиниции персональных данных в целом схожи, но в Казахстане и Кыргызстане они дополнены требованиями о закреплении таких сведений на различных носителях. В целом автор считает, что «есть все условия для дальнейшей

гармонизации норм законов в целях реализации единой цифровой повестки Союза и формирования общего цифрового пространства» [39].

Казахстанское законодательство предполагает наличие персональных данных только у физических лиц и, соответственно, их отсутствие у юридических лиц. Законодательство Исландии, Канады, Бразилии, Австралии, Южной Кореи и других государства предусматривает наличие персональных данных, как у физических, так и у юридических лиц.

Следует отметить, что казахстанское законодательство дает широкое определение понятия «персональные данные» без конкретизации. При этом ни в одном правовом акте нет исчерпывающего перечня персональных данных. Исходя из этого, под персональными данными можно понимать любые сведения, относящиеся к лицу и позволяющие идентифицировать его. С одной стороны с таким подходом можно согласиться, но с другой стороны подобная неопределенность влечет определенные трудности.

М.Б. Добробаба отмечает, что в Российской Федерации схожий подход к определению понятия «персональные данные». При этом автор указывает, что во многих других странах подходы в данном направлении отличаются. К примеру, в Австрии, Исландии и Швейцарии осуществляется защита персональных данных не только физических, но и юридических лиц. В Великобритании осуществляется защита персональных данных только живого лица. Также указанный автор отмечает, что неопределенность понятия и отсутствие исчерпывающего перечня приводит к сложностям правоприменения. Спорным, по мнению ученого, является отнесение к персональным данным IP‑адреса пользователя Сети, электронной почты и телефона, паспортных данных и иных государственных идентификаторов. Для решения поднимаемой проблемы автором предлагается использовать законодательство и судебную практику, а при их отсутствии или невозможности применения использовать метод идентификации, предложенный Н.А. Воронковым, и представляющий собой тест, который позволяет определить личность путем ответа на ряд вопросов о наличии в информации сведений о конкретном человеке, возможности определения субъекта по этой информации [40].

В.Д. Рузанова напротив считает, что установление исчерпывающего перечня персональных данных невозможно, а при наличии сомнений относятся ли какие-либо данные к персональным следует относить их к таковым. При этом большое разнообразие персональных данных, а также сфер их применения усложняют формирование единого правового режима данной информации. Автор считает, что целесообразно признание персональных данных нематериальными благами, выступающими в качестве объекта личного неимущественного права на защиту персональных данных [41].

С.К. Жетписов утверждает, что в Казахстане необходимо утверждение полного перечня персональных данных, а также требуется доработка понятия «распространение персональных данных», в особенности в случаях совершения правонарушений, причинения морального и материального вреда [42].

В настоящее время в Республике Казахстан законодательство в сфере защиты персональных данных можно назвать сформированным. Однако, понятия и предусмотренные казахстанским законодательством меры в значительной степени отличаются от тех, которые закреплены в международных правовых актах и являются ориентиром в защите персональных данных большинства зарубежных государств, что в определенной степени препятствует повышению эффективности работы государственных органов Казахстана по защите персональных данных, в том числе прокурорского надзора в данной сфере. Нельзя не учитывать, что законодательство Казахстана в сфере защиты персональных данных имеет небольшую историю, находится в процессе развития и постоянной трансформации. При этом видится целесообразным при последующем совершенствовании правовых норм учитывать опыт и доказавшие свою эффективность меры зарубежных стран, общепризнанные дефиниции и понятия, а также необходимо рассмотреть возможность присоединения к международным документам в сфере защиты персональных данных.

Стоит отметить, что в юридической литературе последних лет недостаточно комплексных фундаментальных исследований, касающихся выбранной тематики. При этом активная цифровизация и глобализация, а также вероятность серьезных последствий утечки персональных данных требуют дальнейшего и углубленного изучения проблемы с выработкой действенных мер. Также углубленного изучения вопроса требует наличие большого количества законодательных проблем в сфере защиты персональных данных. Одним из наиболее проблемных вопросов на сегодня является определение правового статуса персональных данных.

Статья 6 Закона Республики Казахстан «О персональных данных и их защите» подразделяет персональные данные на общедоступные и ограниченного доступа. Общедоступными персональными данными являются персональные данные или сведения, на которые в соответствии с законами Республики Казахстан не распространяются требования соблюдения конфиденциальности, доступ к которым является свободным с согласия субъекта. Персональными данными ограниченного доступа являются те, доступ к которым ограничен законодательством Республики Казахстан. При этом в законодательстве нет перечня персональных данных, которые следует считать конфиденциальными. В свою очередь, субъекты персональных данных по-разному относятся к свободному доступу к своим данным, в одних случаях желая сохранения их анонимности, а в других напротив желают максимальной публичности.

Не дает ясности и позиция государственных органов. Так, в Информационной системе «Параграф» размещено письмо Министра внутренних дел Республики Казахстан, согласно которому «персональные данные ограниченного доступа - персональные данные, доступ к которым ограничен законодательством Республики Казахстан. К ним относятся установочные данные лица (фамилия, имя, отчества, год, дата рождения,

национальность), сведения о месте жительства (место регистрации), индивидуальном идентификационном номере (ИИН), документах, удостоверяющих личность (номер) и другие сведения» [43].

Несмотря на то, что понятие «персональные данные ограниченного характера» достаточно часто используется в законодательстве, в настоящее время исчерпывающий перечень таких данных нормативно не закреплен. Только в единичным случаях прямо указаны виды персональных данных, доступ к которым ограничен.

Так, согласно пункту 1 статьи 8 Закона «О дактилоскопической и геномной регистрации» дактилоскопическая и геномная информация относится к персональным данным ограниченного доступа [44].

Законы «О государственных секретах», «Об оперативно-розыскной деятельности» и «Об органах национальной безопасности Республики Казахстан» относят к государственным секретам:

- сведения лиц, раскрывающие их принадлежность к кадровому составу органов разведки, контрразведки Республики Казахстан;

- сведения о личности конфиденциальных помощников, оказывающих (оказывавших) содействие в осуществлении разведывательной, контрразведывательной или оперативно-розыскной деятельности;

- сведения о сотрудниках и военнослужащих, выполняющих (выполнявших) задания в специальных службах иностранных государств и иных зарубежных организациях, преступных группах.

Фактически в других законодательных актах Республики Казахстан не указаны иные виды персональных данных ограниченного доступа. При таких обстоятельствах остальные персональные данные при условии наличия согласия субъекта персональных данных на свободный доступ к ним могут быть общедоступными. Это может касаться и персональных данных, которые затрагивают неприкосновенность частной жизни и охраняемые законом тайны (усыновления, медицинского работника и другие). В то же время не ясно, если субъектом персональных данных не дано согласие на свободный доступ к его персональным данным, считаются ли они персональными данными ограниченного характера.

Такой подход, на наш взгляд, имеет больше минусов, чем плюсов, поскольку вся ответственность по определению общедоступности персональных данных возлагается на их субъекта, но неясным остается будет ли его согласие на доступ к персональным данным касаться конкретной ситуации либо такое согласие будет считаться выданным для неограниченного количества лиц и ситуаций. Кроме того, не ясен правой статус персональных данных, которые не относятся ни к категории ограниченного доступа, ни к категории тех, на которые субъект персональных данных не давал согласия на доступ.

Примечателен опыт Российской Федерации, где из содержания Федерального закона «О персональных данных», а также Указа Президента Российской Федерации 3 188 от 06.03.1997 года «Об утверждении перечня

сведений конфиденциального характера» следует, что все персональные данные имеют конфиденциальный характер, но субъект персональных данных вправе определить разрешенные для распространения персональные данные с предоставлением доступа к ним неограниченного круга лиц [45, 46]. Полагаем, что такой механизм имеет более четкий и понятный характер.

Еще одной значительной проблемой казахстанского законодательства является неурегулированность вопроса обработки специальных видов персональных данных.

Следует отметить, что Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных [47] и законодательство большинства европейских стран относят данные о судимости лица, расовом или национальном происхождении, политических взглядах, религиозных и других убеждениях, данные о состоянии здоровья и интимной жизни к числу специальных либо чувствительных персональных данных.

Законодательством Казахстана не предусмотрено понятие «специальные (либо чувствительные) персональные данные», сведения о расовом или национальном происхождении, политических взглядах, религиозных и других убеждениях, данные о состоянии здоровья, интимной жизни и судимости правовыми актами не отнесены к персональным данным ограниченного доступа, в связи с чем в обществе на постоянной основе возникают попытки сбора и обработки такой информации, чем ущемляются права граждан.

И.С. Алихаджиева считает, что «после погашения или снятия судимости любая публикуемая информация о ней должна быть отнесена к категории специальных персональных данных и не подлежать разглашению, распространению или обработке, за исключением установленных законом случаев. Факт судимости, когда она погашена или снята, утрачивает свое уголовно-правовое значение и безусловную публичную значимость, что порождает у осужденного лица право на забвение и сохранение сведений об имевшейся судимости как личной тайны» [48]. Целесообразно согласиться с указанным мнением, одновременно, применив недопустимость обработки такой информации и к другим видам чувствительных сведений.

Введение понятия специальные персональные данные в законодательство Казахстана позволит более эффективно защищать права граждан, поскольку прекратит бесконтрольный сбор чувствительных сведений. К примеру, за последние 2 года несколько информационных порталов неоднократно обращались в Генеральную прокуратуру для получения сведений о наличии судимости руководителя Федерации футбола Казахстана «Б.». В другом случае журналисты неоднократно задавали актрисе «А.» вопросы об ее этническом происхождении и ставили под сомнение национальность, несмотря на ее нежелание раскрывать данные сведения. Среди студентов одного из университетов г. Алматы посредством мессенджеров распространена информация относительно обучающихся, где помимо прочего были указаны сведения о наличии/отсутствии у девушек интимной жизни. В 2024 году в г. Астана задержаны и доставлены в отделение полиции более 70 человек, по

словам которых сотрудники полиции осуществляли сбор их данных, как представителей нетрадиционной сексуальной ориентации. Однако, в данных случаях несовершенство законодательства не дает четкого понимания о необходимости вмешательства органов прокуратуры.

Еще одной значительной проблемой казахстанского законодательства является недостаточная регламентация процедуры биометрической аутентификации. Этот вопрос активно изучается зарубежными учеными.

Г. Сингх указывает, что биометрические персональные данные становятся популярными средством аутентификации, подтверждения личности, поскольку имеют множество преимуществ по сравнению с другими более традиционными средствами аутентификации. В то же время это несет серьезные риски для безопасности персональных данных [49].

А. Де Кейзер считает, что ввиду широкого внедрения биометрических систем в различных отраслях, в ближайшее время данный вопрос будет активно изучаться через призму бизнеса и маркетинга, что в свою очередь влечет серьезные риски, поскольку бизнесом получается доступ к данным, которые ране было сложно или даже невозможно получить [50].

А. Иоанну сообщает, что крупные авиационные и морские перевозчики пассажиров утверждают, что принятие биометрических решений, к примеру, путем использования камер, оснащённых алгоритмами компьютерного зрения, которые захватывают лица пассажиров, сравнивают и идентифицируют их с ранее поданными фотографиями, позволит значительно сократить сроки посадки большого количества пассажиров на самолеты или круизные лайнеры [51].

М. Смит утверждает, что возможности биометрического распознавания лиц в сочетании с искусственным интеллектом быстро расширяются и имеют большой потенциал для раскрытия преступлений. Однако эта технология также несет значительный риск нарушения конфиденциальности, что требует законодательного урегулирования. Распознавание лица предполагает автоматизированное извлечение, оцифровку и сравнение пространственного и геометрического распределения черт лица для идентификации личности с фотографией из базы данных. Изображения можно собрать из репозитариев паспортов или водительских удостоверений или огромного количества изображений, которые были загружены в социальные сети и Интернет. Центральное место в этических, правовых и политических вопросах занимает противоречие, которое существует между законным сбором биометрической информации для правоохранительных органов и национальной безопасностью, предоставлением государственных услуг с одной стороны и правом на неприкосновенность частной жизни с другой стороны. Поскольку использование распознавания лиц и других систем биометрической идентификации могут быть оправданы для конкретных целях безопасности, то важным является наличие механизма защиты от злоупотреблений. Граждане должны быть хорошо информированы о биометрических процедурах для лица и становиться их участниками лишь с собственного согласия [52].

В иностранной научной литературе имеется значительное количество работ, посвященных биометрическим персональным данным, в которых отмечается важность вопроса ввиду того, что процедура биометрической идентификации активно входит в повседневную жизнь населения, что требует надлежащего законодательного урегулирования.

Согласно пункту 1 статьи 1 Закона «О персональных данных и их защите» в Казахстане под биометрическими данными понимаются персональные данные, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на основе которых можно установить его личность. При этом законодательство не раскрывает, что понимается под физиологическими и биологическими особенностями субъекта персональных данных.

В настоящее время Законом «О дактилоскопической и геномной регистрации» закреплены два вида биометрических данных: геномная информация и дактилоскопическая информация. Геномная информация содержит сведения о ДНК, а дактилоскопическая информация об особенностях строения папиллярных узоров пальцев и (или) ладоней рук.

При этом в законодательстве Казахстана уже появляются нормы о биометрической идентификации. В пункте 39 статьи 1 и пункте 6 статьи 56 Законе «О платежах и платежных системах» указано, что биометрическая информация является одним из видов идентификационного средства, а биометрические данные могут быть использованы в качестве защитных элементов против несанкционированных платежей [53]. Пункт 7 статьи 35 и пункт 31 статьи 1 Социального кодекса наделяют Единый накопительный фонд правом оказания пенсионных услуг посредством процедуры биометрической идентификации, под которой понимается установление личности физического лица на основании его физиологических и биологических неизменных признаков.

20.08.2024 года введен в действие пункт 5-5 статьи 34 Закона «О банках и банковской деятельности в Республике Казахстан», согласно которому банки для заключения договора банковского займа с физическим лицом посредством Интернета обязаны провести его биометрическую идентификацию [54]. Аналогичные требования введены в Закон «О микрофинансовой деятельности» [55].

01.01.2025 года введены в действие «Правила проведения биометрической идентификации банками, организациями, осуществляющими отдельные виды банковских услуг, и микрофинансовыми организациями», утвержденные Агентством Республики Казахстан по регулированию и развитию финансового рынка 16.08.2024 года [56]. Из содержания данных Правил следует, что биометрическая идентификация будет проводиться по изображению лица путем сличения текущего и эталонного изображения идентифицируемого лица. Таким образом, нововведения в законодательстве о банковской деятельности позволяют под биометрическими данными понимать и изображение лица.

Определенную неразбериху вносит наличие в статье 2 «Соглашения о сотрудничестве в создании государственных информационных систем паспортно-визовых документов нового поколения и дальнейшем их развитии и использовании в государствах-участниках СНГ», утвержденного постановлением Правительства Республики Казахстан от 30.03.2009 года №430, определения понятия биометрические данные, под которыми понимаются сведения, характеризующие физиологические особенности человека и на основе которых можно установить его личность (цифровая фотография, отпечатки пальцев, изображение радужной оболочки глаз и другие биометрические персональные данные), которые могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, в соответствии с законодательством государств-участников настоящего Соглашения [57].

В научной литературе к биометрическим персональным данным помимо фотографии, ДНК и папиллярных узоров также относят радужную оболочку глаз, рост, вес, видеозапись лица, рисунок вен ладони. Однако в законодательстве Казахстана такие виды биометрических персональных данных не выделяются, хотя в жизни граждан страны используются сервисы с применением технологий сбора и использования такой информации. Например, казахстанский стартап-проект «Alaqan» внедряет технологию использования рисунка вен ладони человека для входа в помещения и для оплаты услуг. По сведениям разработчиков стартапа в системе зарегистрировались уже почти сто тысяч человек.

По сведениям Г.С. Кодашевой на начало 2019 года на мировом рынке биометрических систем наиболее активно применялись технологии, основанные на распознавании отпечатков пальцев (38%), рисунков вен (18%), голоса (11%) и геометрия ладони (10%). Менее часто применялись технологии, основанные на распознавании изображения лица (6%), радужной оболочка глаза (7%), поведенческой биометрии (4%), ушных раковин (3%) и сигналов мозга (3%) [58].

Следует отметить, что зарубежное законодательство, как правило, относит к биометрическим персональным данным не только физические и физиологические, но и поведенческие особенности физического лица, которые позволяют произвести или подтверждают однозначную идентификацию этого физического лица.

Ф.В. Грушин отмечает, что в российском законодательстве поведенческие особенности не выделены как отдельная категория данных, но «исследования и внедрение в практику технологий идентификации исключительно по поведенческим характеристикам (таким как голос, подпись, шаблоны ввода, походка, положение тела в пространстве и др.), дают основания полагать, что выделение данной категории в законодательном отражении возможно в ближайшем будущем [59].

Д.В. Бахтеев и И.В. Леднев указывают, что для поиска неустановленных преступников целесообразно применение метода криминологического

профилирования, который некоторые ученые называют криминологическим поведенческим анализом. Целью криминологического профилирования является определение отличительных характеристик преступника, в том числе и поведенческих [60]. В этом контексте урегулирование вопроса биометрических поведенческих данных обретает дополнительную актуальность.

Полагаем, что в Казахстане в ближайшее время также возникнет необходимость законодательного урегулирования порядка сбора такой информации, поскольку уже сейчас осуществляется сбор сведений о поведенческих особенностях лиц.

Так, в 2023 году принят Закон «Об онлайн-платформах и онлайн-рекламе», которым введены такие понятия, как профайлинг и таргетированная онлайн-реклама. Под профайлингом понимаются действия онлайн-платформ по определению предпочтений и (или) интересов пользователей, а под таргетированной онлайн-рекламой онлайн-реклама, направляемая целевым группам на основании профайлинга. Иными словами онлайн-платформам дано право сбора информации о поведенческих особенностях человека [61].

Имеющиеся проблемы в сфере применения биометрической аутентификации планировалось решить при реализации Программы создания Национальной платформы цифровой биометрической идентификации на 2022-2024 годы, но дальше обсуждения проекта она не зашла и не была утверждена в итоге [62].

В законодательстве Казахстан о персональных данных и их защите имеются и другие понятия, которым не даны определения, что влечет сложности правоприменительной практики. К примеру, в Законе «О персональных данных и их защите» девять раз упоминается понятие «общедоступные источники». Посредством них допускается сбор и распространение персональных данных. Между тем, определения данному понятию законодательство не дает. Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан считает допустимым относить к общедоступным источникам онлайн-платформу или иной источник, содержащий общедоступную информацию, то есть информацию, которая не может быть ограничена в силу требований законодательства Республики Казахстан либо которую раскрывает (распространяет) само лицо (физическое или юридическое), а также социальные сети. При этом повторный сбор, обработка и распространение третьими лицами персональных данных, опубликованных на закрытом аккаунте социально сети, допускается лишь с согласия субъекта персональных данных [63]. Однако какого-либо нормативного закрепления данная позиция не имеет. Схожая ситуация и по понятию «охраняемая законом информация», которое используется в Уголовном кодексе и многих других законодательных актах, но не имеет закрепленного в нормативном порядке определения.

Таким образом, несовершенство и отсутствие в действующем законодательстве в сфере персональных данных и их защиты отдельных понятий, в том числе общепризнанных и применяемых в зарубежных странах является сдерживающим фактором эффективной защиты персональных данных, в том числе прокурорского надзора в этой сфере.

Видится целесообразным пересмотр позиции относительно правового закрепления понятия «персональные данные» в пользу метода более широкого трактования с исключением сужающих и ограничивающих положений в виде необходимости фиксирования персональных данных на электронном, бумажном и (или) ином материальном носителе.

Предлагается следующая дефиниция понятия «персональные данные»:

Персональные данные – сведения, совокупность информации, прямо или косвенно относящиеся к определенному или определяемому физическому лицу, являющемуся субъектом (носителем) персональных данных.

Кроме того, необходим концептуальный пересмотр позиции касательно конфиденциальности персональных данных. Полагаем целесообразным законодательное признание конфиденциальности всех персональных данных с наделением субъектов персональных данных правом их раскрытия и распространения, а также предоставления возможности обработки и доступа к своим персональным данным неограниченного круга лиц.

Также требуется введение в законодательство понятия «специальные персональные данные» для исключения бесконтрольного сбора и обработки чувствительных для граждан сведений.

Предлагается под «специальными персональными данными» понимать особо личные сведения, сбор, обработка и распространение которых могут повлечь чувствительные последствия для субъекта данных, в том числе данные о судимости, расовом или национальном происхождении, родовой принадлежности, политических взглядах, религиозных и других убеждениях, данные о состоянии здоровья и интимной жизни, смене пола и пр. При этом важно закрепить в законодательстве не только понятие, но и нормы относительно порядка обработки и конфиденциальности специальных персональных данных, необходимости обязательного согласия субъекта персональных данных на сбор и обработку информации такого рода.

Необходима доработка понятия «биометрические данные», определение и закрепление их видов, в том числе исходя из внедряемых в различных сферах общественных отношений и используемых гражданами средств биометрической идентификации, определение уровня конфиденциальности новых видов биометрических данных, порядка обработки и использования такой информации, а также расширение применения понятия «биометрические данные», охвата им сведений не только о физиологических и биологических, но и поведенческих особенностях человека. Предлагается следующее определение понятия «биометрические данные» – персональные данные, которые позволяют установить личность субъекта персональных данных на основе характеризующих его физиологических, биологических признаков и

поведенческих особенностей (цифровая фотография, отпечатки пальцев и (или) кистей рук, изображение радужной оболочки глаз, рисунок вен, геометрия ушных раковин, сигналы мозга, почерк, походка, динамика нажатия клавиш и другие биометрические персональные данные).

1.2 Принципы и алгоритмы прокурорского надзора в сфере защиты персональных данных

Прокуратура, как орган государственной власти, имеет большую историю, которая в различных странах в силу общественных, государственных и демократических преобразований развивалась, как схожим путем, так и кардинально по-разному.

С.К. Журсимбаев выделяет 4 группы стран с учетом места прокуратуры в системе государственного устройства. 1 группа – государства, где прокуратура входит в состав министерства юстиции. В США, Франции, Бельгии и других государствах прокуроры действуют при судах, но независимы от них. Прокуратуры в этих государствах нередко структурно различаются, министрами юстиции допускается совмещение должности генерального прокурора. 2 группа – государства, где прокуратура полностью включена в состав судебной системы. В Испании, Болгария, Латвии и других государствах прокуратура функционирует только при судах, но обладает автономией. 3 группа – государства, где прокуратура выделена в отдельный государственный орган с подотчетностью парламенту или президенту страны. К этой группе относятся социалистические, постсоциалистические государства и страны Латинской Америки. При этом ряд постсоциалистических стран сложно отнести к данной группе, поскольку в результате проведенных реформ прокуратуры этих государств функционируют в виде части судебной системы, а не как самостоятельный орган. 4 группа – государства, где прокуратура или органы с аналогичными функциями отсутствуют. К примеру, в Великобритании нет прокуратуры, но отдельные должностные лица реализуют свойственные ей функции. Учитывая различный подход к организации работы прокуратуры в разных государствах, С.К. Журсимбаев считает, что возможны определенные коррективы, оптимизация отраслей прокурорского надзора, но реформирование должно идти эволюционным путем, а система прокуратуры должна быть понимаема и отвечать потребностям того общества, в котором она функционирует [64].

Различие законодательства и функциональных обязанностей влияет на роль и степень участия прокуратуры в тех или иных государственных процессах. Между тем, работы исследователей показывают, что, несмотря на существенные расхождения в подходах организации работы органов прокуратуры, зачастую они вовлечены в важные процессы, связанные с защитой прав граждан. К примеру, изучение опыта зарубежных стран показало, что прокуратура играет важную роль на всех этапах урегулирования чрезвычайных ситуаций [65]. В вопросах защиты персональных данных роль прокуратуры является не менее важной.

Становление и развитие прокуратуры Республики Казахстан на современном этапе можно разделить на несколько периодов.

1 период приходится на конец 1991 года – август 1995 года. В этот период образована единая система прокуратуры Казахстана, принят Закон «О прокуратуре Республики Казахстан» 1992 года, роль и компетенция прокуратуры отражены в Конституции Республики Казахстан 1993 года. При этом прокуратура была подотчета Верховному Совету.

2 период продлился с августа 1995 года до августа 2002 года. В этот период были приняты новая Конституция Республики Казахстан и Закон «О Прокуратуре» 1995 года. В них указан единый, централизованный и независимый характер системы прокуратуры. Прокуратура стала подотчета лишь Президенту Республики Казахстан, усилились ее правозащитные функции, начата процедура реабилитации жертв политических репрессий. При этом уголовные статьи, ранее подследственные прокуратуре, вместе с функциями по проведению предварительного следствия были преданы другим правоохранительным органам, но за прокуратурой сохранилось право возглавлять следственные группы.

3 период начался с августа 2002 года. В этот период осуществлялось совершенствование правоохранительной деятельности для повышения уровня законности и защиты прав граждан. Укреплен высший надзор прокуратуры, в том числе введены нормы об ответственности за неисполнение требований и актов прокурора [66]. Полагаем, что данный этап закончился в 2017 году, когда в Конституцию Республики Казахстан внесены изменения, предполагающие наличие пределов прокурорского надзора, исключающие положение об осуществлении надзора за точным и единообразным применением норм права, а также требования об осуществлении прокуратурой уголовного преследования только в случаях, порядке и в пределах, установленных законом. В июне 2017 года принят новый Закон Республики Казахстан «О прокуратуре», которым определены пределы прокурорского надзора, цели и задачи, а также компетенция и порядок функционирования прокуратуры с учетом данных нововведений.

Б.Х. Толеубекова и Т.Б. Хведелизде указывают, что «в послереформенном отраслевом законодательстве о прокуратуре «высший надзор за точным и единообразным применением норм права» не упоминается. Он исключен из ст. 83 Конституции и, соответственно, из нового Закона РК «О прокуратуре» (2017). Таким образом, полагаем, что отказ в результате конституционной реформы в Казахстане в 2017 году от института точности и единоборства в применении закона при осуществлении прокурорского надзора за соблюдением законности не было вызван острой потребностью, вопрос о правомерности данного подхода остается открытым для дискуссий» [67].

Следующий этап начался в 2022 году и продолжается в настоящее время. По инициативе Президента Республики Казахстан К.К. Токаева конституционные нормы о прокуратуре включены в Раздел VII Конституции Республики Казахстан «Суды и правосудие. Прокуратура. Уполномоченный по

правам человека», что связано с приданием конституционного статуса Закону «О прокуратуре». Конституционный статус закона наделил прокуратуру более действенными механизмами реализации надзорных полномочий, усилил правозащитные функции, а также позволил повысить эффективность прокуратуры по защите интересов государства, граждан и бизнеса.

Прокуратура не относится ни к одной из существующих ветвей власти, в связи с чем некоторыми исследователями, как, например, А.Б. Ахметовой предложено выделение отдельной ветви власти – прокурорский власти, поскольку органы прокуратуры наделены государственно-властными полномочиями, независимы от других ветвей власти, а также между ними и прокуратурой существует система сдержек и противовесов [68].

Академией правоохранительных органов отмечено, что в конституциях стран СНГ прокуратуре отведено особое место, но подход зачастую существенно различается. В Азербайджане и Российской Федерации нормы о прокуратуре включены в главы, посвященные судам и правосудию, в Армении, Белоруссии, Молдове, Узбекистане, Таджикистане и Туркменистане в самостоятельные главы «Прокуратура», в Кыргызской Республике в главу «Органы государственной власти Кыргызской Республики со специальным статусом», а в Украине данный раздел исключен из основного закона государства [69]. В Испании, Финляндии, Италии, КНР и Бразилии правовой статус прокуратуры закреплен в конституциях. При этом в ряде стран ОЭСР, таких как Дания, Германия, Великобритания, США и Канада, прокуратура отнесена к исполнительной власти и ее положение закреплено в законах о прокуратуре, деятельности судов, а также кодексах [70].

В Республике Казахстан согласно пункту 1 статьи 83 Конституции на прокуратуру возложено осуществление от имени государства в установленных законом пределах и формах высшего надзора за соблюдением законности на территории Республики Казахстан, уголовного преследования, а также представление интересов государства в суде. При этом компетенция, организация и порядок деятельности прокуратуры Республики определяются законодательством.

21.12.1995 года принят Закон Республики Казахстан «О Прокуратуре» [71], в дальнейшем 30.06.2017 года принят новый Закон Республики Казахстан «О прокуратуре» [72]. 16.03.2022 года Глава государства К.К. Токаев в Послании народу Казахстана «Новый Казахстан: путь обновления и модернизации» указал о необходимости принятия отдельных конституционных законов о прокуратуре и об Уполномоченном по правам человека. 05.11.2022 года принят действующий в настоящее время Конституционный закон Республики Казахстан «О прокуратуре» [73].

В каждом из указанных нормативных правовых актов статьей 3 были определены принципы организации и деятельности органов прокуратуры, которые фактически являются общими для всех видов прокурорского надзора.

Ю.Е. Винокуров отмечает, что «принципы организации и деятельности прокуратуры – это основополагающие, руководящие положения,

определяющие наиболее существенные черты и признаки многогранной деятельности органов прокуратуры и основные предъявляемые к ней требования. Так как принципы определяют наиболее общие признаки и требования, то они обязательны для любого прокурорского работника независимо от занимаемой должности или конкретного направления своей деятельности» (таблица 1) [74].

Таблица 1 – Принципы организации и деятельности органов прокуратуры

Статьи	Принципы
1	2
Статья 3 Закона «О Прокуратуре» 21.12.1995 года	1. Прокуратура Республики Казахстан составляет единую централизованную систему органов, ведомств, учреждений и организации образования с подчинением нижестоящих прокуроров вышестоящим и Генеральному Прокурору Республики. 2. Прокуратура Республики Казахстан осуществляет свою деятельность независимо от других государственных органов и должностных лиц, политических партий и других общественных объединений и подотчетна лишь Президенту Республики Казахстан. 3. Запрещается вмешательство в деятельность органов прокуратуры при осуществлении ими своих полномочий, установленных законодательством. 4. Акты прокурорского надзора, вынесенные на основании и в порядке, установленном законом, обязательны для всех органов, организаций, должностных лиц и граждан. 5. Органы прокуратуры действуют гласно в той мере, в какой это не противоречит требованиям законодательства Республики об охране прав и свобод граждан, защите государственных секретов.
Статья 3 Закона «О прокуратуре» 30.06.2017 года	1. Прокуратура составляет единую централизованную систему с подчинением нижестоящих прокуроров вышестоящим и Генеральному Прокурору. 2. Прокуратура осуществляет свои полномочия на принципах законности, независимости от других государственных органов, должностных лиц и подотчетности лишь Президенту Республики Казахстан. 3. Запрещается вмешательство в деятельность органов прокуратуры при осуществлении ими своих функций и полномочий. 4. Прокуратура не вправе вмешиваться в деятельность субъектов предпринимательства, организаций и государственных органов, назначать проверки их деятельности, запрашивать информацию либо документы по основаниям, не предусмотренным законом. 5. Органы прокуратуры действуют гласно в той мере, в какой это не противоречит требованиям законодательства об охране прав и свобод человека и гражданина, о защите государственных секретов и иной охраняемой законом тайны.

Продолжение таблицы 1

1	2
Статья 3 Закона Конституционного закона «О прокуратуре» 05.11.2022 года	1. Прокуратура осуществляет свои полномочия на принципах законности, независимости от других государственных органов и должностных лиц, подотчетности лишь Президенту Республики Казахстан, гласности. 2. Запрещается какое-либо вмешательство в деятельность органов прокуратуры при осуществлении ими своих функций и полномочий. 3. Прокуратура не вправе вмешиваться в деятельность субъектов предпринимательства, организаций и государственных органов, назначать проверки их деятельности, запрашивать информацию либо документы по основаниям, не предусмотренным законом. 4. Органы прокуратуры действуют гласно в той мере, в какой это не противоречит требованиям законов Республики Казахстан в части охраны прав и свобод человека и гражданина, о защите государственных секретов и иной охраняемой законом тайны.

Во всех трех вышеуказанных законах о прокуратуре Казахстана практически без изменений сохранились принципы относительно независимости, гласности прокуратуры, запрете вмешательства в ее деятельность, а также подотчетности Президенту. Закон 1995 года к принципам прокурорского надзора относил обязательность актов прокурорского надзора для всех органов, организаций, должностных лиц и граждан. Однако, Законом 2017 года указанный принцип был исключен. На сегодня в подпункте 3 пункта 1 статьи 32 действующего Конституционного закона указывается, что акты прокурорского надзора обязательны для рассмотрения, исполнения органами, организациями и должностными лицами, которым они адресованы. Также в Конституционном законе не сохранился принцип построения прокуратуры в виде единой централизованной системы, который был закреплен в двух предыдущих законах. При этом в пункте 2 Конституции указано, что прокуратура Республики составляет единую централизованную систему с подчинением нижестоящих прокуроров вышестоящим и Генеральному Прокурору Республики, а пункты 1 и 2 статьи 5 Конституционного закона «О прокуратуре» гласят, что единую централизованную систему органов прокуратуры составляют Генеральная прокуратура, подчиненные ей ведомства и организации, а деятельность органов прокуратуры осуществляется на основе подчинения нижестоящих прокуроров вышестоящим прокурорам и Генеральному Прокурору. Помимо этого можно отметить, что Законом 2017 года включен принцип касательно запрета вмешательства прокуратуры в деятельность субъектов предпринимательства, организаций и государственных органов по основаниям, не предусмотренным законом. Данный принцип сохранился и в действующем Конституционном законе. Следует отметить, что схожего принципа деятельности прокуратуры нет в законодательстве других государств и его включение видится более целесообразным не в принципы, а в полномочия и обязанности прокурора. Также в Законе 2017 года с сохранением

в Конституционном законе появился принцип законности при осуществлении прокуратурой своих полномочий, который является одним из важнейших в деятельности прокуратуры.

Т.Б. Хведелидзе и Б.Х. Толеубекова указывают, что «принцип законности должен рассматриваться дифференцированно: как организационно-управленческий принцип и как принцип, являющийся ключевым элементом в определении содержания прокурорского надзора» [75].

А.Е. Алибеков указывает, что «Закон Украины «О прокуратуре» предлагает дополнительные принципы организации и деятельности органов прокуратуры (ст. 4). Такие как: 1) верховенства права и признание человека, его жизнь и здоровье, чести и достоинства, неприкосновенности и безопасности наивысшей социальной ценностью; 2) законности, справедливости, беспристрастности и объективности; 3) территориальности; 4) презумпции невиновности; 5) недопустимости незаконного вмешательства прокуратуры в деятельность органов законодательной, исполнительной и судебной власти; 6) уважения к независимости судей, предусматривающий запрет публичного высказывания сомнений в правосудности судебных решений за пределами процедуры их обжалования в порядке, предусмотренном процессуальным законом;7) прозрачности деятельности прокуратуры, обеспечивается открытым и конкурсным занятием должности прокурора, свободным доступом к информации справочного характера, предоставлением на запросы информации, если законом не установлены ограничения по ее предоставлению; 8) неукоснительного соблюдения требований профессиональной этики и поведения». При этом целесообразность внедрения таких принципов в Казахстане автором подвергается сомнению [76].

Пунктом 1 статьи 6 Конституционного закона «О прокуратуре» определены основные отрасли прокурорского надзора, к которым относится надзор за законностью:

- деятельности государственных, местных представительных и исполнительных органов, органов местного самоуправления, учреждений, их должностных лиц, иных организаций независимо от форм собственности, а также принимаемых ими актов и решений;
- производства по делам об административных правонарушениях;
- досудебного расследования, уголовного преследования, оперативно-розыскной и контрразведывательной деятельности;
- исполнительного производства;
- судебных актов, вступивших в законную силу;
- исполнения уголовных наказаний и применения иных мер государственного принуждения;
- государственной правовой статистики и специальных учетов;
- соблюдения международных обязательств Республики Казахстан.

О.В. Воронин отмечает, что по своей форме и содержанию прокурорская деятельность существенно различается, в связи с чем оправдано наличие в структуре прокурорского надзора отдельных направлений в виде отраслей

надзора. Ни одна из отраслей прокурорского надзора не может считаться определяющей, правовое регулирование каждой отрасли должно быть самостоятельным. При этом конкретный вид прокурорской деятельности может перетекать из одной отрасли в другую [77].

Т.А. Сулейманов и С.Н. Мальцева указывают, что «несмотря на различие функций в деятельности прокуратуры, вся деятельность строится на общих принципах» [78]. В свою очередь, некоторые ученые выделяют принципы, которые относятся и к отдельной отрасли прокурорского надзора. К примеру, А.В. Бородина указывает, что «анализируя доктрину прокурорского надзора за исполнением законов, можно выделить ее принципы. Во-первых, это принцип правомерности вмешательства. Так прокурорских надзор за исполнением законов должен осуществляться на основании нормативно-правового регулирования. Во-вторых, это принцип своевременности вмешательства. Законодатель предусматривает определенные сроки осуществления прокурорского надзора за исполнением закона. В-третьих, это принцип полноты используемых полномочий. Прокурор обязан использовать все доступные полномочия для реализации задач прокурорского надзора за исполнением закона. В-четвертых, это принцип настойчивости в устранении нарушений. Прокурор обязан требовать устранения нарушения. Подобное полномочие имеет ультимативный характер и является не правом, а обязанностью» [79].

В свою очередь М.М. Челпанова приводит пример определения принципов осуществления прокурорского надзора за исполнением законодательства об охране окружающей среды в Российской Федерации, что говорит о возможности определения принципов и для отдельного направления прокурорского надзора [80]. Соответственно, потенциально возможно определить и принципы прокурорского надзора в сфере защиты персональных данных.

Следует отметить, что статьей 4 Конституционного закона «О прокуратуре» определены цели и задачи прокуратуры, к которым отнесены защита и восстановление нарушенных прав и свобод человека и гражданина, охраняемых законом интересов юридических лиц, общества и государства, выявление и устранение нарушений законности, их причин, условий и последствий, координация деятельности правоохранительных и иных государственных органов по обеспечению законности, правопорядка и борьбы с преступностью, а также иные задачи, определяемые законодательством.

В Республике Казахстан институты защиты персональных данных и прокурорского надзора в сфере защиты персональных данных можно назвать достаточно молодыми. Только в 2013 году принят Закон Республики Казахстан «О персональных данных и их защите», в котором первоначально были определены компетенция Правительства, государственных органов и органов прокуратуры. На прокуратуру было возложено осуществление от имени государства высшего надзора за точным и единообразным за применением законодательства в этой сфере. В 2017 году вышеуказанная трактовка

несколько изменена, а именно высший надзор прокуратуры закреплен за соблюдением законности в сфере персональных данных и их защиты (таблица 2).

Таблица 2 – Нормы относительно прокурорского надзора в Законе Республики Казахстан «О персональных данных и их защите»

В первоначальной редакции	С изменениями от 11.07.2017 года
Статья 28. Надзор за применением настоящего Закона	Статья 28. Надзор за применением настоящего Закона
1. Органы прокуратуры от имени государства осуществляют высший надзор за точным и единообразным применением настоящего Закона и иных нормативных правовых актов Республики Казахстан в сфере персональных данных и их защиты	1. Органы прокуратуры осуществляют высший надзор за соблюдением законности в сфере персональных данных и их защиты.

Таким образом, можно сказать, что в Республике Казахстан в качестве самостоятельного прокурорский надзор в сфере защиты персональных данных возник в 2013 году. При этом в первоначальных редакциях Закон Республики Казахстан «О персональных данных и их защите», а также в Кодексе Республики Казахстан об административных правонарушениях контрольными и надзорными функциями в сфере защиты персональных данных, а также правом возбуждения административных дел за нарушения в данной сфере была наделена только прокуратура, которая фактически на тот момент являлась уполномоченным органом в данном направлении. С появлением уполномоченного органа ситуация поменялась.

25.06.2020 года Законом Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий» законодательно введено понятие уполномоченный орган в сфере защиты персональных данных и определены его полномочия [81].

18.01.2021 года в Положение о Министерстве цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан внесены изменения, согласно которыми данный государственный орган наряду с другими сферами определен «осуществляющим руководство в сфере персональных данных и их защиты» [82].

Изначально в Законе Республики Казахстан «О персональных данных и их защите» был определен перечень из 8 полномочий уполномоченного органа, но в дальнейшем 02.01. и 30.12.2021 года законодательно этот перечень дополнен еще 6 видами полномочий, в число которых входит и государственный контроль за соблюдением законодательства о персональных данных и их защите.

При этом в свободном доступе информации о работе уполномоченного органа и достигнутых результатах практически не имеется. В итоге у населения

практически нет представления о методах защиты своих персональных данных. Проведенное анкетирование 127 лиц, из которых 104 обладали средним и высоким уровнем познаний в сфере юриспруденции, показало, что из них только 17,3% известен механизм защиты и порядок действия в случае нарушения законодательства о персональных данных и их защите, только 26,8% известен уполномоченный орган. При этом в случае нарушения своих прав в рассматриваемой сфере в Министерство цифрового развития, инноваций и аэрокосмической промышленности, являющееся уполномоченным органом, обратились бы только 6,3, 31,5% опрошенных лиц обратились бы в прокуратуру, а и 44,% в полицию (Приложение И).

В соответствии с пунктом 4 статьи 5 Конституционного закона «О прокуратуре» при осуществлении надзора органы прокуратуры не подменяют функции иных государственных органов.

После появления уполномоченного органа в сфере защиты персональных данных важным является определение роли и места прокуратуры в сфере защиты персональных данных. При этом необходимо отметить, что появление уполномоченного органа и недостаточное законодательное урегулирование полномочий прокуратуры в отраслевом законе не говорит о том, что надзор в данном направлении должен сужаться или не осуществляться вовсе.

В качестве аналогии можно привести позицию К. Баканова и С. Шпорт, которые отмечают, что несмотря на отсутствие в законодательстве и ведомственных актах относительно безопасности дорожного движения прямых норм, касающихся полномочий прокуроров, в рамках наделенных на функций и при наличии соответствующих оснований органы прокуратуры вправе проводить в данном направлении проверки, запрашивать любую информацию вне зависимости от подведомственности или формы собственности с соблюдением требований по защите персональных данных [83]. Поэтому и в сфере защиты персональных данных следует учитывать, что законодательством прокуратура наделена функциями высшего надзора, позволяющими ей осуществлять свою деятельность без детального урегулирования в отраслевом законодательстве.

На сегодня, какой-либо официальной информации о работе органов прокуратуры Казахстана в сфере защиты персональных данных не имеется, правовые акты, руководящие указания Генерального Прокурора, ведомственные акты, отражающие характер и специфику данного направления надзора, не разрабатывались. Таким образом, отдельные принципы и алгоритмы прокурорского надзора в сфере защиты персональных данных нормативно не закреплены. Кроме того, отсутствует информация о проводимой методологической работе в данном направлении, в том числе о разработанных методических рекомендациях, информационных письмах, проведении анализов с формированием наиболее часто встречающихся нарушений.

Некоторые исследователи считают, что наибольшую эффективность имел бы надзор прокуратуры за соответствием нормативных правовых актов конституционным нормам, а также законодательству о защите персональных

данных [84]. Однако, более целесообразным видится использование всего спектра прокурорского надзора, в том числе возможное создание отдельных подразделений либо закрепление за конкретными структурными подразделениями вопросов, касающихся защиты персональных данных.

В подтверждение этого можно отметить открытие в феврале 2022 года в Генеральной прокуратуре Российской Федерации Отдела по надзору за исполнением законов в сфере информационных технологий и защиты информации [85]. В данном государстве наряду с противодействием киберпреступности, правонарушениям экономической и антисоциальной направленности в сети «Интернет» и другим важным задачам одним из основных направлений прокурорского надзора за исполнением законодательства о противодействии правонарушений в сети «Интернет» является защита персональных данных.

С.А. Бессчасный указывает, что «Приказом Генерального прокурора Российской Федерации от 14.09.2017 года №627 утверждена Концепция цифровой трансформации органов и организаций прокуратуры до 2025 года, согласно которой основными целями цифровой трансформации являются: повышение эффективности деятельности органов прокуратуры Российской Федерации; обеспечение устойчивого и бесперебойного функционирования цифровой инфраструктуры, повышение ее информационной безопасности; развитие свободного, устойчивого и бесперебойного взаимодействия органов прокуратуры Российской Федерации с гражданами и обществом». Данной Концепцией ставятся цели по повышению эффективности деятельности органов прокуратуры и цифровизации объектов надзора, для чего предполагается решение задач по внедрению высокотехнологичного надзора, цифровой инфраструктуры и среды доверия, для чего планируется совершенствование качества деятельности правоохранительных органов по правовому, научно-методическому и организационно-технологическому обеспечению автоматизированной оценки, внедрение современных и информационных технологий во всех видах надзора и другие важные мероприятия [86].

Начиная с 2023 года, в структуре Генеральной прокуратуры Республики Казахстан появилось два подразделения, на которые возложены вопросы информационной безопасности. Однако, они не наделены надзорными функциями, осуществляют лишь информационную защиту органов прокуратуры, а также внедрение информационных технологий в работу органов прокуратуры Республики Казахстан.

При этом, несмотря на отсутствие большого количества информации, органами прокуратуры Казахстана работа по защите персональных данных все же проводится. К примеру, «Инструкция по организации надзора за соблюдением законности досудебного расследования по делам о преступлениях против половой неприкосновенности несовершеннолетних» (утверждена приказом Генерального Прокурора Республики Казахстан №167 от 05.09.2023 года) предусматривает положения об обязательной защите персональных

данных несовершеннолетних жертв преступлений против половой неприкосновенности. Также защищаются данные членов их семей и близких родственников. При нарушении этих требований прокуроры обязаны инициировать досудебное расследование.

В перспективе возможно потребуется внедрение механизмов по защите персональных данных и других участников досудебного расследования, поскольку в настоящее время зачастую поднимается вопрос об избыточном сборе данных, как, например, номер телефона или место жительства.

Нередко прокуроры при проверках организаций для детей-сирот, медико-социальных и других учреждений, в которых содержатся лица, неспособные защитить себя самостоятельно, выявляют нарушения законы, совершенные в условиях наличия доступа к персональным данным.

К примеру, в 2020 году в Жамбылской области прокурорами выявлено, что воспитатель одного из учреждений для детей-сирот, имея доступ к персональным данным воспитанников, похитила принадлежащие им средства. По мерам прокурорского реагирования возбуждено уголовное дело, воспитатель осуждена к лишению свободы.

Таким образом, органами прокуратуры Республики Казахстан осуществляется надзор в сфере защиты персональных данных, но он не имеет структурного, постоянного и целенаправленного характера. В основном нарушения защищенности персональных данных выявляются при проведении проверок по другим направлениям. При этом информация о проверках уполномоченного органа либо операторов баз персональных данных, проведении анализа применения законодательства и оценки актов в данной сфере отсутствует.

Нельзя не отметить, что в настоящее время разрабатывается Цифровой кодекс Республики Казахстан, принятие которого предполагает утрату силы Закона Республики Казахстан «О персональных данных и их защите».

При этом в проекте Цифрового кодекса отсутствуют положения о высшем надзоре прокуратуры и включены лишь полномочия прокурора по направлению уполномоченным органам о проведении проверок, а также по определению законности получения доступа к персональным данным судами, правоохранительными и специальными органами. Проектом Цифрового кодекса сужаются полномочия органов прокуратуры, что не корреспондируется с Конституцией и Конституционным законом «О прокуратуре». Надзор прокуратуры должен распространяться на деятельность всех государственных органов в цифровой среде, в том числе осуществляющих государственный контроль, в отношении посредников по управлению персональными данными, собственников, операторов баз данных, цифровых платформ, операторов связи, сетей связи и телекоммуникаций, а также иных лиц.

Во избежание проблем и конкуренции норм в дальнейшем полномочия органов прокуратуры в цифровой среде видится целесообразным отразить в главе проекта Цифрового кодекса, которая предусматривает положения касательно государственного контроля в сферах, регулируемых кодексом.

Также обоснованные сомнения вызывает целесообразность включения в проект Цифрового кодекса отдельной статьи, выделяющей полномочия органов прокуратуры по определению законности получения доступа к персональным данным судами, правоохранительными и специальными органами, поскольку, как действующее, так и предполагаемое законодательство позволяет уполномоченным, правоохранительным, специальным, государственным органам и судам производить сбор и обработку персональных данных без согласия субъекта персональных данных или его законных представителей. При таких обстоятельствах роль прокуратуры в данной процедуре не ясна.

С.К. Идрышева считает преждевременной кодификацию правового регулирования сверхдинамично развивающихся общественных отношений в условиях отсутствия законодательства о новейших институтах данной сферы [87].

Наряду с указанным следует отметить, что согласно подпункту 1 статьи 6 Конституционного закона «О прокуратуре» органы прокуратуры осуществляют высший надзор за законностью государственной правовой статистики и специальных учетов. В соответствии с приказом Генерального Прокурора Республики Казахстан от 05.01.2022 года №4 «О некоторых вопросах организации прокурорского надзора и контроля в сфере правовой статистики и специальных учетов» КПСиСУ является ведомством, осуществляющим в пределах компетенции Генеральной прокуратуры функции и полномочия государственного органа по формированию правовой статистики и ведению специальных учетов [88]. Закон «О государственной правовой статистике и специальных учетах» (пункт 3 статьи 12) предусматривает 18 видов специальных учетов, из которых 14 относятся к персональным данным, включая дактилоскопические сведения и данные о судимости лиц [89].

Тем самым в рамках реализации данной компетенции органы прокуратуры обладают не только надзорной функцией, но и осуществляют сбор, обработку и защиту персональных данных, являясь одновременно и надзорным органом и оператором баз, содержащих персональные данные.

В частности, КПСиСУ является оператором системы информационного обмена правоохранительных, специальных государственных и иных органов (далее – СИО ПСО), посредством которой возможен доступ к 76 информационным базам государственных органов, содержащим персональные данные. Также к информационным системам КПСиСУ, содержащим персональные данные, относятся автоматизированная дактилоскопическая информационная система (АДИС), автоматизированная информационная система «Специальные учеты» (АИС СУ) и другие, в том числе Единый реестр досудебных расследований (далее – ЕРДР) и Единый реестр административных производств (далее – ЕРАП). В этой связи на КПСиСУ возлагаются права и обязанности оператора, ответственного за обработку данных, в том числе в части защиты персональных данных.

Помимо указанного, КПСиСУ осуществляет информационно-справочное обслуживание физических и юридических лиц, что в том числе предполагает

предоставление им сведений о судимости граждан. Для реализации этих функций приказом Генерального Прокурора Республики Казахстан от 05.01.2023 года №7 утверждена «Инструкция по информационно-справочному обслуживанию физических и юридических лиц органами правовой статистики и специальных учетов» [90].

Таким образом, прокурорский надзор в сфере защиты персональных данных в Республике Казахстан является важным правовым инструментом, направленным на защиту персональных данных и недопустимость необоснованного вмешательства в частную жизнь. Законодательством сформированы принципы прокурорского надзора, которые применимы абсолютно ко всем отраслям, направлениям и видам прокурорского надзора, в том числе в сфере защиты персональных данных. При этом прокурорский надзор в сфере защиты персональных данных еще не имеет структурного, постоянного и целенаправленного характера, что говорит о необходимости совершенствования методики и алгоритмов данного вида надзора. В основном нарушения защищенности персональных данных выявляются при проведении проверок по другим направлениям надзора. При этом наряду с надзорными функциями, органы прокуратуры одновременно являются оператором ряда баз персональных данных, что накладывает на органы прокуратуры, как дополнительные права, так и обязательства.

Повышение эффективности прокурорского надзора в сфере защиты персональных данных сдерживается несовершенством законодательства. При этом при последующем совершенствовании законодательства является недопустимым сужение и ограничение прокурорского надзора в сфере защиты персональных данных.

Деятельность прокуратуры в Республике Казахстан основана на закрепленных Конституцией и Конституционным законом «О прокуратуре» принципах, которые применимы абсолютно ко всем отраслям, направлениям и видам прокурорского надзора, в том числе в сфере защиты персональных данных. При этом надзор в каком-либо определенном направлении, к примеру, в сфере защиты персональных данных может осуществляться по всем отраслям прокурорского надзора.

Под принципами прокурорского надзора следует понимать имеющие нормативно-закреплённый характер и являющиеся обязательными для каждого сотрудника системы органов прокуратуры фундаментальные, основополагающие требования и признаки, на основании которых и при обязательном соблюдении которых осуществляется деятельность органов прокуратуры.

Прокуратура осуществляет свои полномочия на принципах:

- законности;

- независимости от других государственных органов и должностных лиц и подотчетности лишь Президенту Республики Казахстан;

- недопустимости вмешательства, воспрепятствования деятельности прокурора при осуществлении своих функций и полномочий;

- гласности;

- правомерности и своевременности вмешательства;

- сохранности документов, сведений и иной информации, полученных в ходе осуществления своей деятельности, с соблюдением требований законодательства Республики Казахстан о государственных секретах и иной охраняемой законом тайне;

- обязательности актов прокурорского надзора и законных требований прокурора;

- принятия исчерпывающих мер по обеспечению законности, защите и восстановлению нарушенных прав и свобод человека и гражданина, охраняемых законом интересов юридических лиц, общества и государства.

Прокурорский надзор в сфере защиты персональных данных построен на принципах:

- признания права неприкосновенности частной жизни, личной и семейной тайны, защиты чести и достоинства, а также права на защиту персональных данных;

- справедливости;

- беспристрастности;

- объективности;

- эффективности;

- профессионализма, компетентности и постоянного повышения профессионального уровня;

- своевременности реагирования на факты нарушения законодательства в сфере персональных данных и их защиты;

- сохранности и недопустимости разглашения документов, сведений и иной информации, полученных в ходе осуществления своей деятельности и содержащих персональные данные;

- персональной ответственность за разглашение сведений, составляющих охраняемую законом тайну и информацию;

- защиты персональных данных потерпевших и других участников уголовного процесса;

- воспрепятствования разглашению персональных данных из досудебных производств и закрытых судебных разбирательств;

- принципиальной позиции в вопросе устранения нарушений законодательства в сфере персональных данных и их защите, а также в возмещении вреда и привлечении к ответственности виновных лиц;

- принятия исчерпывающих мер по обеспечению законности, защите и восстановлению нарушенных прав и свобод человека и гражданина, охраняемых законом интересов юридических лиц, общества и государства в сфере персональных данных и их защиты.

Исходя из обширного разнообразия междисциплинарных и отраслевых основополагающих начал, охватывающих исследуемую совокупность, в качестве ключевого принципа прокурорского надзора в сфере защиты персональных данных определено принятие исчерпывающих мер по

обеспечению законности, защите и восстановлению нарушенных прав и свобод человека и гражданина, охраняемых законом интересов юридических лиц, общества и государства в сфере персональных данных и их защиты.

Выводы по разделу

1. В условиях всеобщей цифровизации и хранения данных, в том числе персонального характера в цифровом формате, важность сохранения такой информации обретает особую важность. Базы персональных данных подвергаются постоянным кибератакам, значительная часть из них являются успешными и влекут утечки персональных данных. Действия злоумышленников наносят существенный ущерб государствам и коммерческим структурам, а похищенные персональные данные используются для совершения противоправных действий в отношении граждан, о чем свидетельствует серьезный рост киберпреступлений и особенно интернет-мошенничеств во всем мире.

2. Республикой Казахстан избран и успешно реализуется курс активной цифровизации всех отраслей общественных отношений. В различных мировых рейтингах, связанных с цифровизацией и вовлечением граждан в Интернет, Республика Казахстан занимает высокие позиции и является региональным лидером. Между тем, такая политика наряду с позитивными имеет и негативные последствия. Государственные и негосударственные базы данных подвергаются кибератакам, имеют место утечки персональных данных, доступ к персональным данным имеет большое количество третьих лиц, уровень киберпреступлений возрос и находится на высоком уровне.

3. В целях надлежащей защиты персональных данных граждан в Республике Казахстан проводится значительная работа, в том числе принято отраслевое законодательство. Однако, имеет место несовершенство правовых норм, понятия и предусмотренные казахстанским законодательством меры в значительной степени отличаются от тех, которые закреплены в международных правовых актах и являются ориентиром в защите персональных данных большинства зарубежных государств.

4. В вопросы защиты персональных данных вовлечены многие органы и организации, в том числе и органы прокуратуры. При этом следует констатировать, что в настоящее время прокурорский надзор в сфере защиты персональных данных является достаточно новым направлением и еще не имеет структурного и постоянного характера. Вместе с тем в рамках осуществления прокурорской деятельности нередко выявляются нарушения, совершению которых способствует наличие доступа к персональным данным. Органы прокуратуры одновременно являются оператором баз персональных данных, поскольку осуществляют сбор значительного количества персональных данных, в том числе биометрических данных, сведений о судимости и других не менее важных сведений. Деятельность органов прокуратуры по защите персональных данных основана на основных принципах, которые предусмотрены Конституцией и Конституционным

законом, а также на принципах прокурорского надзора в сфере защиты персональных данных, которые возможно выделить путем анализа законодательства, исследований и практического опыта.

2 МЕТОДИКА ОСУЩЕСТВЛЕНИЯ ПРОКУРОРСКОГО НАДЗОРА В СФЕРЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Правовая регламентация средств прокурорского надзора в сфере защиты персональных данных

Для достижения эффективных результатов прокурорского надзора в какой-либо сфере важным является наличие действенной методики прокурорского надзора в данном направлении.

Ю.Е. Винокуров отмечает, что методика прокурорского надзора тесно взаимосвязана с тактикой прокурорского надзора. Их взаимосвязь построена на том, что методика проведения проверочных мероприятий строится с учетом тактики, а тактика может обогащать новыми методами, приемами и теоретическими положениями методикой. Под понятием «методика прокурорского надзора» понимается совокупность методов и приемов, применяемых прокурорами в целях выявления, устранения и предупреждения нарушений законов и способствующих им обстоятельств. Прокурорский надзор состоит в применении предусмотренных законом правовых средств. При этом обязательные рекомендации в каких ситуациях и случаях какие именно средства необходимо применять закон не содержит и содержать не может. Такие рекомендации вырабатываются в результате научной и практической деятельности. Доказавшие свою эффективность рекомендации в дальнейшем закрепляются в правовых актах прокуратуры, методических пособиях, информационных письмах, указаниях и других подобных документах. Совокупность таких научно обоснованных и проверенных на практике методов и приемов (способов) применения правовых средств составляет методику прокурорского надзора. Тактика прокурорского надзора – это определение и реализация прокурором путей наилучшей организации и осуществления прокурорского надзора в целях достижения наилучших конечных результатов. Составными частями тактики прокурорского надзора являются тактика проверки и тактика реагирования на нарушения законов. Методика прокурорского надзора бывает общая, что предполагает методы осуществления надзора в целом, а также частная, определяющая методику осуществления надзора за исполнением отдельных законов или направлений [74, с. 109-118].

Р.М. Махьянова указывает, что «в настоящее время в органах и организациях прокуратуры разрабатывается большое количество методик о проведении проверок по различным отраслям прокурорского надзора. Однако ввиду отсутствия единого научного подхода к понятию основ тактики прокурорского надзора, содержание методик в большинстве случаев однообразно, а предлагаемые способы действий и методы применимы лишь к условиям состояния законности в конкретном периоде времени, который характеризуется статистическими и аналитическими сведениями. Тактика же учитывает динамику обстоятельств складывающейся надзорной ситуации, и ее основная задача состоит именно в изыскании рационального решения независимо от типа надзорной ситуации (типичный, не типичный) для

достижения поставленных целей. По нашему мнению, отсутствие четкого механизма методического обеспечения надзорной деятельности прокуратуры негативно отражается на результативности проверок» [91].

В научной литературе указывается, что реализация методики прокурорского надзора осуществляется, как правило, правовыми средствами прокурорского надзора. При этом законодательство Республики Казахстан, в том числе Конституционный закон «О прокуратуре» не дают определения понятию «правовые средства прокурорского надзора».

Позиция ученых относительно данного вопроса нередко расходится. О.В. Воронин указывает, что понятие «правовые средства прокурорского надзора» используется достаточно широко, но в науке нет единого подхода к его определению. Чаще всего это понятие определяют, как полномочия прокурора, а также порядок и форму их реализации, полномочия и акты прокурорского реагирования, формы реализация полномочий по выявлению, устранению и предупреждению нарушений законодательства, формы деятельности прокурора по реализации своих полномочий. Сам автор считает, что правовые средства прокурорского надзора являются комплексным понятием, включающим полномочия прокурора, акты прокурорского надзора (реагирования), а также порядок реализации прокурорских полномочий и вынесения актов прокурорского надзора [92].

Е.Р. Ергашев и Е.А. Габышева отмечают, что несмотря на отсутствие в законодательстве Российской Федерации определения понятия «правовые средства прокурора», этот вопрос вызывает оживленные дискуссии в научном сообществе. При этом среди специалистов в сфере прокурорского надзора нет единого мнения по поводу определения правовых средств прокурора. Авторы считают ошибочной позицию некоторых исследователей, которые отождествляют правовые средства прокурора с полномочиями прокурора, поскольку полномочия прокурора являются урегулированными законодательством возможностями, которые не могут быть правовыми средствами, так как правовые средства являются урегулированными законом действиями прокурора. Правовые средства прокурора связаны и обусловлены его полномочиями, но не сводятся только к ним. Лишь при наделении прокурора соответствующими полномочиями правовые средства могут быть действенным инструментом. Единой позиции нет и относительно квалификации правовых средств прокурора. В некоторых работах правовые средства прокурора разделяются на общие, являющиеся характерными для всех отраслей прокурорского надзора, и специальные, которые характерны только для отдельных отраслей прокурорского надзора. В других правовые средства прокурора подразделяют на процессуальные и непроцессуальные, применяемые к поднадзорным и неподнадзорным субъектам. Существуют и другие позиции. По результатам изучения и анализа мнения различных ученых Е.Р. Ергашев и Е.А. Габышева предложили под правовыми средствами прокурора понимать регламентированные законодательством и осуществляемые в определенном порядке действия прокурора, которые

направлены на выявление нарушений закона, способствующих им причин и условий, восстановление нарушений законности и привлечение к ответственности виновных лиц. По целевому назначению предложено правовые средства прокурора разделить на средства выявления нарушений закона и средства реагирования на нарушения закона [93].

Следует отметить, что вопросы правовых средств прокурора широко не исследовались, фундаментальные работы по данному направлению отсутствуют. В научной литературе имеются исследования российских ученных.

При этом еще в 2014 году А.Б. Ахметова указывала, что «прокуратура Республики Казахстан наделена большим перечнем функций, чем прокуратура Российской Федерации. Прокурорский надзор, в отличие от Российской Федерации, в Республике Казахстан является высшим. Здесь прокуратура, кроме тех функций, которые она выполняется в Российской Федерации, формирует государственную правовую статистику с целью обеспечения целостности, объективности и достаточности статистических показателей, ведет специальные учеты, осуществляет надзор за применением законодательства в сфере правовой статистики и специальных учетов; координирует деятельность по обеспечению законности, правопорядка и борьбы с преступностью» [94].

Принимая во внимание специфику казахстанской прокуратуры, в том числе наделение дополнительными функциями в результате реформ Конституции 2017 и 2022 года, полагаем неверным для Казахстана под правовыми средствами прокурора понимать только действия, которые направлены на выявление нарушений закона, способствующих им причин и условий, восстановление нарушений законности и привлечение к ответственности виновных лиц.

Так, с 2022 года Конституция и Конституционный закон «О прокуратуре» помимо осуществления высшего надзора выделяют еще два основных назначения прокуратуры - представление интересов государства в суде, а также осуществление уголовного преследования от имени государства.

Кроме того, в составе системы органов прокуратуры Республики Казахстан имеется два ведомства (КПСиСУ и Комитет по возврату активов), а также Академия правоохранительных органов при Генеральной прокуратуре, сотрудники которых являются прокурорами, но большинство из них не осуществляют надзорных функций. К примеру, в соответствии со статьей 6 Закона «О государственной правовой статистике» на КПСиСУ возложено 22 функции, из которых 21 функция (формирование правовой статистики, ведение специальных учетов, информационно-аналитическая деятельность и т.д.) не относится к надзорной. Академия правоохранительных органов осуществляет обучение, подготовку, переподготовку, повышение квалификации и профессионального уровня сотрудников правоохранительных органов, а также координацию и проведение межведомственных научных исследований. Таким образом, действия данной категории казахстанских прокуроров не направлены

на выявление нарушений закона, способствующих им причин и условий, восстановление нарушений законности и привлечение к ответственности виновных лиц.

Также необходимо отметить, что 15.02.2021 года Президент Казахстана К.К. Токаев на встрече с руководителями органов прокуратуры отметил необходимость укрепления позиции по координационной деятельности прокуратуры не только в рамках правоохранительной системы, но и с другими государственными органами. Уже в 2022 году на законодательном уровне в Конституционном законе «О прокуратуре» появилась новая глава, регулирующая деятельность и наделяющая прокуратуру функциями по координации и взаимодействию.

Н.М. Абдиров отмечает, что «динамика развития координационных отношений и практика координационной деятельности вновь создаваемых координационных органов свидетельствует о том, что именно прокуратура является единственным и безальтернативным органом, способным оптимально координировать деятельность правоохранительных органов по обеспечению законности, правопорядка и борьбы с преступностью, в силу специфики своего правового статуса», а также, что «при осуществлении координационной деятельности недопустимо разглашение сведений, представляющих собой различные секреты личной жизни гражданина» [95].

Учитывая слабую научную разработанность темы правовых средств прокурора в Казахстане, предлагается авторская классификация, а именно в правовые средства прокурора предлагается включить:

- правовые средства прокурорского надзора;
- правовые средства представления интересов государства в суде;
- правовые средства уголовного преследования от имени государства;
- правовые средства по координации и взаимодействию;
- правовые средства реализации иных полномочий прокурора.

Правовые средства представления интересов государства в суде разделяются на процессуальные и непроцессуальные. Под процессуальными следует понимать правовые средства, вытекающие из полномочий прокурора, регламентированных уголовно-процессуальным, гражданским процессуальным законодательством, законодательством об административных правонарушениях и административном судопроизводстве, под непроцессуальными понимаются иные правовые средства прокурора, используемые в данном виде деятельности прокурора, в том числе мониторинг, обобщение судебной практики, рассмотрение обращений, подготовка заключений, согласование позиции с вышестоящим прокурором и другие.

Правовые средства уголовного преследования от имени государства разделяются на процессуальные и непроцессуальные. Под процессуальными следует понимать правовые средства, вытекающие из полномочий прокурора, регламентированных уголовно-процессуальным законодательством, под непроцессуальными понимаются иные правовые средства прокурора, используемые в данном виде деятельности прокурора, в том числе создание

межведомственных следственно-оперативных групп, личные приемы граждан, оперативные совещания и другие.

Правовые средства по координации и взаимодействию включают в себя правовые средства, вытекающие из полномочий прокурора по координации деятельности правоохранительных и иных государственных органов по обеспечению законности, правопорядка и противодействию преступности, а также взаимодействия прокуратуры по защите и восстановлению нарушенных прав и свобод человека и гражданина с государственными, местными представительными и исполнительными органами, органами местного самоуправления, учреждениями, их должностными лицами, субъектами квазигосударственного сектора и иными организациями независимо от форм собственности, а также с Уполномоченным по правам человека. К действиям прокурора, входящих в данную категорию правовых средств, относятся проведение заседаний Координационного совета по обеспечению законности, правопорядка и борьбы с преступностью, межведомственных совещаний, коллегий, подписание меморандумов, форумов по защите бизнеса и другие мероприятия, схожего характера. Кроме того, к этой категории можно отнести координацию межведомственных научных исследований в сфере правоохранительной деятельности, а также координацию деятельности по международно-правовому сотрудничеству в целях возврата активов.

Правовые средства реализации иных полномочий прокурора включают в себя правовые средства, вытекающие из полномочий прокурора по формированию государственной правовой статистики, выявлению и возврату государству незаконно приобретенных активов, обучению и повышению квалификации сотрудников правоохранительных органов, а также участие участию в нормотворческой деятельности.

При этом полагаем целесообразным согласиться с мнением, что к правовым средствам прокурорского надзора относятся средства выявления нарушений закона (способствующих им причин и условий), средства восстановление нарушений законности и средства привлечения к ответственности виновных лиц.

Более подробно остановимся на правовых средствах прокурорского надзора по выявлению нарушений закона в Республике Казахстан, которые в первую очередь закреплены статьей 17 Конституционного закона «О прокуратуре», где указано, что высший надзор от имени Республики Казахстан осуществляется посредством проведения проверки соблюдения законности, анализа состояния законности, оценки актов, вступивших в силу.

По сведениям КПСиСУ за 2022-2023 годы и 9 месяцев 2024 года только в социально-экономической сфере прокурорами проведено 16 146 проверок, в ходе которых выявлено 61 006 нарушений, а также 17 596 анализов, в ходе которых выявлено 36 397 нарушений. Статистический учет проведенных оценок актов, вступивших в законную силу, не ведется. Однако учитывается количество изученных прокурором изданных нормативно-правовых актов. За указанный период изучен 12 631 такой акт [96].

При этом порядок их назначения и проведения определяется Конституционным законом, законами Республики Казахстан и актами Генерального Прокурора. Также отдельно отмечено, что в сферах контрразведывательной деятельности, обеспечения безопасности охраняемых лиц и объектов высший надзор осуществляется с учетом особенностей законодательства в этой сфере.

Порядок назначения и проведения проверок соблюдения законности, анализов состояния законности, оценки актов, вступивших в силу, пределы и ограничения прав прокурора при осуществлении таких форм высшего надзора определены статьями 18, 20 и 21 Конституционного закона «О прокуратуре». Приказом Генерального Прокурора Республики Казахстан от 17.01.2023 года №32 «О некоторых вопросах организации прокурорского надзора» утверждены «Правила назначения и проведения органами прокуратуры проверок соблюдения законности, анализа состояния законности, а также осуществления оценки актов, вступивших в силу», которые детализируют требования к проведению проверок соблюдения законности, анализа состояния законности, осуществлению оценки актов, вступивших в силу » [97].

Таким образом, в Республике Казахстан основными правовыми средствами прокурора по выявлению нарушений законности являются проверка соблюдения законности, анализ состояния законности и оценка актов, вступивших в законную силу. При этом проверку соблюдения законности, анализ состояния законности и оценку актов, вступивших в законную силу следует считать правовыми средствами прокурора по выявлению нарушений законности являются в узком смысле. В более широком смысле полагаем целесообразным также считать правовыми средствами прокурорского надзора по выявлению нарушений и другие функции, вытекающие из полномочий прокурора, а именно к правовым средствам прокурора по выявлению нарушений в более широком смысле отнести:

- привлечение специалистов государственных, правоохранительных органов и других организаций, независимо от формы собственности;
- привлечение сотрудников правоохранительных органов для обеспечения безопасности лиц, проводящих проверку;
- назначение экспертиз;
- инициирование незамедлительной отмены мер запретительного или ограничительного характера, приостановления полностью или частично действия незаконного акта;
- истребование информации, материалов и документов, уголовных, гражданских, административных дел, дел об административных правонарушениях, исполнительных производств, необходимых для осуществления надзора, получение доступа к ним;
- получение доступа к информационным системам и ресурсам правоохранительных и иных государственных органов и организаций;
- изучение статистических данных, сведений государственных и международных организаций, средств массовой информации, материалов

гражданских и уголовных дел, дел об административных правонарушениях, а также иных источников информации;

- получение доступа на объект проверки, проверяемую территорию, к имуществу, связанному с предметом проверки;

- применение имеющихся в наличии технических средств, в том числе технических средств фиксации, замера, отбора проб для сбора фактической информации о проверяемом субъекте/объекте, документах, материалах, помещениях, процессе деятельности проверяемого субъекта/объекта, а также подтверждения фактов нарушения законности;

- осуществление персональной фото-видеосъемку лица без его согласия при воспрепятствовании законной деятельности, совершении нарушения либо для фиксации таких фактов;

- вызов и получение пояснений от должностных, физических лиц и представителей юридических лиц по вопросам проводимой проверки;

- инициирование осуществления оперативно-розыскных мероприятий для выявления скрытых нарушений законодательства;

- проведение визуального осмотра объекта (субъекта), расположенного в открытых для посещения местах (места общественного пользования либо на открытой местности);

- направление уполномоченным органам требований о производстве проверок с обязательным информированием об их результатах;

- рассмотрение обращений;

- проведение проверки учетно-регистрационной дисциплины;

- проведение проверки законности доставления, задержания лиц по подозрению в совершении уголовных правонарушений, лиц, совершивших административные правонарушения, а также порядка и условий содержания лиц, находящихся под стражей либо иным ограничением свободы;

- мониторинг информационной системы об электронном учете посетителей в правоохранительных органах;

- санкционирование проведения оперативно-розыскных и контрразведывательных мероприятий.

Правовыми средствами прокурорского надзора по восстановлению нарушений законности являются акты прокурорского надзора, к которым относятся протест, санкция, представление, постановление и акты прокурорского реагирования, к которым относятся ходатайство, заявление (иск), обращение, разъяснение о недопустимости нарушений законов.

По мнению А.С. Майлыбаева, «правовой основой реагирования на выявленные случаи нарушения закона являются составленные акты, содержащие в себе отражение соответствующих нарушений, выявленных в ходе прокурорского надзора, а также требования для их устранения» [98].

Следует отметить, что акты прокурорского надзора и реагирования обязательны для рассмотрения, исполнения органами, организациями и должностными лицами, которым они адресованы. При этом у каждого из них свои особенности, сроки рассмотрения и основания вынесения.

Так, при выявлении актов, противоречащих Конституции Республики Казахстан, законам, актам Президента и ратифицированным международным договорам, прокурором приносится протест в государственный орган, учреждение, организацию, должностному или иному уполномоченному лицу, принявшему незаконный акт. До принятия решения по протесту прокурор вправе приостановить исполнение опротестованного акта либо действия своим постановлением. В случае отклонения протеста, прокурор уполномочен обратиться в суд с в порядке, предусмотренным ГПК и АППК. Таким же образом опротестовываются незаконные действия или бездействия административных органов и должностных лиц.

При этом существует ограничение, а именно не подлежат опротестованию законодательные акты Республики Казахстан, акты Президента, Администрации Президента, Конституционного Суда и Высшей аудиторской палаты (по итогам проведенных проверок).

Санкция прокурора подразумевает под собой согласие на совершение отдельных действий правоограничительного характера либо на получение доступа к сведениям, содержащим охраняемую законом тайну. Другими словами санкцией разрешается совершение процессуальных действий, которыми могут быть затронуты права граждан. Санкция крайне важна с точки зрения недопущения бесконтрольного доступа правоохранительных и специальных органов к информации персонального характера и к сведениям о частной жизни лица.

Указание прокурора дается по вопросам досудебного расследования, оперативно-розыскной деятельности, негласных следственных действий, дополнительных проверок по делам об административных правонарушениях, исполнительного производства, исполнения наказаний, проверок по требованию прокуратуры, государственной правовой статистики и специальных учетов, а также по иным вопросам.

Представление прокурором вносится для устранения нарушений законности, устранения причин и условий, способствующих совершению уголовных и иных правонарушений, а также в иных случаях, установленных законами. При чем, такие случаи имеют существенно различающийся характер. К примеру, представление Генеральным Прокурором может вноситься в адрес Президента и Парламента страны для получения согласия на привлечение к уголовной или административной ответственности судей и депутатов.

Постановление прокурором выносится во многих случаях, в том числе при возбуждении дисциплинарных производств, прекращении оперативно-розыскных-мероприятий и негласных следственных действий, назначении проверок, экспертиз, принудительном исполнении актов прокурора, в случаях, предусмотренных уголовно-процессуальным, уголовно-исполнительным законодательством, законодательством об административных правонарушениях и в других. В сроки, установленные прокурором, постановление подлежит обязательному исполнению.

Ходатайство прокурором инициируется для пересмотра судебных актов, не вступивших в законную силу, и вносится в порядке, установленном процессуальным законодательством.

Прокурор вправе обратиться с заявлением (иском) в суд в порядке и на основаниях, которые установлены законами. В соответствии с пунктом 2 статьи 8 и пунктом 3 статьи 54 Гражданского процессуального кодекса прокурор вправе обратиться в суд с иском в целях осуществления возложенных на него обязанностей. Иски могут быть поданы для восстановления нарушенных прав и защиты интересов:

- лиц, которые в силу физических, психических и иных обстоятельств не могут самостоятельно осуществлять их защиту;

- лиц, общества и государства, если это необходимо для предотвращения необратимых последствий для жизни, здоровья людей либо безопасности Республики Казахстан;

- неограниченного круга лиц;

- субъектов квазигосударственного сектора, крупного предпринимательства, в том числе банков, получавших государственную поддержку.

Следует отметить, что согласно пункту 3 статьи 31 Административного процедурно-процессуального кодекса по первым двум основаниям прокурором может быть подан и административный иск.

Основания для подачи заявления (иска) прокурором, предусмотренные законами, крайне многочисленны. К примеру, прокурор может подать заявление о признание забастовки незаконной, признании лицензии недействительной, ограничении и лишении родительских прав, признании усыновления незаконным, отмене усыновления, признании брака недействительным, признании недействительным соглашения об уплате алиментов, нарушающего интересы получателя алиментов и многих других случаях, однако исчерпывающего перечня в настоящее время нет. Ряд таких оснований указаны в методических рекомендациях органов прокуратуры. К примеру, механизм конфискации преступных доходов и возврата имущества включает возможное инициирование иска о возмещении причиненного преступлением ущерба, возврате имущества государству и иному законному владельцу или собственнику [99].

Прокуроры вправе выступить с обращением к должностным лицам, государственным органам, физическим и юридическим лицам в целях обеспечения законности и общественной безопасности, предупреждения правонарушений, а также защиты прав и свобод человека и гражданина. Обращение распространяется через средства массовой информации или иным публичным способом.

В свою очередь для предупреждения правонарушений, обеспечения общественной безопасности, защиты прав и свобод человека и гражданина или при наличии сведений о готовящихся противоправных деяниях прокурор также может разъяснить физическим лицам и представителям юридических лиц о

недопустимости нарушений законов и предупредить их об установленной ответственности. Разъяснение дается в письменной или устной форме.

Вместе с тем, исходя из положений Конституционного закона «О прокуратуре» и «Правил назначения и проведения органами прокуратуры проверок соблюдения законности, анализа состояния законности, а также осуществления оценки актов, вступивших в силу» к правовым средствам прокурорского надзора по восстановлению нарушений законности также можно отнести проведение совещаний с обсуждением результатов проверки, инициирование перед Генеральным Прокурором вопроса об обращении в Конституционный и (или) Верховный суды, направление информационных писем.

Правовые средства прокурорского надзора по привлечению к ответственности виновных лиц включают в себя:

- передачу материалов в подразделение по надзору за законностью уголовного преследования, в том числе для принятия решения о регистрации фактов в ЕРДР;
- регистрацию материалов в Книге учета информации (далее – КУИ);
- возбуждение производства по делу об административном правонарушении;
- возбуждение дисциплинарного производства;
- постановка вопроса о привлечении к ответственности в актах надзора.

По сведениям КПСиСУ за 2022-2023 годы и 9 месяцев 2024 года по актам надзора прокурора только к дисциплинарной, административной и материальной ответственности привлечено 91 363 человека.

Правовые средства прокурорского надзора по выявлению нарушений закона (способствующих им причин и условий), восстановлению нарушений законности и привлечению к ответственности виновных лиц являются общими для всех отраслей и направлений прокурорского надзора, за исключением тех, порядок реализации которых урегулирован отдельными законодательными нормами, к примеру, уголовно-процессуальным законодательством. Соответственно, они распространяются и на прокурорский надзор в сфере защиты персональных данных.

При этом ни в научной литературе, ни в законодательных актах, ни в методических рекомендация органов прокуратуры правовые средства прокурорского надзора в сфере защиты персональных данных отдельно не выделялись. Однако считаем такую задачу вполне реализуемой, для необходимо учитывать следующее.

В.Д. Рузанова указывает, что правовой режим персональных данных является комплексным и содержит нормы различных отраслей права, в связи с чем для защиты прав субъектов персональных данных могут использоваться разноотраслевые механизмы [41, с. 77-82].

В соответствии с Конституционным законом «О прокуратуре» прокурор вправе инициировать досудебное расследование, что применимо и к случаям выявления нарушений законодательства о персональных данных, в которых

усматривается наличие уголовного правонарушения. Также пункт 4 статьи 32 Уголовно-процессуального кодекса наделяет прокурора правом начать производство по делам частного обвинения [100], к категории которых части 1 и 2 статьи 147 Уголовного кодекса (Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите).

Помимо указанного следует отметить, что в принятом в 2001 году Кодексе об административных правонарушениях (далее – КоАП) появилась статья 84-1, которая ввела административную ответственность за нарушение законодательства о персональных данных. Возбуждение дел об административном правонарушении такой категории относилось к компетенции прокурора, а рассмотрение к компетенции суда [101].

В новом КоАП 2014 года сохранилась административная ответственность за такие нарушения, которая предусмотрена статьей 79.

При этом возбуждение дел этой категории, как и раньше, относилось к компетенции прокурора, а рассмотрение к компетенции суда [102].

25.06.2020 года, как известно, появился уполномоченный орган в сфере персональных данных. К его компетенции было отнесено составление протоколов о правонарушениях и рассмотрение дел об административных правонарушениях по статье 79 КоАП.

Между тем, согласно статье 805 КоАП прокурор выносит постановление о возбуждении дел об административных правонарушениях по конкретным статьям КоАП, но имеет право вынести такое постановление и об иных правонарушениях, то есть по сути по любой статье КоАП, в том числе за нарушение законодательства Республики Казахстан о персональных данных и их защите.

Также Закон «О персональных данных и их защите» определяет еще одно полномочие прокуратуры, а именно направление прокурором в адрес уполномоченного органа требования о проведении внеплановой проверки по конкретным фактам причинения либо об угрозе причинения вреда правам и законным интересам физических и юридических лиц, государства (подпункт 3 пункта 3 статьи 27-3 Закона). Данное полномочие должно быть действенным правовым средством прокурорского надзора.

К примеру, в 2024 году ввиду взлома инфраструктуры Robo Finance, материнской экосистемы, поддерживающей многие финансовые организации, в том числе Zaimer.kz, произошла утечка персональных данных значительного числа казахстанцев. По сведениям уполномоченного органа только за 6 дней (7-12 марта) по данному факту поступило более 1,4 тысяч жалоб [103]. При этом точное количество пострадавших оказалось неизвестным, что говорит об их неограниченном круге. Соответственно, в этот и других похожих случаях органам прокуратуры следует направлять в адрес уполномоченного органа требования о проведении проверок.

Помимо указанного относительно защиты неприкосновенности частной жизни, защиты персональных данных следует отметить право Генерального

Прокурора и его заместителей на внесение в уполномоченный орган в области масс-медиа представления об устранении нарушений законности с требованием о принятии мер по временному приостановлению доступа к объектам информатизации в виде программного обеспечения и интернет-ресурса и (или) размещенной на них информации при использовании сетей и (или) средств связи в преступных целях, наносящих ущерб интересам личности, общества и государства, а также в иных случаях, что предусмотрено частью 1 статьи 41-1 Закона «О связи» [104].

Нельзя не отметить межведомственное взаимодействие. К примеру, с начала 2019 года функционирует система «Кибернадзор», которая предназначена для систематизации и оптимизации, проводимой государственными органами работы по выявлению, учету, оценке и блокированию доступа к противоправным материалам в сети Интернет. В работе задействованы 22 государственных органа, в том числе Генеральная прокуратура. Среди выявляемых противоправных материалов имели место и нарушения законодательства о защите персональных данных [105].

Таким образом, учитывая слабую научную разработанность темы правовых средств прокурора в Казахстане, предлагается авторская классификация, а именно в правовые средства прокурора предлагается включить:

- правовые средства прокурорского надзора;
- правовые средства представления интересов государства в суде;
- правовые средства уголовного преследования от имени государства;
- правовые средства по координации и взаимодействию;
- правовые средства реализации иных полномочий прокурора.

Правовые средства прокурорского надзора состоят из:

- правовых средств прокурора по выявлению нарушений закона (способствующих им причин и условий);
- правовых средств прокурора по восстановлению нарушений законности;
- правовых средств прокурора по привлечению к ответственности виновных лиц.

Вместе с тем, с учетом анализа законодательства, а также практики прокурорского надзора правовыми средствами прокурорского надзора в сфере защиты персональных данных предлагается считать:

- проверку соблюдения законности в сфере защиты персональных данных;
- анализ состояния законности в сфере защиты персональных данных;
- оценку актов в сфере обработки персональных данных, вступивших в законную силу;
- рассмотрение обращений о нарушениях законодательства о персональных данных и их защите;
- инициирование досудебного расследования;

- инициирование производства по делам об административных правонарушениях по фактам нарушения законодательства в сфере персональных данных и их защиты;

- требование от уполномоченного органа в сфере защиты персональных данных проведения внеплановой проверки по конкретным фактам причинения либо об угрозе причинения вреда правам и законным интересам физических и юридических лиц, государства;

- дача уполномоченному органу в сфере защиты персональных данных обязательного для исполнения указания по вопросам внеплановой проверки, проводимой по требованию прокурора;

- требование от уполномоченного органа в области масс-медиа принятия мер по временному приостановлению доступа к объектам информатизации в виде программного обеспечения и интернет-ресурса и (или) размещенной на них информации;

- прекращение незаконных оперативно-розыскных мероприятий и негласных следственных действий;

- обеспечение конфиденциальности данных досудебных расследований и закрытых судебных разбирательств;

- назначение экспертиз, в том числе судебных технологических экспертиза, судебно-экспертных исследований средств компьютерной технологии;

- межведомственное взаимодействие в сфере защиты персональных данных, в том числе межведомственных совещаний;

- взаимодействие с Уполномоченным по правам человека по вопросам защиты персональных данных граждан;

- проведение заседаний Координационного совета по обеспечению законности, правопорядка и борьбы с преступностью по вопросам совершения преступлений в отношении охраняемой законом информации, а также преступлений, совершенных с использованием похищенных персональных данных;

- проведение коллегий по вопросам защиты персональных данных;

- подписание меморандумов с ведущими организациями в области цифрового права и защиты персональных данных;

- участие в нормотворческой деятельности в целях совершенствования законодательства о персональных данных и их защите.

2.2 Прокурорская проверка, анализ и оценка актов, вступивших в законную силу, как основные правовые инструменты прокурора в сфере защиты персональных данных

Л.В. Потапова и А.И. Британов указывают, что прокурорская проверка является ключевым правовым инструментом надзорной деятельности, а также наиболее распространенным и максимально действенным способом обнаружения нарушений закона, а также реагирования на них. Проверка должна подвергаться реформам, чтобы отвечать актуальным запросам

общества. Обновления требует и методический аспект прокурорской проверки. При этом не все сферы надзорного процесса органов прокуратуры обеспечены методическими разработками, что особенно проявляется при формировании новых направлений, которые становятся приоритетными ввиду определенных обстоятельств либо имеющихся поручений [106].

Исходя из положений, предусмотренных статьей 18 Конституционного закона «О прокуратуре», а также «Правил назначения и проведения органами прокуратуры проверок соблюдения законности, анализа состояния законности, а также осуществления оценки актов, вступивших в силу», основанием для проверки соблюдения законности являются поручение Президента или Генерального Прокурора Республики Казахстан.

Еще одним основанием является необходимость защиты прав, свобод и законных интересов лиц, которые не могут самостоятельно осуществлять их защиту в силу определенных обстоятельств, несовершеннолетних лиц, неограниченного круга лиц, для предотвращения необратимых последствий для жизни, здоровья людей либо безопасности Республики Казахстан, а также для защиты субъектов частного предпринимательства при вмешательстве в их деятельность государственных, местных представительных и исполнительных органов, органов местного самоуправления, их должностных лиц. По данному основанию решение о проведении проверки соблюдения законности может быть принято заместителями Генерального Прокурора, прокурорами областей и районов, а также приравненными к ним прокурорами. По сути, данное основание определяет пределы высшего надзора в форме проверки соблюдения законности, если это не касается поручения Президента Республики Казахстан или Генерального Прокурора.

Обязательным условием для проведения проверки соблюдения законности является вынесение соответствующего постановления и его последующая регистрация в государственном органе по правовой статистике и специальным учетам. При этом проверка деятельности субъектов частного предпринимательства может проводиться только по поручению Президента Республики Казахстан, Генерального Прокурора либо по согласованию с ними. Проверка соблюдения законности может быть проведена только лицами, указанными в постановлении об ее проведении, и должна быть проведена в течение не более тридцати рабочих дней. При этом в установленных случаях допускается приостановление проверки, а также продление срока ее проведения, но не более чем на тридцать рабочих дней.

При проведении прокурорами проверок соблюдения законности не допускается нарушение сроков их проведения, истребование не относящихся к предмету проверки документов и информации. Не допускается разглашение полученных сведений, в том числе персональных данных. Также запрещается воспрепятствование нормальному функционированию проверяемого объекта. Исключением являются случаи, создающие угрозу законности и общественному порядку, социально-экономической стабильности в регионе, конституционному строю и национальной безопасности Республики Казахстан,

а также угрожающие возникновением необратимых последствий для жизни и здоровья людей.

Для участия в проверке могут быть привлечены специалисты государственных, правоохранительных органов и других организаций, независимо от формы собственности. Также для обеспечения безопасности лиц, проводящих проверку, возможно привлечение сотрудников правоохранительных органов.

В ходе проверки соблюдения законности прокурор вправе:

- назначить экспертизу;

- требовать незамедлительной отмены мер запретительного или ограничительного характера, приостановления полностью или частично действия незаконного акта;

- истребовать информацию, материалы и документы, уголовные, гражданские, административные дела, дела об административных правонарушениях, исполнительные производства, необходимые для проведения проверки, получать доступ к ним, а также к информационным системам и ресурсам правоохранительных и иных государственных органов и организаций;

- получать доступ на объект проверки, проверяемую территорию, к имуществу, связанному с предметом проверки;

- для сбора фактической информации о проверяемом субъекте/объекте, документах, материалах, помещениях, процессе деятельности проверяемого субъекта/объекта, а также подтверждения фактов нарушения законности применять имеющиеся в наличии технические средства, в том числе применять технические средства фиксации, замера, отбора проб;

- при воспрепятствовании законной деятельности, совершении нарушения либо для фиксации таких фактов осуществлять персональную фото-видеосъемку лица без его согласия;

- вызывать и получать пояснения от должностных, физических лиц и представителей юридических лиц по вопросам проводимой проверки;

- вносить акты прокурорского надзора и реагирования, а также реализовать иные полномочия, установленные Конституционным законом и иными законами Республики Казахстан;

- для выявления скрытых нарушений законодательства инициировать осуществление оперативно-розыскных мероприятий;

- требовать производства уполномоченными органами проверок с обязательным информированием об их результатах.

Л.В. Потапова характеризует проверку, как основное правовое средство, а также отмечает, что «методика прокурорской проверки представляет собой некую инструкцию, содержащую алгоритм действий и решений, принимаемых в рамках проверочного мероприятий на примере определенного направления надзора, поднадзорного объекта или конкретного нарушения» [107].

В правовых актах и методических рекомендациях не закреплены порядок и основания прокурорских проверок соблюдения законности в сфере применения законодательства о персональных данных и их защите, что,

учитывая текущую ситуацию с защищенностью персональных данных, видится не вполне обоснованным.

Проверки соблюдения законности в сфере защиты персональных данных должны быть 2 видов: предметные, направленные на проверку соблюдения законности в сфере применения законодательства о персональных данных и их защите, а также тематические, то есть проводимое по иным вопросам, но с выключением в предмет проверки вопроса защиты персональных данных.

Предметные проверки могут проводиться:

1. В деятельности уполномоченного органа в сфере защиты персональных данных.

2. В деятельности государственных органов и их должностных лиц по вопросам соблюдения законодательства о персональных данных и их защите.

3. В деятельности местных исполнительных органов по вопросам реализации их компетенции.

4. В деятельности квазигосударственных организаций, государственных учреждений (школы, больницы и т.д.), коммунальных предприятий, других организаций.

5. В деятельности собственников и операторов баз, содержащих персональные данные.

6. В деятельности правоохранительных, специальных и иных государственных органов относительно законности получения пользователями сведений из СИО ПСО, ЕРДР и ЕРАП.

7. В иных случаях, в том числе по поручениям Президента и Генерального Прокурора Республики Казахстан.

Иные случаи могут быть крайне разнообразными, от случаев массовой утечки персональных данных, до проверок организаций, осуществляющих обслуживание информационных систем и баз данных, а также предоставляющих услуги связи.

В.И. Солдатова описывает случай предоставления оператором связи третьему лицу сведений об абонентах, их IP-адресах, предпочтениях и запросах в сети Интернет, что является нарушением их прав на защиту персональных данных [108].

Тематические проверки с выключением в предмет проверки вопроса защиты персональных данных могут проводиться по всем отраслям и направлениям прокурорского надзора. При этом полагаем, что упор должен быть на неопределенный круг лиц, защиту прав уязвимых слоев, несовершеннолетних и лиц, которые не могут себя защитить.

Примером может послужить проведенная в 2024 году Генеральной прокуратурой Казахстана проверка по вопросам соблюдения законодательства в сфере здравоохранения, в ходе которой установлены многочисленные факты внесения персональных данных граждан в отчеты о посещении медицинских учреждений и получении медицинских процедур. По результатам проверки внесен акт надзора, в котором поставлен вопрос о внедрении процедуры аутентификации пациентов для подтверждения фактов действительного

получения медицинских услуг. По результатам рассмотрения акта надзора внедрен цифровой механизм подтверждения специалиста, который в качестве пилотного проекта внедрен в 37 медицинских объектах г. Астана, а с 2025 году будет поэтапно внедряться по всей стране. Данный цифровой механизм предусматривает биометрическую идентификацию пациентов при посещении медицинских учреждений, что делает невозможным фальсификацию отчетов об оказанных медицинских услугах, а также предотвращает нецелевое расходование бюджетных средств. По предварительным оценкам внедрение данной технологии снизило статистические показатели оказанных медицинских услуг на 24,5% [109].

Исходя из положений, предусмотренных статьей 20 Конституционного закона «О прокуратуре», а также «Правил назначения и проведения органами прокуратуры проверок соблюдения законности, анализа состояния законности, а также осуществления оценки актов, вступивших в силу», основанием проведения анализа состояния законности являются:

- постоянный мониторинг ситуации на поднадзорной территории;
- полученные из различных источников информации, в том числе обращений, информаций, документов и иных материалов сведения и данные о нарушениях законности;
- поручения Президента Республики Казахстан, Генерального Прокурора;
- поручения вышестоящей прокуратуры;
- годовой или квартальный план актуальных вопросов с учетом приоритетности направлений либо особенностей региона.

В соответствии с пунктами 33-35 «Правил назначения и проведения органами прокуратуры проверок соблюдения законности, анализа состояния законности, а также осуществления оценки актов, вступивших в силу» раз в квартал анализ по вопросу защиты прав предпринимателей, раз в полгода прокуроры проводят анализы по 10 различным вопросам (расходование бюджетных средств, осуществление закупа товаров, работ и услуг, применение налогового, экологического законодательства, законодательства, в области предупреждения и ликвидации чрезвычайных ситуаций природного и техногенного характера, об особо охраняемых природных территориях, о недрах и недропользовании, а также письменным и устным обращениям по фактам вмешательства в деятельность субъектов предпринимательства), не реже одного раза в год еще по 4 направлениям (законность усыновления, работа с детьми с особенностями поведения, защита прав детей с ограниченными возможностями, защита прав лиц с инвалидностью). В пунктах 36 и 37 определены по 5 вопросов для военных и транспортных прокуроров, которые они должны анализировать не реже одного раза в год.

Анализ инициируется рапортом, который согласовывается соответствующим руководителем органов прокуратуры. В рапорте указываются основания, предмет, период и сроки проведения анализа, а также лицо, инициирующее его проведение. В некоторых случаях проведение анализа может проводиться предметно-сквозной группой под руководством

руководителя самостоятельного структурного подразделения Генеральной прокуратуры, органов военной и транспортной прокуратуры, прокурора области и приравненного к нему прокурора, районного и приравненного к нему прокурора, а также их заместителей либо лиц, исполняющих их обязанности. В этом случае к проведению анализа может быть привлечены органы, ведомства и учреждения органов прокуратуры.

Анализ состояния законности должен быть проведен в течение не более тридцати рабочих дней. При этом в установленных случаях допускается приостановление, а также продление срока проведения анализа, но не более чем на тридцать рабочих дней.

Проведение анализа предполагается без посещения прокурорами субъектов (объектов) путем изучения статистических данных, сведений государственных и международных организаций, средств массовой информации, материалов гражданских и уголовных дел, дел об административных правонарушениях, а также иных источников информации.

В ходе анализа используются:

1) статистические данные;

2) информация о выделенных средствах из государственного бюджета;

3) итоги встреч с населением;

4) факты неэффективной работы государственных органов, в том числе по вопросам профилактики экстремизма и терроризма, выявления, предупреждения и локализации нарушений общественного порядка, которые могут вызвать конфликты на межэтнической и/или межконфессиональной почве, социальное недовольство граждан, акции протеста;

5) результаты рассмотрения обращений физических и юридических лиц уполномоченными государственными органами;

6) публикации в средствах массовой информации (в том числе на интернет-ресурсах);

7) информация государственных органов, их баз данных;

8) информационные системы и ресурсы, в том числе интегрированные с системой информационного обмена правоохранительных, специальных государственных и иных органов;

9) материалы уголовных, гражданских, административных дел и дел об административных правонарушениях;

10) результаты предыдущих проверок прокуратуры и государственных органов;

11) другие источники информации.

При проведении анализа состояния законности прокурор вправе:

- истребовать от государственных, местных представительных и исполнительных органов, органов местного самоуправления и иных организаций независимо от форм собственности информацию, документы и иные материалы, связанные с проведением анализа состояния законности;

- получать доступ к информации и материалам, связанным с проведением анализа;

- вызывать и получать пояснения от должностных, физических лиц и представителей юридических лиц по вопросам проводимого анализа;

- назначить экспертизу в случаях, требующих специальных научных знаний и когда без ее назначения не представляется возможным реализовать анализ;

- проводить визуальный осмотр объекта (субъекта), расположенного в открытых для посещения местах (места общественного пользования либо на открытой местности), в том числе объектов транспорта (поезда, воздушные и морские суда) и их оборудования, путем применения фото и видеофиксации в случаях воспрепятствования законной деятельности прокурора, совершения нарушения либо необходимости фиксации фактов, подтверждающих нарушение законности;

- направлять государственному органу требования на проведение таможенного досмотра товаров (в таможенной сфере).

Результаты анализа состояния законности оформляются в виде справки, в которой указываются установленные и имеющие значение для анализа данные, выводы о состоянии законности, в том числе причины совершения правонарушений, предложения о способах их разрешения и устранения, а также имеющиеся проблемы и недостатки в законодательстве. В случае необходимости получения официальной позиции от субъекта анализа, справка направляется для ознакомления уполномоченному государственному органу либо организации, которые при наличии возражений предоставляют их письменно в течение трех рабочих дней со дня вручения справки. По результатам анализа состояния законности:

- принимаются меры прокурорского надзора либо реагирования;

- осуществляется информирование уполномоченных органов;

- материалы передаются в структурные подразделения, осуществляющие надзор за законностью уголовного преследования, в том числе для решения вопроса о необходимости регистрация документов и материалов об уголовном правонарушении в ЕРДР;

- материалы регистрируются в КУИ;

- в уполномоченные государственные органы направляются требования о проведении проверки;

- принимается решение о проведении прокурором проверки соблюдения законности;

- перед Генеральным Прокурором инициируется обращение в Конституционный и (или) Верховный суды;

- принимаются иные мер.

Указанные меры, за исключением решения о внесении актов прокурорского надзора и реагирования, могут быть приняты прокурором до завершения анализа и подведения его итогов в случаях, не требующих отлагательств.

Д.Б. Шабанов считает, что аналитическая работа, проводимая прокурорами, существенно влияет на состояние законности и играет

важнейшую роль при осуществлении надзорной деятельности. При этом главным критерием оценки деятельности прокуроров являются конкретные результаты в укреплении законности и правопорядка, которые невозможны без комплексного анализа имеющихся проблем [110].

Ю.О. Карпышева отмечает, что эффективному накоплению необходимых для анализа состояния законности будет способствовать получение и систематизация данных государственных органов о результатах их контрольно-надзорной деятельности [111].

В правовых актах и методических рекомендациях не закреплены порядок и основания проведения анализов состояния законности в сфере применения законодательства о персональных данных и их защите, что, учитывая текущую ситуацию с защищенностью персональных данных, видится не вполне обоснованным. Следует отметить, что отдельные анализы в этом направлении все же проводятся. Например, в 2023 году прокуратурой Балхашского района Алматинской области по результатам анализа деятельности коммунальных предприятий выявлены факты многочисленных нарушений законодательства о персональных данных и их защите [112].

При этом видится целесообразность проведения анализов состояния законности важных вопрос, связанных с защищенностью персональных данных.

Таким образом, анализ состояния законности является важным правовым инструментом по защите персональных данных.

Исходя из положений, предусмотренных статьей 21 Конституционного закона «О прокуратуре», а также вышеназванных Правил, оценка актов, вступивших в силу, осуществляется:

- в ходе анализов, проверок, рассмотрения обращений;

- по поручениям Президента Республики Казахстан, Генерального Прокурора, заместителя Генерального Прокурора, руководителя самостоятельного структурного подразделения Генеральной прокуратуры, органов военной и транспортной прокуратуры, прокурора области и приравненного к нему прокурора, их заместителей, районного и приравненного к нему прокурора, их заместителей либо лиц, исполняющих их обязанности.

Осуществляется оценка нормативных правовых актов, правовых актов индивидуального применения, решений государственных органов, учреждений и иных организаций, а также вступивших в законную силу судебных актов по уголовным, гражданским, административным делам и делам об административных правонарушениях.

Органы прокуратуры проводят оценку актов, вступивших в силу, путем изучения: актов и решений Правительства Республики Казахстан, иных государственных, местных представительных и исполнительных органов, органов местного самоуправления, учреждений, субъектов квазигосударственного сектора, их должностных лиц, а также актов и решений иных организаций независимо от форм собственности, если данные акты и решения касаются лиц, которые в силу физиологических особенностей,

психических отклонений и иных обстоятельств не могут самостоятельно осуществлять защиту своих прав, несовершеннолетних лиц, а также неограниченного круга лиц либо носят публичный характер. Данные акты изучаются на предмет наличия компетенции и полномочий по их принятию, соответствия установленным законами требованиям, противоречий нормативным правовым актам, в том числе вышестоящих уровней, наличия государственной регистрации и опубликования в установленном законом порядке (при необходимости) и других вопросов.

Также осуществляется оценка приговоров, решений, постановлений и иных актов суда (судьи), а также уголовных, гражданских, административных дел и дел об административных правонарушениях. При этом их оценка осуществляется в порядке, предусмотренном уголовно-процессуальным, гражданским процессуальным законодательством, законодательством об административных правонарушениях и административном судопроизводстве.

Осуществляя оценку актов, вступивших в силу, прокурор вправе:

- истребовать и получать необходимые для проведения оценки информацию, материалы и документы, а также уголовные, гражданские, административные дела и дела об административных правонарушениях, исполнительные производства, доступ к ним, а также информационным системам и ресурсам правоохранительных и иных государственных органов и организаций.

- вызывать и получать пояснения от должностных, физических лиц и представителей юридических лиц по вопросам проводимой оценки;

- вносить акты прокурорского надзора и реагирования, а также реализовать иные полномочия, установленные Конституционным законом и иными законами Республики Казахстан.

По результатам оценки принимаются следующие решения:

1) о внесении актов прокурорского надзора и реагирования, информировании уполномоченных органов, передаче материалов в структурные подразделения, осуществляющие надзор за законностью уголовного преследования и принятии иных мер;

2) о проведении проверки или анализа;

3) о регистрации материалов в КУИ и принятии других мер, предусмотренных уголовным законодательством Республики Казахстан;

4) об инициировании перед Генеральным Прокурором вопроса об обращении в Конституционный и (или) Верховный суды Республики Казахстан.

Р.В. Пузиков определяет оценку актов, вступивших в законную силу, как принципиальное новшество в Республике Казахстан, а также отмечает эффективность права прокурора по приостановлению исполнения опротестованного акта, поскольку это позволяет достигать оперативности принятия мер. Вместе с тем автор указывает, что оценке подвергаются только вступившие в законную силу актов, а не их проекты, что, по мнению некоторых исследователей, сужает пределы правовых полномочий прокурора [113].

Следует отметить, что «Правилами назначения и проведения органами прокуратуры проверок соблюдения законности, анализа состояния законности, а также осуществления оценки актов, вступивших в силу», даны определения некоторым используемым в Конституционном законе «О прокуратуре» важным понятиям. В частности указывается, что «к лицам, которые в силу физиологических особенностей, психических отклонений и иных обстоятельств не могут самостоятельно осуществлять защиту прав, свобод и законных интересов, относятся: лица, с ограниченными возможностями, обусловленными отклонением от нормального функционирования организма; лица, находящиеся в трудной жизненной ситуации, а также находящиеся в специальных организациях, учреждениях, в том числе с особым режимом содержания, в специальных центрах адаптации, реабилитации, обучения и социальной реабилитации; лица, с психическими, поведенческими расстройствами (заболеваниями), к которым отнесена группа заболеваний согласно международной классификации болезней, характеризующихся нарушением психической деятельности; лица, признанные вступившим в законную силу решением суда недееспособными или ограниченно дееспособными; иные лица, не способные самостоятельно осуществлять защиту своих прав, свобод и законных интересов. Под несовершеннолетними лицами понимаются лица, не достигшие восемнадцатилетнего возраста (совершеннолетия), в том числе дети-сироты, дети, оставшиеся без попечения родителей, дети с ограниченными возможностями, дети, находящиеся в трудной жизненной ситуации, а также дети, находящиеся в специальных организациях образования, организациях образования с особым режимом содержания, центрах адаптации несовершеннолетних, учебно-воспитательных учреждениях с обеспечением особых условий воспитания, обучения и социальной реабилитации. Под неограниченным кругом лиц понимается индивидуально неопределенный круг лиц или множественность участников правоотношений, при которой невозможно либо затруднительно заранее определить их количественный состав. Под необратимыми последствиями для жизни, здоровья людей либо безопасности Республики Казахстан понимаются принятие правового акта либо совершение действия (бездействие), если они причинили либо могут причинить вред здоровью, жизни человека и гражданина, повлекли или могут повлечь угрозу национальной безопасности (общественной, военной, политической, экономической, информационной, экологической)».

В анализируемой сфере оценке подлежат нормативные правовые акты в сфере персональных данных и их защиты акты центральных государственных органов, правовые акты уполномоченного органа, акты операторов и собственников баз данных об утверждении перечней персональных данных, необходимых и достаточных для выполнения осуществляемых ими задач, а также определяющие политику в отношении сбора, обработки и защиты персональных данных и другие акты в данной сфере. К примеру, в настоящее время ряд правовых актов центральных государственных органов об утверждении перечней персональных данных, необходимых и достаточных для

выполнения осуществляемых задач, предусматривает сбор сведений относительно юридических лиц, тогда как персональные данные касаются только физических лиц, что требует оценки органами прокуратуры данных актов на предмет соблюдения закона.

По результатам проведения проверок, анализов, оценки актов, вступивших силу, необходимо применение правовых средств прокурора по восстановлению нарушений законности и правовых средств прокурора по привлечению к ответственности виновных лиц, а также использование иных полномочий органов прокуратуры, как, например, по координации и межведомственному взаимодействию. Поэтому по результатам проверок, анализов, оценки актов, вступивших силу, по вопросам применения законодательства о персональных данных и их защите целесообразно проведение заседаний координационных советов, коллегий, инициирование межведомственных мероприятий.

Ю.С. Телина отмечает необходимость, как осуществления прокурорского надзора на предмет соответствия действующих нормативных правовых актов требования Конституции и законодательства о персональных данных, так и подготовку и внесение в законодательные органы и органы, обладающие правом законодательной инициативы, предложений о совершенствовании законодательства о персональных данных [114].

Соглашаясь с этой позицией, полагаем в случаях выявления прокурорами в ходе проверок, анализов, оценки актов, вступивших силу, по вопросам применения законодательства о персональных данных и их защите несовершенства законодательства необходимым реализовывать полномочия прокурора об участии в нормотворческой деятельности путем внесения уполномоченным и иным государственным органам предложений о совершенствовании законодательства Республики Казахстан.

Таким образом, прокурорская проверка, анализ и оценка актов, вступивших в законную силу, являются основными правовыми инструментами прокурора в сфере защиты персональных данных.

Однако в правовых актах и методических рекомендациях органов прокуратуры не закреплены порядок и основания прокурорских проверок соблюдения законности, анализов состояния законности, а также оценки, актов вступивших в законную силу, в сфере применения законодательства о персональных данных и их защите, что, учитывая текущую ситуацию с защищенностью персональных данных, видится не вполне обоснованным.

Проверки соблюдения законности в сфере защиты персональных данных должны быть 2 видов: предметные, направленные на проверку соблюдения законности в сфере применения законодательства о персональных данных и их защите, а также тематические, то есть проводимое по иным вопросам, но с выключением в предмет проверки вопроса защиты персональных данных.

Предметные проверки могут проводиться:

1. В деятельности уполномоченного органа в сфере защиты персональных данных.

2. В деятельности государственных органов и их должностных лиц по вопросам соблюдения законодательства о персональных данных и их защите.

3. В деятельности местных исполнительных органов по вопросам реализации их компетенции.

4. В деятельности квазигосударственных организаций, государственных учреждений (школы, больницы и т.д.), коммунальных предприятий, других организаций.

5. В деятельности собственников и операторов баз, содержащих персональные данные.

6. В деятельности правоохранительных, специальных и иных государственных органов относительно законности получения пользователями сведений из СИО ПСО, ЕРДР и ЕРАП.

7. В иных случаях, в том числе по поручения Президента и Генерального Прокурора Республики Казахстан.

Тематические проверки с выключением в предмет проверки вопроса защиты персональных данных могут проводиться по всем отраслям и направлениям прокурорского надзора. При этом полагаем, что упор должен быть на неопределенный круг лиц, защиту прав уязвимых слоев, несовершеннолетних и лиц, которые не могут себя защитить.

Анализу состояния законности подлежат важные вопросы, связанные с защищенностью персональных данных.

Оценке подлежат нормативные правовые акты в сфере персональных данных и их защиты акты центральных государственных органов, правовые акты уполномоченного органа, акты операторов и собственников баз данных об утверждении перечней персональных данных, необходимых и достаточных для выполнения осуществляемых ими задач, а также определяющие политику в отношении сбора, обработки и защиты персональных данных и другие акты в данной сфере.

2.3 Особенности применения современных технологий в деятельности прокурора по защите персональных данных

В мировых рейтингах по цифровизации и развитию цифровизации Казахстан занимает высокие места, лидирует среди стран СНГ и Центральной Азии, обгоняет многие развитые страны. В рейтинге электронного участия граждан наше государство показывает сильнейшие показатели, поскольку доля пользователей интернета (от 6 до 74 лет) составляет более 92%.

Э.Б. Тлесова, Г.М. Аубакирова, Ф.М. Исатаева, С.В. Пашков, Р.К. Сарпеков, А.Е. Воробьев, Н.Ф. Сарсенбиева, В.В. Синкевич и многие другие ученные изучили вопросы цифровизации экономики, здравоохранения, образования, промышленности, земледелия, нефтедобычи, уголовного процесса, правового пространства Казахстана, а также и многие другие направления. По результатам исследований авторы в основном пришли к выводам, что цифровизация во всех сферах продолжится и имеет значительные перспективы [115-121]. Следует понимать, что массовая разнонаправленная

цифровизация предполагает сбор огромного количества данных, в том числе персонального характера, что, безусловно, повышает риски утечки или утраты информации с последующим ее использованием в противоправных целях.

Тенденции цифровизации не обошли стороной и правоохранительную сферу, в том числе деятельность органов прокуратуры. В соответствии с инициативой 4.6. «Цифровизация правоохранительных органов и судов» Стратегического плана Развития Казахстана до 2025 года при непосредственном участии органов прокуратуры уголовные, гражданские дела и дела об административных правонарушениях поэтапно переведены в электронный формат, создан механизм электронной подачи обращений, оплаты штрафов, в судопроизводство внедряются технологии искусственного интеллекта [122].

02.09.2024 года, выступая с Посланием народу Казахстана, Глава государства К.К. Токаев поставил задачу широкого внедрения в стране искусственного интеллекта и развития цифровых технологий. При этом технологии искусственного интеллекта уже начали активно внедряться в различные отрасли общественных отношений [123].

Однако возникает резонный вопрос относительно необходимости урегулирования и минимизации негативных последствий повсеместного применения искусственного интеллекта.

Ж.У. Тлембаева указывает, что «в условиях, когда развитие технологий искусственного интеллекта порождает вызовы и создает много рисков и неопределенностей, возникает настоятельная потребность в установлении глобальных стандартов регулирования искусственного интеллекта и использования его положений в качестве модели для формирования внутреннего законодательства государств» [124].

В этой связи нельзя не отметить одобренный 13.03.2024 года Европейским Парламентом Закон «Об искусственном интеллекте», который фактически является первым правовым актом в мире, регулирующим применение данной технологии. Сфера действия данного закона охватывает все виды искусственного интеллекта, запрещает его применение в некоторых случаях, обязывает маркировать файлы, сгенерированные нейросетями без участия демонстрируемого человека, а также предусматривает множество других нововведений. В полном объеме он начнет действовать только в 2026 году.

Безусловно, во многих правовых актах различных государств вопросы применения технологий искусственного интеллекта затрагивались, но все же изучение показывает, что вышеуказанный закон Европейского Парламента является основным правовым ориентиром.

Отдельные государства более активны в этом направлении. Например, в Англии в 2018 году принят закон, регулирующий вопросы эксплуатации беспилотных транспортных средств, а в Китае с 2023 года разработан ряд правовых актов относительно управления генеративным искусственным интеллектом. Отдельные нормы этих актов касаются обработки персональных

данных. Между тем, законодательство этих государств не содержит конкретных или полных положений по классифицированию и оцениванию услуг или технологий искусственного интеллекта.

Большая часть государств все же находится на начальном пути в области разработки законодательства о применении искусственного интеллекта. В Российской Федерации принята Стратегия развития искусственного интеллекта до 2030 года, в рамках которой будет разрабатываться законодательство. В Республике Казахстан в 2024 году утверждена Концепция развития искусственного интеллекта на 2024-2029 годы, а проекты Цифрового кодекса и Закона «Об искусственном интеллекте» уже разрабатываются.

Важность урегулирования данного вопроса крайне высока, поскольку возможности искусственного интеллекта расширяются и, по мнению некоторых ученых, могут быть использованы и для совершения тяжких преступлений. К примеру, Ю.В. Грачева и А.А. Арямов считают, что роботы с искусственным интеллектом могут совершать убийства и участвовать в террористических актах [125].

Н.О. Дулатбеков и С.Н. Бачурин по результатам изучения теоретических проблем в использовании искусственного интеллекта при построении новой трехзвенной модели судебной и правоохранительной деятельности сформулировали ряд выводов, в том числе, что «принципиально решить вопрос о базовом программном обеспечении, на котором будут строиться платформы для работы госорганов, бизнеса и т.д., исключающем несанкционированный доступ и хищение персональных данных» [126]. Между тем, ни в Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023-2029 годы, ни в Концепции развития искусственного интеллекта на 2024-2029 годы не ставятся задачи по разработке отечественного программного обеспечения для сбора, обработки и хранения персональных данных в Казахстане.

При таком высоком уровне цифровизации и внедрения цифровых технологий важным является надлежащий контроль со стороны государства, в том числе эффективный прокурорский надзор в сфере персональных данных и их защиты. Однако решение современных проблем невозможно без применения современных технологий.

В этом направлении органами прокуратуры Казахстана проводится активная работа по цифровизации и внедрению технологий искусственного интеллекта для решения задач, возложенных на прокуроров.

Следует отметить, что проекты органов прокуратуры по цифровизации уголовных, гражданских дела и дел об административных правонарушениях, а также другие проекты органов прокуратуры получили высокую оценку в обществе. К примеру, в 2020 году проект Генеральной прокуратуры «Единый реестр административных производств» завоевал премию «Digital Almaty Awards», как лучший информационный проект в государственном секторе.

Планомерная работа в данном направлении продолжается.

30.04.2024 года Генеральный Прокурора Республики Казахстан Б.Н. Асылов доложил Главе государства о запуске аналитической платформы в работе по возврату активов и розыску преступников. В свою очередь Президент К.К. Токаев поручил продолжить использование широкого спектра современных технологий по поиску и возврату незаконно выведенных за рубеж активов [127].

06.08.2024 года Б.Н. Асылов через социальные сети и СМИ сообщил, что органами прокуратуры разработана информационная система с элементами искусственного интеллекта по автоматическому распознаванию скрывающихся преступников, должников и пропавших без вести, которая в двух городах страны подключена к видеокамерам наблюдения. С помощью данной системы удалось выявить 53 лица, находившихся в розыске [128]. При этом внедрение в такую систему биометрических персональных данных о поведенческих особенностях человека, например, об особенностях походки, безусловно, способствовало бы повышению ее эффективности. Сбор образцов голоса преступников смог бы помочь в борьбе с интернет-мошенничеством. Таким образом, сбор биометрических сведений о поведенческих особенностях лиц имеет существенные перспективы для использования в противодействии преступности.

С.А. Гречаный считает, что «правильно подобранная и установленная система будет работать с высокой точностью и сможет значительно помочь с обеспечением безопасности на любом объекте, выполняя работу, не доступную человеку. Как мы понимаем, человек не может, например, рассмотреть в толпе сразу десятки, а то и сотни лиц и быстро сравнить их с имеющимися у него тысячами ориентировок. Системы распознавания лиц, как и интеллектуальные системы видеонаблюдения в целом, непрерывно развиваются и, вместе с этим, становятся все более доступными. Уже сейчас камеры с распознаванием лиц по цене приблизились к стандартным камерам среднего ценового сегмента. Поэтому уже сейчас любой пост охраны, аэропорт, вокзал или другое особо охраняемое место можно оснастить высокофункциональным оборудованием, практически не потратив лишних средств из бюджета» [129]. О.И. Лукьянчиков также считает, что «современные методы распознавания лиц, представленные различными обученными моделями, демонстрируют высокую точность в условиях воздействия внешних факторов, обеспечивая в то же время сравнительно высокую производительность» [130].

В.В. Яцуценко полагает, что «основная цель внедрения цифровых технологий в деятельность органов прокуратуры заключается в достижении более эффективных результатов в поддержании законности в стране, доступности населению и прозрачности ее работы. Цифровизация деятельности органов прокуратуры – сложный и многоэтапный процесс, но автоматизированные программы, электронный документооборот и искусственный интеллект помогут повысить качество и уровень работы правоохранительных органов, что будет способствовать повышению законности» [131].

Ю.О. Карпышева предлагает использовать возможности искусственного интеллекта для мониторинга, фильтрации и отбора интересующих прокурора публикаций средств массовой информации и сети Интернет в целях использования данной информации при проведении анализа состояния законности, а также последующего планирования работы органов прокуратуры и проведения проверок [132].

В действительности возможности искусственного интеллекта целесообразно использовать для надзорной деятельности прокурора.

Р.М. Махьянова предлагает в целях оптимизации деятельности прокуроров прокурорам-предметникам осуществлять накопление объективной информации о состоянии законности и составлять электронные карты накопители (ЭК) надзорных характеристик объекта надзора с включением в них сведений относительно каждого поднадзорного объекта. Систематический и комплексный анализ этих сведений будет являться основой для планирования надзорной деятельности, прогнозирования надзорных ситуаций. «Кроме обработки первичной информации о состоянии законности (имеющейся на поднадзорных объектах) (как, например, это осуществляется в настоящее время в органах прокуратуры) на ЭК рекомендуется хранить всю итоговую информацию по конкретному объекту надзора, включая результаты проверочной и предупредительной деятельности, а также оценки эффективности междуведомственного взаимодействия и каждого проверочного мероприятия в отдельности» [133].

Поддерживая эту идею в целом, следует отметить, что в настоящее время прокурорами при проведении проверок и анализов не всегда достаточное внимание уделяется результатам проверок, проведенных уполномоченными органами. Поэтому обобщение таких сведений с их последующей обработкой искусственным интеллектом могло бы способствовать более эффективному планированию проверок и анализов, правильному определению предметов и вопросов проверок, а также определению субъектов, относящихся к «зоне риска», то есть которые допускают многочисленные нарушений либо не проверялись уполномоченными органами. Мониторинг искусственным интеллектом источников информации с правильным определением критериев мог бы определять вопросы, по которым прокурором необходимо направление требований в адрес уполномоченных органов о проведении проверок, в том числе это касается и сферы защиты персональных данных.

Таким образом, органами прокуратуры Казахстана достаточно активно осуществляется внедрение и применение современных технологий в надзорной деятельности и масштабная работа в данном направлении будет продолжаться.

В контексте же применения современных технологий в деятельности прокурора по защите персональных данных следует отметить, что в настоящее время одной из основных задач является исключение человеческого фактора, а именно преднамеренного распространения персональных данных лицами, имеющими доступ к базам, содержащим персональные данные.

Для реализации этих функций прокурор наделен значительным арсеналом правовых средств и инструментов в виде проверок, анализов, оценки актов, вступивших в законную силу, права направления требований в уполномоченные органы для производства проверок и других. Важным является обеспечение неотвратимости наказания, привлечение к ответственности лиц, которые преднамеренно распространили персональные данных других лиц, использовали доступ к базам персональных данных в собственных целях или интересах третьих лиц. Однако, учитывая стремительный рост количества государственных и негосударственных баз данных, одними проверочными мероприятиями достижение указанных целей невозможно, в связи с чем необходимо применение современных технологий.

Как указывалось выше, органы прокуратуры являются оператором значительного количества информационных систем и баз данных, содержащих персональные данные. Следует отметить, что ранее имели место отдельные недоработки и несовершенства систем, в результате которых допускались факты необоснованного доступа и получение пользователями систем информации, в том числе и персональных данных.

Например, в 2014 году Генеральной прокуратурой Республики Казахстан сообщено о выявлении многочисленных нарушений, выразившихся в необоснованном направлении запросов по уголовным делам в СИО ПСО. В некоторых случаях по одному и тому же основанию было направлено по 20 тысяч и более запросов.

В 2023 году КПСиСУ проведена проверка в правоохранительных и государственных органах на предмет законности и обоснованности получения данных их СИО ПСО, по результатам которой выявлено более 330 тысяч фактов необоснованных запросов сведений. Всего по итогам проверки прокурорами в адрес органов внесено 72 акта надзора и 8 информационных писем, возбуждено 1 административное и 2 дисциплинарных производства, 125 лиц привлечены к дисциплинарной ответственности, 1 лицо к административной ответственности. 50 фактов зарегистрированы в КУИ, из них по 3 начаты досудебные расследования, 47 направлены в орган для привлечения к дисциплинарной ответственности [134].

В таких случаях зачастую практически нереально было установить всех виновных лиц, поскольку использовалась электронная цифровая подпись (далее – ЭЦП) одного сотрудника, а сведения получали многие другие.

Одной из причин этого являлось то, что согласно пункту 3 «Правил формирования, доступа, использования, хранения, защиты и уничтожения сведений из системы информационного обмена правоохранительных, специальных государственных и иных органов», утвержденных приказом Генерального Прокурора Республики Казахстан №21 от 13.01.2023 года, для получения доступа к СИО ПСО сотруднику правоохранительного органа достаточно было получить ЭЦП, направить заявку оператору системы и подписать согласие на условия использования. Вход в информационную систему посредством ЭЦП не гарантировал, что использовать ее ресурсы будет

именно данный сотрудник. Фиксировалось немало фактов, когда ЭЦП находилось у других сотрудников и лиц, в том числе ранее уволенных со службы и даже посторонних.

Однако, 04.07.2024 года в данные правила внесены изменения, согласно которым теперь для входа в СИО ПСО необходимо прохождение многофакторной аутентификации, включая проверку ЭЦП и биометрии пользователя (отпечатков пальцев либо Face ID), либо подтверждение личности через SMS-код, что направлено на решение имевшихся проблем [135].

Следует отметить, что вопросы надлежащего контроля доступа к базам данных являлись предметом многих исследований и по результатам предлагались различные решения, в том числе о чипировании лиц, имеющих доступ к базам персональных данных.

Чипирование сотрудников правоохранительных органов идея не новая. В 2004 году 160 сотрудников прокуратуры Мексики, в том числе Генеральный прокурор имплантировали микрочипы с целью повышения конфиденциальности и безопасности. Это позволило им получить уникальный идентификационный номер, который через радиочастотную идентификацию RFID предоставлял доступ к новому федеральному информационному центру по борьбе с преступностью и другим сведениям ограниченного характера. Кроме того, внедрение чипов позволяло использовать их для поиска и обнаружения пропавших сотрудников.

В Казахстане чипирование ответственных сотрудников могло быть способствовать снижению вероятных противоправных проявлений в отношении данных с ограниченным доступом и персональных данных. Также такая технология способна повысить контроль над доступом сотрудников к информационным системам правоохранительных органов, которые содержат значительный объем персональных и других важных сведений.

Еще одной категорией лиц, которая в силу возложенных обязанностей и наделенных полномочий, имеет доступ к различным базам данных, являются государственные служащие, лица и работники организаций, имеющих доступ к государственным базам персональных данных

В настоящее время численность государственных служащих в Республике Казахстан составляет свыше 90 тысяч человек, работников Государственной корпорации «Правительство для граждан» более 22 тысяч человек. Доступ к государственным базам также имеют нотариусы, частные судебные исполнители и другие лица.

Следующей категорией подлежащих чипированию должны рассматриваться работники организаций, являющихся собственником или оператором базы персональных данных, поскольку сбор и обработка персональных данных активно осуществляется субъектами бизнеса, которые зачастую не уделяют должного внимания защите персональных данных и безопасности своих баз данных.

Без применения современных технологий крайне проблематично обеспечить постоянный эффективный контроль за пользование

государственными базами данных по меньшей мере 200 тысяч сотрудников правоохранительных органов, государственных служащих и других лиц, поэтому чипирование перечисленных категорий лиц могло бы стать действенным механизмом по защите персональных данных.

В некоторых государствах вопрос чипирования уже рассматривался официально. К примеру, приказом Министерства промышленности и энергетики Российской Федерации №311 от 07.08.2007 года утверждена Стратегия развития электронной промышленности России на период до 2025 года, из которой следует, что рассматривался вопрос вживления россиянам «электронных устройств многофункционального назначения», то есть чипов.

В отдельных зарубежных государствах законодательно закреплены нормы, позволяющие чипирование людей и использование данных, полученных с помощью чипирования. В то же время в некоторых странах, как, например, в Швеции процедура чипирования законодательно не урегулирована, но широко применяется населением.

В зарубежных странах граждане нередко положительно оценивают преимущества чипирования, что влечет ежегодное увеличение количества желающих прибегнуть к данной процедуре. Позиция же казахстанского и российского общества в большой степени из-за многочисленных слухов и мифов в основном негативная, вопрос чипирования вызывает дебаты и научную полемику.

Использование возможностей чипов могло бы восполнить недостающие части компьютерно-технических и судебных экспертиз. В разное время метод Henssge, 3D-моделирование, BIM-технология, мультиспиральная компьютерная томография, искусственный интеллект и другие современные начали применять при производстве судебно-медицинских экспертиз, как что-то новое и революционное, а в настоящее время они достаточно часто применяются, в том числе в юридической практике в качестве источников доказательств при расследовании и рассмотрении уголовных дел.

В целом, для принятия решения по такому щепетильному вопросу требуется надлежащее научно-обоснованное медицинское и юридическое опровержение всех мифов чипирования, исследование и объяснение негативных и положительных сторон данной технологии, в том числе как одного из инструментов защиты персональных данных. Технология чипирования, безусловно, имеет плюсы в виде повышения защищенности личной информации, снижения фактов несанкционированного доступа к персональным данным и других факторов, но так же имеет и минусы [136].

В качестве одного из инструментов решения проблемы «человеческого фактора» А.М. Амировым и Е.Н. Бегалиевым предложено применение современных технологий и новых методов, одним из которых могло бы стать оснащение компьютерной мыши технологией RFID, которая даст возможность применения данного аксессуара только во взаимодействии датчика с чипом, содержащим и подтверждающим информацию о наличии у конкретного лица прав использования компьютера и доступа к базам данных.

02.02.2024 года получен патент на полезную модель – Компьютерная мышь со встроенным RFID – датчиком. Целью полезной модели является исключение фактов применения компьютеров, лицами, не имеющими права использования конкретного компьютера, а также фиксация времени, пользователя и других сведений при работе лица с компьютером, в том числе с документами ограниченного доступа, в базах данных и базах персональных данных (Приложение Г).

Эксплуатировать компьютерную мышь со встроенным RFID-датчиком предполагается для информационной безопасности, защиты персональных данных в деятельности в деятельности правоохранительных и специальных органов, государственных служащих, НАО «Правительство для граждан», других организаций и лиц (частные судебные исполнители, нотариусы и др.), имеющих доступ к государственным базам данных, частных организаций, являющихся владельцами баз данных, а также любыми другими лицами, желающими ограничить возможность использования их компьютеров посторонними.

Применение данной разработки будет способствовать снижению количества фактов необоснованного доступа лиц, не имеющих соответствующего права, к базам данных, базам персональных данных, поможет безошибочно определять лиц, которые в конкретное время использовали компьютер, входили в базу данных, базу персональных данных или работали с документами ограниченного характера. Кроме того, в качестве превентивного механизма такой девайс повысит защищенность персональных данных и в итоге может повлиять на уровень интернет-преступности.

Следует отметить, что применение данной технологии менее затратно по сравнению с другими биометрическими системами контроля доступа (дактилоскопические, радужная оболочка глаз и другие).

Наибольшую эффективность применение такой компьютерной мыши имело бы при оснащении компьютеров системами мониторинга периферийных портов, которые блокируют возможность подключения к ним сторонних устройств, то есть применение иной компьютерной мыши было бы невозможным, а для использования компьютерной мыши со встроенным RFID-датчиком необходима аутентификация с помощью чипа.

Еще одной современной технологией, которая в настоящее время активно применяется банками, разработчиками крупных приложений, мессенджерами, внедряется в различные программы, приложения и веб-сайты является система защиты контента и предотвращения несанкционированного копирования информации, которая предполагает невозможность фотографирования или скриншота экрана.

Для этого могут быть использованы различные методы бля блокировки клавиш, комбинации клавиш или действий, в результате которых создаются скриншоты экрана. Для предотвращения фотографирования экрана возможно наложение позволяющих отследить контент видимых или невидимых водяных

знаков, внедрение программного обеспечения, которое распознает захват изображения, заменяет его на черный экран или другое изображение.

Внедрение таких технологий органами прокуратуры в собственные информационные системы, а также инициирование их внедрения в государственные и негосударственные информационные системы и базы персональных данных способствовало бы повышению защищенности персональных данных. Также целесообразно применение технологий, которые используются для защиты интеллектуальной собственности.

В.Н. Пахомов, описывая проблемы в этой сфере, приводит пример работы электронных библиотек, где электронные книги доступны только для чтения, но невозможно их копирование, скачивание или распечатка [137]. Также и для информационных систем и баз персональных данных целесообразно внедрение технологий, при которых обработка персональных данных возможно только для целей ее сборки, но невозможно копирование и распечатка сведений, содержащих персональные данные, без соответствующего разрешения руководства либо фиксации данных действий в памяти информационных систем или баз данных.

А.В. Сырбу для повышения эффективности экспертиз считает, что «для единообразного оформления и способов изъятия компьютерной техники, а также в целях информирования следственного аппарата об объеме возможностей экспертов в сфере компьютерных технологий, полагаем необходимым формирование единого нормативного документа (инструкции) для правоохранительных органов» [138]. Соглашаясь с этим мнением, полагаем, что в таких правовых актах целесообразно указание возможностей технологии чипирования.

Помимо исключения человеческого фактора, еще одной важной задачей для прокуроров можно определить исключение фактов совершения преступлений с использованием персональных данных, в первую очередь интернет-мошенничества, для чего также возможно применение современных технологий.

Существенным элементом противодействия преступлениям, совершенным с использованием IT-сервисов, является пресечение пропуска телефонных звонков с подменных номеров и из иностранной юрисдикции. К примеру, законодательство Российской Федерации предусматривает право операторов связи прекратить оказание услуг связи в случае, если инициированное в сети связи иностранного оператора связи соединение, в том числе для передачи текстового сообщения, сопровождается нумерацией, соответствующей российской системе и плану нумерации, но у оператора связи отсутствует информация об абонентском номере или уникальном коде идентификации абонента, инициировавшего это соединение [139].

А.В. Сычева сообщает, что крупнейший российский оператор связи «М.» ежедневно блокирует около 500 тысяч звонков с подменных номеров, при этом рост мошенничества связан также и с простотой использования широкого диапазона номеров [140]. По сведениям К.О. Карабекова в Казахстане тоже

проводится подобная работа, Министерством внутренних дел реализуется проект «Киберпол», что позволило пресечь более 43 миллионов звонков с подменных номеров, используемых мошенниками [141]. 05.08.2024 года Национальный банк Казахстана запусти Центр по обмену данными о мошеннических транзакциях (Антифрод-центр), работа которого заключается в противодействии мошенническим транзакциям, оперативном реагировании на операции с признаками мошенничества, обмен информацией. За непродолжительное время работы центра удалось выявить около 400 инцидентов и заблокировать порядка 30 миллионов тенге, связанных с мошенническими действиями [142].

Прокуратура тоже участвует в этой работе. К примеру, в августе 2024 года при координации прокуратуры г.Астаны пресечена деятельность группы мошенников, которые используя устройства для подмены абонентских номеров и изменения географической локации, осуществляли более 10 тысяч телефонных звонков с подменных номеров в сутки.

Между тем, необходимо отметить, что законодательство Казахстана не возлагает задачи по блокированию звонков с подменных номеров на операторов связи. Кроме того, в Казахстане остается актуальной проблема широкого доступа и отсутствия достаточного контроля за оборотом мобильных телефонных номеров, которые в настоящее реализуются не только через операторов сотовой связи, но и практически повсеместно. При этом операторы связи регистрируют устройства связи с помощью онлайн-сервисов без подтверждения личности, что дает возможность регистрации номера с помощью данных любого человека, в том числе не имеющего никакого отношения к регистрируемому устройству.

Решение данной проблемы предполагается путем внесения в «Правила оказания услуг связи», утвержденные приказом исполняющего обязанности Министра по инвестициям и развитию Республики Казахстан от 24.02.2015 года №171, изменений, предполагающих оказание услуг связи на основании договора между оператором и абонентом с предоставлением абонентов биометрических данных (изображения лица) [143]. Проект изменений в данные Правила находится на стадии обсуждения.

Вместе с тем координационными мерами или мерами межведомственного взаимодействия прокурор имеет возможность использования полученных сведений об осуществлённых подменных звонках для оповещения населения и предотвращения интернет-мошенничеств.

В частности, многие крупные компании, как, например, «Яндекс» внедряют сервисы автоопределителей звонков, которые предупреждают владельца телефона о подозрительном звонке. Такие же механизмы целесообразно внедрять и в Казахстане с использованием сведений, получаемых правоохранительными органами, операторами связи, банками, а также другими заинтересованными организациями и лицами.

Во избежание деятельности мошеннических колл-центров в местах лишения свободы целесообразно использовать опыт Российской Федерации,

где с 2019 года в местах содержания осужденных лиц осуществляется радиомониторинг, что только в 2020 году позволило выявить более 27 тысяч абонентских номеров, используемых заключенными. В 2021 году принят закон, обязывающий операторов связи блокировать такие номера.

Также следует обратить внимание на функционирование различных сервисов, которые по номеру телефона показывают, как его владелец записан у других лиц. С помощью таких программ мошенники могут узнать личные сведения, достаточные для использования в специальных манипулятивных приемах и техниках мошенничества. К примеру, мошенник с помощью таких приложений может узнать имя, фамилию, место жительства, место работы, имена близких родственников и другие сведения, после чего в разговоре апеллирует этими данными, что оказывает манипулятивное воздействие на жертву, получаемая информация кажется аргументируемой и правильной, а приводимые личные сведения заставляют поверить словам мошенника.

Кроме того, органам прокуратуры в рамках взаимодействия с другим государственными органами, в том числе в рамках работы системы «Кибернадзор» следует обеспечить мониторинг сети Интернет, направленный на выявление сайтов-зеркал, то есть сайтов, маскирующихся под официальные ресурсы государственных органов, социальных сетей и различных маркетплейсов, поскольку целью таких сайтов является похищение персональных данных и другие противоправные действия в отношении граждан.

Еще одной современной технологией органов прокуратуры по защите персональных данных могло бы стать получение постоянного доступа к государственному и негосударственным сервисам контроля доступа к персональным данным, что дало бы возможность осуществления надзора и оценки законности действий по сбору и обработке персональных данных граждан. То есть, получив доступ к этим сервисам, прокурор будет видеть давал ли субъект персональных данных согласие на те или иные действия с его персональными данными, которые осуществляет оператор базы данных, прекратил ли оператор обработку персональных данных после отзыва согласия субъекта, а также прокурору будет доступна другая важная информация.

Таким образом, органы прокуратуры Казахстана достаточно активно используют в работе современные технологии, их применение для осуществления надзора в сфере защиты персональных данных имеет значительные перспективы, в особенности для исключения «человеческого фактора» при использовании информационных систем и баз персональных данных, противодействия телефонным звонкам с подменных номеров, выявления и пресечения деятельности приложений и сайтов, целью которых является незаконный сбор или похищение персональных данных.

Выводы по разделу

1. Методика и тактика прокурорского надзора в сфере защиты персональных данных на сегодня не разработаны и не внедрены. При этом

изучение исследований, законодательства, практической деятельности показывают, что органы прокуратуры Казахстана обладают достаточно широким арсеналом правовых средств прокурорского надзора в сфере защиты персональных данных.

2. Основными правовыми инструментами прокурора в сфере защиты персональных данных, безусловно, являются проверка соблюдения законности, анализ состояния законности, а также оценка актов, вступивших в силу. Вместе с тем следует отметить важность и других правовых средств прокурорского надзора в сфере защиты персональных данных, а также целесообразность их применения для повышения эффективности защиты прав граждан.

3. Органами прокуратуры Казахстана в условиях необходимости противодействия современным вызовам и угрозам, решения иных возложенных задач, проводится активная работа по цифровизации и применению новейших технологий. Проекты прокуратуры по цифровизации получили высокие оценки в обществе и в настоящее время активно используются в работе, как прокуратуры, так и других правоохранительных и иных государственных органов. Применение современных технологий в деятельности прокуратуры для защиты персональных данных имеет существенные перспективы, в особенности для исключения «человеческого фактора» при использовании баз персональных данных.

3 ПУТИ СОВЕРШЕНСТВОВАНИЯ ПРОКУРОРСКОГО НАДЗОРА В СФЕРЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Анализ целесообразности и возможности имплементации в Республике Казахстан передового опыта защиты персональных данных

В большинстве источников первым упоминанием относительно юридической защиты персональной информации считается, опубликованная в 1890 году в Гарвардском юридическом журнале статья Луиса Д. Брандейса и Самюеля Уоррена под названием «Право на приватность». В ней авторы выделяют «право быть оставленным в покое» или «право быть предоставленным самому себе», а также утверждают, что новые изобретения и методы ведения бизнеса подвергают личную приватность опасности. По мнению авторов, вторжение в частную жизнь является тяжким преступлением, требующим эффективных средств защиты, в связи чем они предложили выделение специального «права приватности» [144].

Между тем, официальное законодательное закрепление права на приватность, недопустимость вмешательства в частную жизнь получило несколько позже.

10.12.1948 года резолюцией 217 А (III) Генеральной Ассамблеи ООН принята Всеобщая декларация прав человека, в статье 12 которой указано, что личная и семейная жизнь не может подвергаться произвольному вмешательству и каждый человек обладает правом защиты от такого вмешательства или посягательства [145].

В дальнейшем право каждого на уважение личной и семейной жизни закреплено в Европейской конвенции о защите прав и основных свобод в 1950 году [146], а в 1966 году в Международном пакте о гражданских и политических правах [147]. При этом Международный пакт о гражданских и политических правах запрещает не только произвольное, но и незаконное вмешательство и посягательство на личную и семейную жизнь.

Таким образом, право на неприкосновенность частной жизни встало в один ряд с основными «классическими» правами человека, что повлекло за собой попытки правового регламентирования, как вопросов неприкосновенности частной жизни, так и защиты персональной информации.

Следует отметить, что Республика Казахстан, вступив в ООН, приняла на себя обязательства по выполнению норм Всеобщей декларации прав человека, а в 2005 году ратифицировала Международный Пакт о гражданских и политических правах. Таким образом, в нашем государстве должны создаваться все условия для соблюдения норм указанных правовых актов, в том числе в части неприкосновенности частной жизни и защиты персональной информации.

В целом, в большинстве государств мира законодательное регулирование вопросов защиты персональных данных в основном связано с существенно возраставшей компьютеризацией общества, последовавшим после этого

массированным сбором и обобщением данных граждан и организаций, а также возникшими рисками утраты этих сведений.

Европейские государства первыми отметились в разработке законодательства, связанного с защитой данных. На начальном этапе европейское законодательство содержало лишь нормы об автоматизированной обработке данных. В 1970 году в Германии, а затем и в других европейских государствах были приняты национальные законы, касающиеся защиты данных (Франция, Швеция) [148]. В 1974 году в США был принят Закон о неприкосновенности частной жизни, согласно которому граждане данного государства получили право на доступ и корректировку своих персональных данных, а также право на получение информации об использовании их данных. Однако, все эти законодательные акты не связывали право на защиту данных с какими-либо основополагающими правами человека и гражданина [149].

Впервые право на защиту данных в качестве конституционного положения закреплено в Австрии в 1978 году [150]. Таким же путем пошли Венгрия, Словакия, Чехия, Норвегия и другие европейские государства. К примеру, пункт 3 статьи 19 Конституции Словакии и пункт 3 статьи 10 Конституции Чехии наделяют каждого гражданина указанных государств правом на защиту от необоснованного сбора или опубликования данных о своей личности либо иного злоупотребления ими. При этом следует отметить, что этими государствами отдельно признается право каждого на защиту от необоснованного вмешательства в частную и семейную жизнь (пункт 2 статьи 19 Конституции Словакии и пункт 2 статьи 10 Конституции Чехии). В статье 59 Конституции Венгерской Республики указано, что каждый обладает право на доброе имя, неприкосновенность жилища, а также правом на защиту личной тайны и персональных сведений. При этом отмечено, что для принятия закона о защите персональных сведений необходимо голосование двух третей присутствующих депутатов Государственного собрания [151, 152].

В 80-е годы массовая компьютеризация общества продолжилась, изобретен Интернет, в связи с чем, вопросы защиты данных не оставались без повышенного внимания. Так, правовые акты о защите данных приняты в Нидерландах, Англии, Канаде, Финляндии, Японии и других.

Первым международным документом по защите данных стала принятая Советом Европы в 1981 году Конвенция о защите физических лиц при автоматической обработке персональных данных [47], которой урегулированы вопросы автоматизированной обработки данных. Следует отметить, что в последующем, помимо большинства европейских государств, к данной Конвенции присоединились и многие неевропейские государства, такие как Мексика, Тунис, Аргентина и другие.

В 90-е годы широкое применение получили персональные компьютеры, запущены первые веб-сайты, достигнуты серьезные прорывы в сфере информатизации, что способствовало продолжению нормативного регулирования вопросов защиты данных.

Европейский Парламент совместно с Советом Европейского Союза, в 1995 году разработали и приняли совместную директиву. Она касалась защиты и свободного обращения персональных данных физических лиц. В последующем в эту Директиву включены разработанные ОЭСР рекомендации в виде 7-ми ключевых принципов по защите данных [153].

В 2000 году права на уважение частной и семейной жизни, а также на защиту персональных данных были включены в Хартию Европейского Союза об основных правах [154].

В 2016 году Советом Европейского Союза и Европейским парламентом принят Генеральный регламент о защите персональных данных (General Data Protection Regulation, далее - GDPR) [155]. Этот регламент предусматривает порядок защиты прав и свобод физических лиц при обработке персональных данных, а также определяет правила свободного обращения персональных данных.

Исходя из вышеизложенного, можно сделать вывод, что в Европе более 40 лет назад введен новый отдельный от неприкосновенности частной жизни институт защиты персональных данных. Ученые по-разному относятся к вопросу соотношения понятий «неприкосновенность частной жизни» и «защита персональных данных».

М.А. Важорова описывает три подхода ученых к этому вопросу. Согласно первому подходу (Э.А. Цадыкова, Н.И. Петрыкина) понятие «частная жизнь» является общим и более широким, а «персональные данные» частным и более узким. Представители этого подхода считаю, что персональные данные представляют собой информацию, дающую возможность идентифицировать личность. В соответствии со вторым подходом (Е.В. Климович, Д.М. Ветров) понятие «персональные данные» более широкое, а сведения о частной жизни являются их составной частью. В обоснование приводится аргумент, что информация о частной жизни составляет сведения, связанные с неофициальным и неформальным межличностным общением. Третьий подход (С.Г. Пилипенко, С.А. Федосин) основывается на том, что рассматриваемые понятия не являются идентичными, одно не охватывает другое, их содержание пересекается лишь в некоторых случаях, но одинаковыми по объему они не являются. Информация о частной жизни может персонализировать личность и являться частью персональных данных, но в то же время существует значительное число персональных данных, которые не содержат сведений о частной жизни [156].

Полагаем, что каждый из перечисленных трех подходов имеет как свои веские аргументы, так основания для критики. При этом следует признать, что вопрос соотношения понятий «неприкосновенность частной жизни» и «защита персональных данных» до настоящего времени остается достаточно сложным и дискуссионным. Законодателями и ученными многих государств единый подход к данному вопросу не определен. Безусловно, данные понятия в определенной степени можно назвать смежными и они зачастую применяются во взаимодействии друг с другом. В то же время нарушение неприкосновенности частной жизни не всегда связано с распространением

персональных данных, а разглашение персональных данных не всегда затрагивает частную жизнь. Нельзя не отметить и тот факт, что зачастую вмешательство в частную жизнь связано с нарушением неприкосновенности жилища, что в свою очередь никаким образом не касается персональных данных. Полагаем, что споры касательно соотношения указанных понятий будут продолжаться еще долгие годы и не исключено, что единый подход в итоге выработан не будет. При этом уже сейчас понятно, что значимость, важность и необходимость защиты, как частной жизни, так и персональных данных, крайне высоки.

Т.Д. Оганесян отмечает, что европейские ученые нередко обсуждают целесообразность отделения права на защиту персональных данных от права неприкосновенности частной жизни. Учитывается, что защита персональных данных закреплена в качестве основополагающего права, как и право на уважение частной жизни в Хартии Европейского Союза об основных правах, то есть данные права рассматриваются отдельно. Ряд европейских ученых считают, что защита данных является частью неприкосновенности частной жизни. Существует и другое мнение, что становление отдельного права на защиту данных уже произошло. Право на уважение частной жизни изначально являлось лишь негативным обязательством по недопущению необоснованного вмешательства в частную жизнь. Право на защиту данных разработано в прецедентной практике европейских судов в большей степени как позитивное обязательство государств, обязывающие их принимать меры по защите данных. В этом заключается отличие между данными правами. В целом, Т.Д. Оганесян приходит к выводу, что «право на защиту персональных данных нельзя в полной мере признавать в качестве полноценного и самостоятельного права. Оно уже прошло стадию зарождения и закрепления на международном уровне, но пока еще не может обладать необходимыми элементами, присущими только ему, которые позволили бы полностью отделиться от права на уважение частной жизни. Для того, чтобы соответствующее право на защиту данных стало полностью «дееспособным», нужно также, чтобы оно было сбалансировано настолько, чтобы не было необходимости обращаться к элементам права на уважение частной жизни. Будущее права на защиту данных во многом зависит от ЕСПЧ и Суда ЕС, которым принадлежит доминирующая роль в толковании данного права, обогащении его новыми элементами и последующем влиянии на развитие прецедентной практики и законодательства в государствах – членах Совета Европы и ЕС» [157].

Полагаем целесообразным в целом согласиться с данным мнением. При этом необходимо отметить, что в Республике Казахстан также имели место попытки разделения данных прав.

Так, статьей 32 Конституции Республики Казахстан от 28.01.1993 года были закреплены нормы относительно неприкосновенности частной жизни гражданина, запрета вмешательства в нее. Вместе с тем в этой же статье Конституции было указано, что без согласия граждан только в установленных

законом случаях допускается сбор, хранение, использование и распространение информации личного характера [22].

В новой Конституции, а именно в статье 18 Конституции Республики Казахстан от 30.08.1995 года сохранилось право на неприкосновенность частной жизни, но были исключены положения касательно запрета вмешательства в нее, а также относительно использования информации личного характера с согласия граждан (таблица 3) [23].

Таблица 3 – Нормы относительно неприкосновенности частной жизни в конституциях Республики Казахстан

Конституция Республики Казахстан (1993 года)	Конституция Республики Казахстан (1995 года)
Статья 33. Частная жизнь гражданина неприкосновенна	Статья 18
Запрещается вмешательство в частную жизнь гражданина, а также посягательство на его честь и достоинство. *Сбор, хранение, использование и распространение информации личного характера без согласия гражданина допускаются только в случаях и в порядке, прямо установленных законом*	*Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства*

Полагаем, что в данном случае законодатель под информацией личного характера понимал, в том числе и персональные данные. Таким образом, можно сделать вывод, что в Республике Казахстан права на неприкосновенность частной жизни и защиту персональных данных законодательно разделялись, а право на защиту персональных данных хоть и непродолжительный срок являлось конституционным правом граждан. Указанные обстоятельства свидетельствуют о том, что законодательный подход к соотношению понятий «неприкосновенность частной жизни» и «защита персональных данных» в Республике Казахстан менялся. В настоящее время, учитывая рост значимости персональных данных и многочисленность совершаемых с их использованием различных правонарушений, в ближайшей перспективе не исключается рассмотрение вопроса повышения статуса права на защиту персональных данных и выделении его в качестве отдельного конституционного права.

При таком высоком уровне цифровизации общества, наличии серьезных проблем, связанных с персональными данными особую значимость обретает надлежащее законодательное урегулирование, направленное на защиту от необоснованного и незаконного вмешательства частной жизни и персональных данных.

В 1990-х годах насчитывалось около 20 стран, которые законодательно урегулировали вопросы сбора и обработки персональных данных. При этом согласно отчету ООН относительно электронного правительства по состоянию на 2022 год законы о конфиденциальности данных были приняты уже в 145 странах [158]. О.Д. Исмагилова и К.Р. Хаджи выделяют 3 подхода к

регулированию защиты данных на национальном уровне: 1 подход - принятие отдельного закона о защите персональных данных. Такая практика характерна для стран Европейского союза, где действует GDPR, но ряд вопросов регулируется каждым государством самостоятельно. Также и для других государств, где приняты отдельные законы о защите персональных, например, Россия, Азербайджан, Армения, Израиль, Казахстан, Кыргызстан, Малайзия, Мексика, Молдавия, Сингапур, Турция, Узбекистан, Украина, Южная Корея и Япония. 2 подход - включение положений о защите персональных данных в соответствующие секторальные законы, но без принятия отдельного закона о защите персональных данных. Такого пути придерживаются Вьетнам, Индонезия, Иран, Нигерия и Чили. 3 подход - комплексный, что предполагает принятие отдельного закона о защите персональных данных, а также внесение соответствующий изменений в секторальные законы. Такой подход избрали Австралия и Канада. Помимо закона о защите данных, вопросы передачи финансовых, медицинских и других видов данных регулируется отдельными правовыми актами [159].

Среди них следует отметить особенности правил использования персональных данных в отдельных странах, которые нередко воспринимаются, как достаточно кардинальные.

К примеру, в 2018 году Бразилия с целью обеспечения безопасности и целостности информации, принадлежащей владельцу данных, законодательно закрепила набор правил и принципов для сбора и обработки персональных данных. Новым законом создана основа для защиты персональных данных и регулирования их обработки в стране. Закон предусматривает обязательное соблюдение мер безопасности, направленных на защиту прав и интересов владельцев данных. К ним относятся строгие требования к организациям, осуществляющим сбор и обработку персональных данных, а также наличие санкций за нарушение правил. Закон обеспечивает повышенную защиту персональных данных в Бразилии и создает рамки ответственного и безопасного использования информации в цифровой среде.

Общий закон о защите данных был принят в Бразилии 18.09.2020 года. Граждане стали владельцами своих персональных данных и обладателями права на эту информацию. У них появилась возможность требовать прозрачности сбора, хранения и использования данных. Введено обязательство об информировании относительно реальных случаев утечки персональных данных. Целью законодательных нововведений в Бразилии является подчеркивание важности принципов защиты персональных данных, интересов интернет-пользователей и наличия преимуществ для всего бразильского общества [160].

Некоторые из проблем, выявленных при реализации Закона о защите данных в Бразилии, связаны с необходимостью правовых корректировок и соответствующего обучения, разработки полного плана действий для компаний по соблюдению данного правового акта, специализированного внедрения процессов управления персональными данными, применения технологий

защиты информации, информирования бразильского общества об этом законе, а также демонстрации прав и обязанностей граждан. Поэтому, по мнению Дж. Соуза, Дж. Абэ, Л. Лима, и Н. Соуза предстоит множество дебатов и обсуждений относительно закона и ее соответствия GDPR, а также вопросов, связанных с применением действующего законодательства в Бразилии [161].

О. Озкан, М. Шахинол, А. Айдыноглу и Ю. Сон отмечают, что новый турецкий закон о защите персональных данных вызывает различные проблемы, вызванные широким сбором разнообразной информации. При этом даже в отношении конфиденциальной информации игнорируется важность согласия субъекта данных. В законе нет ограничений на сбор данных, поэтому все виды данных могут быть собраны, осуществляется сбор и данных о сексуальной жизни [162].

Некоторые государства проявляют большую снисходительность, предоставляя компаниям и ассоциациям более значительную степень саморегулирования, как, например, в случае с США. Однако стоит отметить, что позднее США вынуждены были ужесточить некоторые аспекты своего регулирования [163].

Учитывая важность практики Европейского суда по правам человека (далее - ЕСПЧ), а также ее влияние на формирование требований к защите персональных данных, следует более детально остановиться на данном вопросе.

ЕСПЧ разработаны критерии правомерного ограничения прав на защиту персональных данных, которые соответствуют общим принципам законного вмешательства в частную жизнь. Они включают в себя требования о необходимости соответствия закону и легитимности целей вмешательства.

В практике ЕСПЧ понятие «согласно закону» трактуется и как требование соответствия мер основаниям в законе, и как требование к качеству этого закона. Таким образом, закон должен быть доступен лицам, использующим персональные данные, а последствия его применения должны быть предсказуемыми. Доступность закона предполагает, что нормативно-правовой акт должен быть обнародован, а предсказуемость, что норма должна быть ясной и дающей лицу возможность при необходимости регулировать свое поведение [164].

В случае, если действия с персональными данными отвечают насущным общественным потребностям и являются пропорциональными преследуемой законной цели, то они считаются легитимными, а вмешательство необходимым в демократическом обществе. Например, интересы национальной безопасности могут считаться превалирующими над частными интересами субъекта персональных данных [165].

Критерии и ограничения, определенные практикой ЕСПЧ, должны соблюдаться для правомерной обработки персональных данных и защиты прав и свобод граждан.

Понятие «персональные данные» в практике ЕСПЧ включает в себя не только информацию о «частной жизни». При этом публичная информация

рассматривается как «частная жизнь», если она систематически собирается и хранится в государственных базах данных [166].

ЕСПЧ устанавливает широкий спектр персональных данных, охватывающий следующие виды: данные, собираемые в официальных переписях населения, включающие информацию о поле, семейном положении, месте рождения, этнической принадлежности и другие личные сведения; снятие отпечатков пальцев, фотографий, образцов клеток, ДНК-профилей и другой личной или публичной информации, даже если соблюдаются условия конфиденциальности; сбор и хранение медицинских данных и других медицинских записей; прослушивание, запись и хранение телефонных разговоров; системы идентификации личности, разработанные для административных и гражданских целей, такие как базы данных в сфере здравоохранения, социальной помощи и налоговых органов; видеозаписи, сделанные системами видеонаблюдения на улице; системы перехвата разговоров между заключенными и их родственниками в комнатах для свиданий в учреждениях исполнения наказания и др.

Таким образом, ЕСПЧ устанавливает широкий спектр персональных данных, на которые распространяются его решения и примеры, что иллюстрирует разнообразие ситуаций, в которых происходит обработка персональных данных. Это помогает определить границы и защиту прав субъектов данных в соответствии с национальным законодательством.

Среди выделенных в практике ЕСПЧ прав субъекта персональных данных можно отметить:

1. Право на доступ к своим персональным данным, которое включает обязанность государства не вмешиваться произвольно в частную жизнь, ограничивая возможность лица получить доступ к информации о себе, которая собирается, хранится, используется и передается государственными органами. Это право вытекает из положительных обязанностей государства обеспечить уважение к частной жизни путем установления механизмов доступа к персональным данным. Право на доступ должно быть эффективным, то есть не только обеспечивать возможность ознакомления с персональными данными и составления собственных письменных выписок, но и предоставлять возможность получения копий документов с персональными данными. Кроме того, это право должно быть реализовано в разумные сроки. Ограничения права на доступ к персональным данным могут быть установлены в интересах государства, например, для защиты национальной безопасности, а также в частных интересах, например, для защиты конфиденциальной информации третьих лиц.

2. Обеспечение защиты персональных данных предполагает положительную обязанность государства по обеспечению уважения к частной жизни путем введения системы правил и гарантий, направленных на защиту данных. Это включает практический и эффективный механизм защиты, который исключает возможность несанкционированного доступа к персональным данным.

3. Право на изменение или уничтожение своих персональных данных является одним из прав. Согласно судебной практике отказ в предоставлении возможности опровергнуть неправильные персональные данные является нарушением права на уважение частной жизни. Кроме того, положительная обязанность государства в обеспечении уважения частной жизни включает создание процедур, позволяющих вносить изменения в персональные данные, включая информацию об этническом происхождении.

4. Право на забвение, которое предусматривает, что длительное хранение персональных данных без достаточных оснований может составлять несоразмерное вмешательство в право на уважение частной жизни.

В Испании действует Закон «О защите персональных данных и гарантиях цифровых прав», в котором предусматривает наличие алгоритмов в социальных сетях (и публичных ресурсах), позволяющих исправить и удалить опубликованную информацию, а также право на забвение в поисковых системах и социальных сетях. Кроме того, в законе имеется целая глава посвящена гарантиям цифровых прав, в том числе в сфере труда в виде запрета использования видеонаблюдения и звукозаписи на рабочем месте, использования систем геолокации при исполнении трудовых обязательств. Еще одной особенностью данного закона Испании является норма, предусматривающая цифровое завещание, то есть процедуру передачи в случае смерти человека его аккаунтов наследникам.

ЕСПЧ при обнаружении нарушения Европейской Конвенции о защите прав человека может применить различные меры для защиты прав субъекта персональных данных. Ниже перечислены некоторые из этих мер:

1. Присуждение справедливой сатисфакции потерпевшей стороне, которая включает компенсацию как морального, так и имущественного вреда. Компенсация морального вреда может быть выражена в денежной форме, либо можно признать, что само признание нарушения Конвенции и его последствий является достаточной формой справедливой сатисфакции.

2. Восстановление предыдущего юридического состояния, которое субъект персональных данных имел до нарушения Конвенции, насколько это возможно.

3. Применение других мер, предусмотренных в решении ЕСПЧ, которые могут быть направлены на обеспечение эффективной защиты прав субъекта персональных данных.

Таким образом, практика ЕСПЧ сформулировала критерии, определяющие правомерное ограничение прав на персональные данные, в соответствии с общими принципами правомерного вмешательства в частную жизнь. Согласно этим критериям вмешательство должно соответствовать закону. Это означает, что меры, предпринятые для ограничения прав на персональные данные, должны иметь законное основание и быть предусмотренными соответствующими нормативно-правовыми актами.

При осуществлении вмешательства необходимо иметь легитимную цель. То есть, такое вмешательство должно быть обоснованным и направленным на

достижение законных целей, таких как защита национальной безопасности, поддержание общественного порядка, предотвращение преступности и прочее. Вмешательство должно быть необходимым в рамках демократического общества. Это означает, что ограничения, касающиеся персональных данных, должны быть пропорциональными и необходимыми для достижения легитимной цели, а также соответствовать принципам демократического общества.

Право на персональные данные получает свою защиту в соответствии с практикой ЕСПЧ в рамках права на личную жизнь. Понятие персональных данных включает любую информацию, относящуюся к конкретному лицу или лицу, которое может быть определено. Субъект персональных данных обладает рядом прав, включая право на доступ, изменение, уничтожение и защиту своих персональных данных. Однако эти права могут быть ограничены для достижения легитимной цели, при условии, что такое ограничение соответствует закону и является необходимым в рамках демократического общества [167].

В последние годы проводились многочисленные исследования касательно защиты персональных личных данных, результатом которых являются значимые теоретические выводы.

Д. Мангку, Н. Юлиартини, И. Суастика, И. Вираван отмечено, что важность защиты персональных данных повышается учетом роста числа пользователей мобильных телефонов и Интернета, что требует наличие конкретного и всеобъемлющего законодательства, регулирующего эту сферу [168].

Исследование Н. Фибрианти, А. Холиш показало, отсутствие конкретных и всеобъемлющих норм, обеспечивающих юридическую защиту персональных данных потребителей, создает правовой вакуум в отношении защиты персональных данных именно потребителей [169].

Следует согласиться с данным мнением, а также отметить, что в законодательстве Казахстана также отсутствуют нормы, определяющие порядок сбора и обработки персональных данных потребителей. При этом, к примеру, статья 15 Федерального закона Российской Федерации «О персональных данных» определяет права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также обязывает операторов немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных в таких целях. Во Франции в дополнение к GDPR действует Закон «Об обработке данных, файлах и свободах», который предоставляет любому субъекту персональных данных право зарегистрироваться в специальном регистре Bloctel, что предполагает его отказ на 3 года от рекламных звонков и писем. Такой отказ в дальнейшем может продлеваться еще на 3 года.

По мнению Г. Татару и С. Татару, правила, установленные GDPR, требуют от операторов ответственности, прозрачности и уважения прав человека, а также напоминают им о недопустимости рассмотрения людей,

человеческих ресурсов, а также данных исключительно в качестве объектов для эксплуатации [170].

В исследовании, проведенном Б. Миттельштадт, отмечаются, что пользователи внедряемых в настоящее время систем всеобщего сбора конфиденциальных персональных данных не полностью осознают потенциальные последствия нарушения конфиденциальности и интеллектуального анализа данных [171].

По мнению В. Юстицкис, в защите персональных данных значительную роль играет принцип балансировки, который широко применяется европейскими судами для разрешения споров, возникающих при применении права на защиту данных. Этот принцип также выступает основой гармонизации европейского и национального законодательства, а также для применяется для установления надлежащего соотношения интересов Европейского Союза и признающих его решения государств [172]. Балансировка играет решающую роль в повседневной практике защиты данных. GDPR предусматривает, что балансировка должна быть основным средством регулирования отношений между правом на защиту данных и другими правами.

К. Лабади и К. Легнер высказывают точку зрения о том, что правила защиты данных предоставляют физическим лицам набор прав, направленный на обеспечение прозрачности обработки данных и четкое определение объема действий по обработке данных. Это означает, что организации обязаны выполнять определенные требования. Для этого используются концепция жизненного цикла процесса и бизнес-правила, чтобы показать, как эти требования влияют на методы управления данными [173].

Таким образом, исследователи приходят к выводам, что для обеспечения эффективной защиты данных и соблюдения принципов приватности необходим осознанный подход к защите персональных данных, учет балансировки интересов, а также создание прозрачных правил. При этом нельзя не учитывать возможные негативные последствиях излишней регулировки и ограничений, которые могут возникнуть при разработке слишком строгого законодательства в этой области. Поиск баланса между защитой данных и развитием инноваций является непростой задачей, требующей дальнейшего детального изучения и обсуждения с участием специалистов во многих областях.

З. Сунь и З. Лю приходят к выводу, что защита конфиденциальной личной информации должна быть усилена и классифицирована. Законы о защите личной информации должны использоваться в качестве ориентира, а в уголовно-правовом аспекте должны быть конкретно указаны акты, объекты, объем и критерии уголовного преследования нарушений, связанных с чувствительной личной информацией [174].

GDPR разработан с целью создания консолидированной основы для регулирования коммерческого использования персональных данных, усиления защиты данных для граждан ЕС и направлен на стандартизацию и модернизацию законодательства о защите данных, связанных с Интернетом, социальными сетями и цифровым рынком, а также на обеспечение и

расширение прав граждан ЕС в отношении конфиденциальности их данных. Р. Карвальо, К. Прете, Й. Мартин, Р. Риверо, М. Онен, Ф. Скьяво, А. Румин. Х. Муратидис, Дж. Йельмо, М. Куковини отмечают, что передача контроля над персональными данными физическим лицам в ЕС с предоставлением новых прав субъектам данных ЕС оказывает влияние на то, как организации работают с личной информацией. И именно GDPR изменил методы сбора и управления личной информацией, включая определение новых ролей в организациях, работающих с данными [175].

В. Обригаву считает, что GDPR значительно повлиял на политику безопасности данных во всем мире, а также существенно повысил осведомленность и контроль граждан над их персональными данными и. Повышение стандартов защиты данных способствовало пересмотру крупнейшими технологических корпорациями подходов к работе с персональными данными, заставило их уделять большее внимание конфиденциальности. При этом для эффективной реализации GDPR необходимо активнее использовать инструменты, предусмотренные GDPR [176].

М. Графенштейн, Т. Якоби, Г. Стивенс отмечают, что концепция повышения эффективности законодательства о защите данных путем внедрения правовых норм в техническую и организационную структуру обработки данных существует уже давно. Вопросы о защите данных и конфиденциальности обсуждаются уже много лет. Однако лишь недавно произошел сдвиг в сторону включения защиты данных в рамках закона, но полные последствия такого подхода еще не вполне изучены. Согласно статье 25 GDPR субъекты регулирования обязаны не только внедрить правовые нормы в структуру обработки данных, но и сделать это эффективным образом. Законодатель путем прямого требования эффективности мер защиты как обязательного результата непременно ставит вопрос о методах проверки и обеспечения эффективности. Фактически, распространение оценки соответствия законодательству на реальные последствия требуемых мер открывает возможность использования (неюридических) методологий, специализирующихся на эмпирической оценке мер защиты данных [177].

С. Куанч, П. Тайчон, К. Мартин, С. Уивен и Р. Паламтье подчеркивают необходимость исследований угроз конфиденциальности, возникающих в результате применения новых цифровых технологий, включая искусственный интеллект. В рамках исследований следует затрагивать вопросы восприятия потребителями стратегий использования данных, существующую практику обеспечения конфиденциальности данных и уровень регулирования, что в итоге может способствовать созданию долгосрочных, основанных на технологиях результатов для всех заинтересованных сторон [178].

Р. Дукато указывает, что научные исследования являются одной из областей, в которые государства-члены могут вмешиваться с конкретными положениями для улучшения защиты персональных данных, как на уровне ЕС, так и на национальном уровне [179].

З. Матвеева считает, что внедрение новой правовой базы для защиты персональных данных в ЕС обновило принципы путем введения новых требований к прозрачности, доступу и удалению, а также отчетности, что способствует повышению уровня защиты в различных сферах современного общества [180]. В этом контексте точное соблюдение принципов защиты персональных данных является ключевым элементом обеспечения защиты личных прав. Более того, их должное соблюдение прекратит практику безоговорочного сбора и использования таких данных и создаст условия для качественной обработки персональных данных.

М. Соколова отмечает, что GPDR задал новый вектор развития цифрового общества и стал эффективным инструментом для защиты данных, европейские регуляторы начали жестко подходить к вопросам соблюдения законодательства и фактам утечки персональных данных, привлекая виновных лиц к значительным штрафам, размеры которых доходят до 2 миллионов долларов или 4% от годового оборота компании. Только за первые 2 года действия GDPR было возбуждено около 206 тысяч дел о нарушении безопасности персональных данных, по которым общая суммы взысканий превысила 56 млн. долларов США. При этом в 2018 году во всем мире компании за нарушение законодательства о персональных данных были оштрафованы на 320 млн. долларов США, а в 2019 году суммы штрафов были еще больше [181]. Для сравнения в Казахстане по статье 79 Кодекса об административных правонарушениях, то есть за нарушения законодательства Республики Казахстан о персональных данных и их защите, для субъектов крупного предпринимательства предусмотрено максимальное взыскание в виде штрафа в размере 1000 месячных расчетных показателей, а по статье 641 за нарушение законодательства об информатизации в размере 200 месячных расчетных показателей, что, безусловно, не является ощутимой для них санкцией. К примеру, в 2024 году по сведениям уполномоченного органа по защите персональных данных за нарушения информационной безопасности, повлекшие утечку персональных данных казахстанцев, крупные компании «Air Astana» и «Казахтелеком» привлечены к административной ответственности с наложение штрафа в размере 100 месячных расчетных показателей. В этой связи в качестве положительного международного опыта следует рассмотреть вопрос об увеличении санкций по фактам утечек персональных данных, но важен баланс и объективная оценка возможностей компаний, поскольку в Европе высокие штрафы стали причиной закрытия многих компаний. Также следует продумать дифференцированный подход, то есть санкции для компаний, которые принимают значительные меры по информационной безопасности и защите персональных данных должны быть в разы ниже, чем для тех, кто пренебрегает такими требованиями.

Исследования ученых подтверждают значимость проблемы защиты персональных данных и необходимость разработки соответствующего законодательства для обеспечения юридической защиты и учета прав и интересов пользователей и потребителей. В то же время, нужно понимать, что

слишком строгое и подробное законодательство в области защиты персональных данных может негативно сказаться на развитии инноваций и цифровой экономики. Излишняя регулировка может ограничить свободу действий компаний и ограничить доступ к данным, что в свою очередь может препятствовать разработке новых технологий и прогрессу. Также обеспечение полной защиты персональных данных может быть практически невозможным в связи с быстро меняющейся технологической средой и постоянно возникающими новыми угрозами. Кроме того, индивидуальная ответственность пользователей в области безопасности данных также играет важную роль и не должна полностью перекладываться на государственные органы и законодательство.

Для повышения уровня безопасности необходимо, чтобы не только те, кто непосредственно имеет полномочия на контроль персональных данных, но и все участники процессов защиты данных хорошо знали принципы и могли эффективно их применять. Их глубокое понимание необходимо не только для оценки нарушений в обработке данных, но и для определения факта нарушения прав физического лица. Принципы защиты персональных данных устанавливают рамки применения законодательной базы, регулируя сбор и обработку персональных данных, а также служат основой для разрешения споров между конкурирующими правами. Они могут помочь избежать ограничений в передаче персональных данных через границы между государствами-членами ЕС с различными стандартами и снизить риск злоупотребления личными данными непосредственно в Республике Казахстан.

Международное законодательство предусматривает значимые превентивные меры в рамках регулятивных отношений для предотвращения нарушений прав субъектов персональных данных в будущем. В связи с широким сбором и увеличивающейся угрозой безопасности персональных данных в некоторых странах принимаются законы, предоставляющие контрольные функции определенным лицам в отношении сбора, обработки и передачи персональных данных государственным и частным организациям.

М. Бисалиевым и К. Шакировой исследованы основные подходы к использованию знаний о цифровых следах в Интернете как важном факторе обеспечения безопасного обращения с персональными данными в киберсреде. В статье представлено авторское определение цифровых следов и предложен алгоритм для выявления способов нарушения безопасности персональных данных с использованием глобальной информационной сети. Также показаны типичные фазы таких нарушений и распространенные действия правонарушителей. В результате исследования были сделаны предложения о принятии международного или регионального (европейского) акта, который бы устанавливал стандарты для использования специализированных знаний при обнаружении незаконного доступа к персональным данным, включая их перехват в рамках информационного обмена в Интернете [182].

При изучении зарубежного опыта нельзя не отметить подход к учету собственников и операторов баз, содержащих персональные данные.

А.Н. Прокопенко указывает, что в Российской Федерации ведется реестр операторов персональных данных. При этом ранее предусматривались исключения для компаний, которые ведут учет своих работников, и которые ведут сбор персональных данных клиентов для заключения договоров, а также в ряде других случаев. 01.09.2022 года такие положения из законодательства были исключены и в настоящее время действуют единые требования для всех операторов персональных данных. В целом, это привело к улучшению ситуации с соблюдением законодательства о персональных данных, но в то же время обнажило проблему нехватки специалистов в сфере информационной защиты [183]. По сведениям Роскомнадзора количество зарегистрированных операторов персональных данных превысило 397 тысяч. В Республике Казахстан в настоящее не известно даже приблизительное число операторов баз, содержащих персональные данные.

С.К. Жетписов и Г.А. Алибаева изучили вопросы защиты персональных данных в Казахстане в эпоху глобализации, по результатам чего внесли ряд предложений, одно из которых утверждения перечня субъектов, осуществляющих хранение персональных данных, поскольку в настоящее время не известно какие организации и в каком объеме хранят такую информацию [42].

Еще одним интересным зарубежным опытом является предоставление и обмен медицинскими и специальными персональными данными между лицами, планирующим вступить в брак. К примеру, статья 30 Семейного кодекса Украины обязывает жениха и невесту сообщить друг другу о состоянии своего здоровья, а сокрытие сведений, важных для здоровья будущих потомков, может повлечь признание брака недействительным [184]. Во Франции, Узбекистане и ряде штатов США предусмотрено обязательное медицинское обследование будущих супругов и информирование о физиологических, психических заболеваниях, отклонениях сексуальной жизни и прочих сведениях, препятствующих ведению семейной жизни [185].

Республика Казахстан относится к числу мировых лидеров по количеству расторжений браков, причинами которых чаще всего являются алкоголизм, наркомания, бытовое насилие, лудомания, а также около 20% браков распадаются по причине невозможности зачатия и рождения детей. Социальные опросы показывают, что нередко браки расторгаются по причине нетрадиционной сексуальной ориентации одного из супругов [186, 187].

Статья 12 Кодекса Республики Казахстан «О браке (супружестве) и семье» предусматривает добровольное медицинское обследование лиц, вступающих в брак (супружество), а его результаты могут быть представлены предполагаемому супругу только с согласия обследованного лица. Исключением являются случаи, когда имеется заболевание, способное создать угрозу для здоровья другого лица, вступающего в брак (супружество) [188].

Расторжению брака также может способствовать скрытая от будущего супруга информация о наличии судимости, предыдущих браков, детей, гражданстве, просроченной задолженности, имеющихся обязательствах, в том

числе по алиментам, а также обман о реальном возрасте, наличии имущества, жилья и пр. Нельзя не учитывать и особенности традиций страны, особенно в части запрета и крайне негативного отношения к бракам между родственниками и лицами, близкими по родоплеменным признакам.

Поэтому видится целесообразным обязательное проведение медицинского обследования лиц, вступающих в брак (супружество), а также обмен ими важными персональными данными.

Для этой цели предлагается внедрить Паспорт персональных данных, который будет содержать сведения о наличии/отсутствии судимости, ВИЧ-статусе, врожденных и приобретенных заболеваниях, способных повлиять на потомство, наличии предыдущих браков, детей и обязательств перед ними, непогашенной задолженности, образовании, наличии недвижимого имущества, долей в юридических лицах и др. В дальнейшем не исключается использование, в том числе в усеченном виде данного Паспорта в иных целях, к примеру, для изучения кандидатов при трудоустройстве на работу. При этом возможна интеграция паспортов персональных данных с государственной и негосударственными системами контроля доступа к персональным данным, что даст субъекту персональных данных в каждом случае использования его Паспорта персональных данных определять перечень сведений, который он готов предоставить тому или иному лицу.

Помимо указанного следует отметить, что международное законодательство предусматривает обязательное создание отдельного независимого надзорного органа, обеспечивающего защиту прав граждан в сфере сбора и обработки персональных данных. Такие органы созданы во многих государствах мира, в том числе в соседних с Казахстаном странах.

К примеру, уполномоченными являются самостоятельные органы в Российской Федерации – Роскомнадзор, в Кыргызской Республике - Государственное агентство по защите персональных данных при Кабинете Министров, в Республике Таджикистан - Служба связи при Правительстве, в Республике Узбекистан - Государственный центр персонализации при кабинете министров, в Республике Беларусь - Национальный центр по защите персональных данных, а в Республике Армения - Агентство по защите персональных данных Министерства юстиции.

В Республике Казахстан уполномоченным органом в сфере защиты персональных данных определено Управление по защите персональных данных, являющееся структурным подразделением Комитета информационной безопасности, который в свою очередь входит в состав Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан.

Исследование Б. Максутова посвящено вопросам создания уполномоченного органа по защите персональных данных в Республике Казахстан. В этом исследовании представлена правовая структура такого органа, его миссия, цели, задачи и принципы деятельности. Также представлены практические рекомендации, основанные на мировой и кейсовой

практике Европейского суда по правам человека, относительно учреждения органа по защите персональных данных. Автор исследования предлагает внедрить отдельный правовой механизм для обеспечения права на защиту персональных данных путем создания Органа по защите персональных данных [189].

Л.К. Каирбаева считает в Казахстане необходимым «учреждение Национального агентства по защите персональных данных – специализированного органа, который будет осуществлять государственный контроль в области сбор и обработки персональных данных в соответствии с передовой зарубежной практикой» [190].

Следует отметить, что в некоторых странах на уполномоченные органы по защите персональных данных возлагаю и другие права и обязанности.

А.Н. Халиков отмечает, что наличие современных технических возможностей, изощренные способы совершения преступлений, например, в виртуальном пространстве диктуют необходимость пересмотра старых подходов к производству привычных следственных действий, приводящихся в гласном порядке. В ряде стран, в том числе в Казахстане создан уголовно-процессуальный институт негласных следственных действий, поскольку невозможно только открытыми следственными действиями бороться с преступностью. Институт негласных следственных действий в Казахстане имеет постоянную тенденцию к совершенствованию в целях активного противодействия преступлениям. Широкий спектр негласных следственных действий предусмотрен в Грузии. В Эстонии и Молдове такие действия названы оперативно-розыскными или розыскными действия, а в России институт негласных следственных действий законодательно закреплять не стали. Примечательным является опыт проведения негласных следственных действий в Грузии, где санкцию на их проведение выдает судья, а в безотлагательных случаях прокурор. При этом контроль и надзор за производством тайных следственных действий осуществляется Службой защиты персональных данных [191].

Относительно опыта работы органов прокуратуры следует отметить, что в системе прокуратуры Молдовы действую Антикоррупционная прокуратура и Прокуратура по борьбе с организованной преступностью и особым делам. В специализированных прокуратурах работаю на постоянной основе офицеры уголовного преследования, розыскные офицеры и специалисты, функционально подчиненные главному прокурору специализированной прокуратуры. Данные должностные лица в индивидуальном порядке отбираются и откомандировываются в специализированные прокуратуры из других учреждений на срок до пяти лет, который может быть продлен на такой же срок. Откомандирование осуществляется приказом Генерального прокурора с согласия руководителя учреждения, в котором работает командируемое лицо. Оплата труда осуществляется из бюджета прокуратуры в соответствии со специальным законодательством [70, с. 102-105].

Схожий механизм целесообразно было бы предусмотреть в Казахстане для работы органов прокуратуры по обеспечению надзора в сфере защиты персональных данных, информационной безопасности, искусственного интеллекта, поскольку для достижения эффективных результатов требуется наличие значительной квалификации и знаний в области информационных технологий, которыми прокуроры зачастую не обладают.

Таким образом, зарубежными государствами проводится значительная работа по разработке законодательства в сфере защиты персональных данных. Кроме того, сформировать требования по защите персональных данных, а также права субъектов персональных данных позволила практика ЕСПЧ. В качестве передового опыта зарубежных стран в контексте его возможной имплементации в Казахстане можно выделить опыт Франции по внедрению системы, позволяющей отказаться от рекламных звонков и писем, опыт Испании, где за гражданами закреплено право исправления и удаления опубликованной о нем информации, а также право на забвение в поисковых системах и социальных сетях, опыт европейских и других государств, в том числе при применении GDPR по наложению на компании крупных штрафов за утечки персональных данных, а также опыт Российской Федерации в части обработки персональных данных граждан в целях продвижения товаров, работ, услуг на рынке и по учету операторов персональных данных. Отдельно следует отметить положительный опыт функционирования во многих государствах отдельных специальных органов по защите персональных данных, целесообразность образования которого имеет место и в Республике Казахстан.

В целях снижения количества разводов, причинами которых являлось сокрытие или незнание информации о наличии заболеваний или иных факторов, препятствующих семейной жизни, видится целесообразным внедрение обязательного проведения медицинского обследования лиц, вступающих в брак (супружество), а также обмен ими важными персональными данными с внедрением для этих целей Паспорта персональных данных, который будет содержать сведения о наличии/отсутствии судимости, ВИЧ-статусе, врожденных и приобретенных заболеваниях, способных повлиять на потомство, наличии предыдущих браков, детей и обязательств перед ними, непогашенной задолженности, образовании, наличии недвижимого имущества, долей в юридических лицах и др. Для этих целей необходима доработка законодательства о браке (супружестве) и семье.

3.2 Рекомендации по комплексному совершенствованию прокурорского надзора в сфере персональных данных и их защите

Как указывалось выше, проверки соблюдения законности в сфере защиты персональных данных должны быть 2 видов: предметные, направленные на проверку соблюдения законности в сфере применения законодательства о персональных данных и их защите, а также тематические, то есть проводимое по иным вопросам, но с выключением в предмет проверки вопроса защиты персональных данных.

Предметные проверки могут проводиться:

1. В деятельности уполномоченного органа в сфере защиты персональных данных по вопросам реализации государственной политики и государственного контроля в сфере персональных данных и их защиты, организации деятельности консультативного совета по вопросам персональных данных и их защиты, а также реализации иных полномочий, предусмотренных законодательством.

2. В деятельности государственных органов и их должностных лиц по вопросам соблюдения законодательства о персональных данных и их защите. Такие проверки в большей степени будут иметь отраслевой характер, то проводиться, например, в сфере законности исполнительного производства, государственной правовой статистики, исполнения уголовных наказаний и применения иных мер государственного принуждения, по линии оперативно-розыскной и контрразведывательной деятельности и т.д. При этом особую роль, безусловно, будут иметь проверки законности оперативно-розыскной и контрразведывательной деятельности.

С.И. Захарцев и Н.О. Кирюшина указывают, что оперативно-розыскная деятельность подразумевает ограничение конституционных прав человека и вторжение в его личную жизнь. Поэтому при организации и осуществлении надзора за оперативно-розыскной деятельностью прокуроры помимо прочих направлений должны уделять внимание на соблюдение прав человека и гражданина на неприкосновенность частной жизни, личную и семейную тайну, защиту чести и доброго имени. Также указывается, что «осуществляя надзор за законностью проведения оперативно-розыскных мероприятий, прокурор должен обращать внимание на соответствие мероприятий целям и задачам ОРД, законность и обоснованность решений об их проведении или прекращении. Как показывают материалы уголовных дел в отношении сотрудников органов внутренних дел имеются, увы, случаи проведения мероприятий не для решения указанных задач, а в личных целях. Так, встречаются факты наблюдения за женами и любовницами, прослушивания телефонных переговоров бизнесменов по «заказу» их конкурентов, сбора компрометирующей информации в интересах частных лиц, иные вопиющие нарушения закона». Проверки в данной сфере, по мнению названных ученых, должны проводиться по обращениям, по результатам изучения уголовных дел о нераскрытых преступлениях, в плановом порядке, по поручениям вышестоящих прокуроров и по другим основаниям [192].

3. В деятельности местных исполнительных органов по вопросам реализации их компетенции, в том числе по осуществлению государственного контроля за соблюдением законодательства о персональных данных и их защите в отношении субъектов частного предпринимательства.

4. В деятельности квазигосударственных организаций, государственных учреждений (школы, больницы и т.д.), коммунальных предприятий, других организаций, в деятельности которых осуществляется сбор и обработка большого количества персональных данных по вопросам соблюдения

законодательства, в том числе в части сохранности и конфиденциальности персональных данных, недопущения их сбора в излишнем количестве.

5. В деятельности собственников и операторов баз, содержащих персональные данные, в части соблюдения предусмотренных Законом «О персональных данных и их защиты», иными законодательными актами обязательств и недопущения нарушений прав субъектов персональных данных, а также относительно надлежащей деятельности лиц, ответственных за организацию обработки персональных данных.

6. В деятельности правоохранительных, специальных и иных государственных органов относительно законности получения пользователями сведений из СИО ПСО и Единого реестра административных производств.

Следует отметить, что имеется множество проблем и нередки случаи доступа к персональным данных посторонних лиц.

К примеру, 22.12.2020 года в г. Нур-Султан осуждены 5 бывших и действующих сотрудников полиции, которые за вознаграждение предоставили третьим лицам право пользования базами Министерства внутренних дел и Генеральной прокуратуры, содержащим персональные данные [193]. 30.08.2024 года на крупном информационном портале «100baksoff» с аудиторией около 2 миллионов человек опубликована информация, что сотрудники дорожной полиции и участковые инспекторы полиции используют доступ к информационным системам в своих целях, как, например, в описанных случаях для знакомства с противоположным полом, то есть, используя ставшие известными в процессе работы данные, с помощью информационных систем устанавливают абонентские номера и другие сведения заинтересовавших их лиц. Не исключено, что таким же методом персональные данные каких-либо лиц могут передаваться третьим лицам, не имеющим права доступа к таким сведениям.

Э.Т. Халиуллина отмечает, что «судебно-следственной практике известны многочисленные случаи, когда сотрудниками правоохранительных органов систематически используется, вопреки интересам службы, доступ в различные базы данных МВД России, в том числе в ГИБДД, для получения персональных данных с последующем размещением на различных ресурсах в сети Интернет объявлений о предоставлении за денежное вознаграждение неопределенному кругу заинтересованных лиц, полученных персональных данных.» [194].

7. В иных случаях, в том числе по поручениям Президента и Генерального Прокурора Республики Казахстан.

Тематические проверки с выключением в предмет проверки вопроса защиты персональных данных могут проводится по всем отраслям и направлениям прокурорского надзора. При этом полагаем, что упор должен быть на неопределенный круг лиц, защиту прав уязвимых слоев, несовершеннолетних и лиц, которые не могут себя защитить.

В научно-практическом пособии Университета прокуратуры Российской Федерации к наиболее часто встречающимся нарушениям, допускаемым медицинскими организациями, отнесено нарушение прав граждан на охрану

здоровья и медицинскую помощь, в том числе несоблюдение врачебной тайны. Также приведены примеры внесения без ведома граждан их персональных данных в учетные документы медицинских учреждения для последующего получения денежных средств за якобы полученные ими медицинские услуги. При этом в пособии указывается, что «нарушения прав граждан на охрану здоровья и медицинскую помощь органами прокуратуры и органами государственного контроля (надзор) выявляются в деятельности медицинских организаций всех категорий, в том числе в амбулаторно-поликлинических учреждениях, больницах и иных учреждениях, оказывающих стационарную медицинскую помощь населению, на станциях скорой медицинской помощи, в лечебно-профилактических организациях» [195].

Е.А. Иванченко проведено обобщение и анализ надзорной практики органов прокуратуры, что позволило выделить типичные нарушения в сфере обращения лекарственных средств, в число которых вошла «ненадлежащая организация органами государственной власти обеспечения граждан необходимыми лекарственными средствами, в том числе далеко не единичные факты необоснованного отказа лечебными учреждениями гражданам, относящимся к категориям льготников, в выписке лекарственных средств, которые они должны получать на безвозмездной основе в силу прямого указания закона» [196].

В Казахстане отмечается значительный уклон в сторону цифрового здравоохранения, внедрен электронный паспорт здоровья, что предполагает структурирование персональных медицинских данных о состоянии здоровья физического лица и оказываемой ему медицинской помощи на протяжении всей жизни, ведется сбор большого количества персональных медицинских данных и сведений, относящихся к тайне медицинского работника.

Указанные обстоятельства, наряду с предоставлениям права доступа к персональным медицинским данным большому количеству организаций, в том числе поставщикам медицинских и фармацевтических услуг, организации, ответственной за финансовое возмещение затрат на оказание медицинской помощи, уполномоченным органам в сфере здравоохранения и в области социальной защиты населения и другим, значительно увеличивает риски утечки личной медицинской информации.

Медицинские персональные данные, в особенности лиц, которые не могут себя защитить самостоятельно, нередко используются для совершения противоправных действий. Так, в г.Алматы на протяжении 10 лет устойчивая преступная группа, имеющая в составе работников Центра психологического здоровья, используя доступ к данным пациентов, определяла одиноких людей с психическими расстройствами, у которых имелась в собственности недвижимость. В дальнейшем эти люди похищались и содержались в неволе, а некоторые были убиты. Их собственность незаконно отбиралась и реализовывалась. В настоящее время проходит судебный процесс в отношении 22 обвиняемых лиц [197].

Поэтому при проверках соблюдения законодательства о здравоохранении целесообразно включать в предмет проверки защиту персональных медицинских данных пациентов. Внимание следует обращать и на работу информационных систем в сфере медицины. Например, пользователи приложения «Damumed» зачастую указывают о наличии записей о получении медицинских услуг, которые фактически не оказывались. Также допускается ошибочное указание наличия психических, неврологических и других расстройств. Не исключены факты использования персональных данных граждан для фиктивного указания и повышения объема оказанных медицинских услуг для последующего получения оплаты.

А.М. Нурмагамбетов отмечает, что IT-специалисты, которые обслуживают медицинские информационные системы имеют прямой доступ к персональным медицинским данным, но на них не распространяется тайна медицинского работника, что не исключает возможности освобождения их от ответственности [198]. Н.В. Унижаев считает, что «не все пользователи информационной системы персональных данных должны иметь одинаковые права, но еще не менее важным при моделировании учитывать так называемый «эффект Сноудена», когда главная утечка происходит от системного администратора, в функционал которого входит организация безопасности» [199].

Вопрос защищенности персональных данных следует включать в проверки трудового законодательства.

Р. Ахамбаевым и Ж. Ахметовой рассмотрены основные принципы обеспечения безопасности личных данных пользователей в организации. В этой статье особое внимание уделено рекомендациям по защите персональных данных, которые являются активами организации. Исходя из проведенных исследований, акцентируется на важности оптимизации масштаба угроз, даже без необходимости проведения аудита и применения методов управления рисками [200].

Ф. Сырлыбаевой рассмотрены положения о защите информационных прав работников в Казахстане и в некоторых зарубежных странах. В результате исследования выявлены пробелы в правовом регулировании защиты информационных прав, а также сделаны определенные выводы в области защиты трудовой информации работников [201].

В соответствии с требованием Трудового кодекса работник имеет право на обеспечение защиты персональных данных, хранящихся у работодателя, а работодатель обязан осуществлять сбор, обработку и защиту персональных данных работника в соответствии с законодательством о персональных данных и их защите.

Между тем, на практике зачастую требования не соблюдаются, персональные данные работников предоставляются третьим лицам, работодатели требуют от работников непредусмотренные законодательством персональные сведения, в том числе о наличии или отсутствии судимости и другие. В государственных учреждениях выявляются многочисленные факты

фиктивной оплаты трудовой деятельности «мертвых душ» путем использования персональных данных лиц, которые не имеют никакого отношения к данной организации.

Антикоррупционной службой установлена устойчивая организованная преступная группа, которая с января 2020 года по март 2023 года на системной основе занималась хищением бюджетных средств путем перечисления заработной платы физическим лицам, фактически не работавшим в сфере образования, а также на свои личные счета. В результате преступных действий государству причинен ущерб в размере 4,3 миллиарда тенге.

В Туркестанской области органами прокуратуры выявлена преступная, которая путем манипуляций с персональными данными похитила более 4 миллиардов бюджетных средств. В частности, работниками числились одни лица, но для перечисления заработной платы были указаны реквизиты других лиц.

Таким образом, по проверкам в сфере труда возможно выявление многочисленных нарушений прав работников по защите персональных данных, в связи с чем целесообразно в предмет комплексных проверок включать и этот вопрос.

Серьезные нарушения защищенности персональных данных могут выявляться при проверках защиты прав несовершеннолетних.

По проверкам усыновления детей-сирот следует отметить, что в соответствии с пунктом 4 статьи 84 Кодекса «О браке (супружестве) и семье» дети, являющиеся гражданами Республики Казахстан, состоящие на централизованном учете в Республиканском банке данных, могут быть переданы на усыновление иностранцам только в случаях, если ребенок не может быть усыновлен родственниками, гражданами Республики Казахстан, проживающими на территории страны и за ее пределами.

По сведениям из отдельных источников, должностные лица интернатных учреждений зачастую приписывают здоровым детям серьезные заболевания, отягощённую наследственность (якобы родители алкоголики, наркоманы, психбольные и т.д.), что отпугивает потенциальных усыновителей из числа родственников и граждан Казахстана.

После отказа в усыновлении ребенка казахстанцами, они передаются на усыновление иностранцам. Однако, при повторном обследовании детей за рубежом каких-либо заболеваний не выявляют.

Поэтому в целях исключения возможных коррупционных проявлений (подарков, денежных вознаграждений от иностранных граждан), со стороны должностных лиц, за одобрение усыновления казахстанских детей, полагаем целесообразным введение практики перепроверки персональных медицинских данных и обоснованности диагнозов, выставленных детям, в особенности новорожденным и в возрасте до 3 лет.

Реализация данного предложения видится возможной через комплексные медицинские обследования детей, находящихся в домах ребенка, с участием независимых экспертов, что позволит объективно подтвердить либо исключить

поставленные имеющиеся диагнозы, в целях оздоровления ребенка решить вопрос оказания дорогостоящей медицинской помощи (операций, протезирование и т.д.).

Согласно статье 27 Закона «О гражданстве Республики Казахстан» ребенок, являющийся гражданином Республики Казахстан, усыновленный иностранцами, сохраняет гражданство до своего совершеннолетия.

Иностранные усыновители обязаны ежегодно до достижения совершеннолетия усыновленного ребенка через консульские учреждения направлять информацию об условиях жизни, обучения, воспитания и состоянии здоровья в органы опеки и попечительства по прежнему месту проживания ребенка, то есть должен осуществляться сбор персональных данных усыновленных детей.

Однако ранее прокурорами неоднократно устанавливались факты непредставления таких ежегодных отчетов. В ряде случаев отсутствие контроля за условиями проживания усыновленных детей обусловлено тем, что в странах, в которых воспитываются казахстанские дети, отсутствуют посольства или консульские учреждения Республики Казахстан.

Компетентные органы отдельных стран (например, США) отказываются предоставлять необходимую информацию об усыновленных детях казахстанской стороне по причине того, что по их законодательству усыновленные за рубежом дети утрачивают гражданство страны происхождения и приобретают гражданство страны, куда они перевезены приемными родителями. То есть по некоторым усыновленным детям уполномоченным органам ничего не известно.

Ранее об этой проблеме Генеральная прокуратура информировала Правительство, после чего ситуация в целом улучшилась, но отдельные проблемы остаются.

Еще одной серьезной проблемой является ненадлежащее ведение «Черного списка усыновителей», а именно не включение в него персональных данных некоторых лиц. Прокурорами установлено 67 таких фактов. Это приводит к тому, что детей передаются ранее судимым, а также состоящим на наркологическом и психиатрическом учетах лицам.

К примеру, в 2018 году в Восточно-Казахстанской области под опеку переданы двое детей в г.Актобе семейной паре. При этом супруг был судим за изнасилование несовершеннолетней, совершенное группой лиц. В 2017 году в г. Алматы опекуном несовершеннолетнего назначен М., имеющий судимость за насильственные действия сексуального характера, совершенные в отношении заведомо несовершеннолетнего лица. В Павлодарской области несовершеннолетний передан на усыновление ранее судимому по нескольким статьям, в т.ч. за вовлечение несовершеннолетних в преступную деятельность [202].

Администрация медико-социальных учреждений для детей-инвалидов, интернатов для детей-сирот и других подобных учреждений нередко, имея доступ к персональным данным воспитанников, допускает неправомерное

использование их денежных средств. Исследователи относят такие нарушения к числу типичных нарушений прав несовершеннолетних, пребывающих в организациях для детей-сирот и детей, оставшихся без попечения родителей [203]. Схожие нарушения допускаются и в учреждения для взрослых лиц с различными заболеваниями. К примеру, в 2024 году прокуратурой Карагандинской области в ходе проверки центров оказания специальных социальных услуг выявлены серьезные нарушения прав недееспособных граждан, а именно нерациональное использование их пенсий и пособий путем закупа товаров по явно завышенным ценам [204]. Прокуратурой Абайской области в 2024 году при проведении проверки Семейского центра оказания специальных социальных услуг №1 установлены многочисленные нарушение, в том числе хищения пособий со счетов подопечных, страдающих психическими заболеваниями [205].

В 2022 году судом Абайским районным судом Карагандинской области осуждены руководитель Центра оказания специальных социальных услуг, 2 сотрудника Медико-социального учреждения престарелых инвалидов, а также почтальон отделения АО «Казпочта», которые в группе лиц похищали денежные средства у пенсионеров и инвалидов. Так, должностные лица, имея доступ к персональным данным подопечных, в том числе к их диагнозам и сведениям о состоянии здоровья, ежемесячно формировался список, в который включались лиц, не способных самостоятельно распоряжаться своими денежными средствами. Этот список направлялся почтальону АО «Казпочта», которая получала денежные средства за данных лиц. В дальнейшем подделывались подписи в ведомостях, а денежные средства распределялись [206].

Социальные работники имеют доступ к многочисленным персональным данным получателей специальных социальных услуг, информации об индивидуальных особенностях лиц, нуждающихся в специальных социальных услугах, состоянии здоровья, диагнозе заболевания, степени ограничения жизнедеятельности, что составляет профессиональную тайну социального работника. Недостаточная защищенность такой информации может повлечь существенный вред.

При проверках финансового законодательства в деятельности банков целесообразно включение вопроса защищенности персональных данных клиентов.

Проведенное анкетирование 127 лиц, из которых 104 обладали средним и высоким уровнем познаний в сфере юриспруденции, показало, что 37% считают, что наиболее часто персональные данные утекают с банковской сферы. При этом только 40,9% из опрошенных внимательно читают предоставляемые банками согласия на сбор и обработку персональных данных, 10,2% никогда полностью и внимательно не читают, 35,4% просматривают бегло, 12,6% не обращают внимания (Приложение И).

Центром анализа и расследования кибератак (ЦАРКА) в 2021 году проанализирована защищенность веб-ресурсов банков второго уровня

Республики Казахстан, в результате чего из 25 проанализированных ресурсов 9 имели уязвимости к атакам, 6 ресурсов не шифровали передаваемую информацию, в 8 ресурсах выявлены уязвимости по утечке данных, 2 ресурса могли быть атакованы через электронную почту, а также имели место другие недочеты по информационной безопасности [207].

В 2024 году Алмалинским районным судом г.Алматы по уголовным делам осужден А., ранее занимавший должность заместителя директора отделения АО «Банк…», которым со счетов клиентов банка похищено более 200 миллионов тенге. Пользуясь наличием доступа к персональным данным клиентов, А. определял лиц, у которых на счетах имеются значительные денежные суммы. В дальнейшем в информационной системе изменялся доверенный номер клиента, что давало А. доступ к управлению счетом и возможность для вывода денежных средств на подконтрольные ему счета [208].

Имея доступ к персональным данным, сотрудники банков могут совершать и другие противоправные действия. К примеру, в 2024 году Межрайоным судом по уголовным делам г.Астана осужден юрисконсульт одного из банков, который в поступившим к нему документам увидел данные своего знакомого, о чем сообщил ему, чем допустил срыв специальной операции органов национальной безопасности, направленной на пресечение канала поставки огнестрельного оружия и боеприпасов [209].

При проведении проверок в местах лишения свободы следует применять опыт Российской Федерации по искоренению мошеннических колл-центров путем выявления с помощью радиомониторинга абонентских номеров, используемых заключенными, и их последующего блокирования.

Таким образом, в ходе комплексных проверок практически по всем направлением возможно включение в виде дополнительного вопроса соблюдение законности в сфере персональных данных и их защите.

Анализ состояния законности должен проводиться по важным вопросам защищенности персональных данных.

В первую очередь, необходим глубокий и всесторонний анализ следственно-судебной практики по фактам нарушения законодательства о персональных данных.

С возникновением и развитием законодательства о неприкосновенности частной жизни и защите персональных данных практически одновременно встал и вопрос об ответственности за его нарушение.

Так, в Уголовном кодексе Республики Казахстан 1997 года заложена статья 142, которая предусматривала уголовную ответственность за нарушение неприкосновенности частной жизни.

Под такими действиями понималось «незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия, если эти деяния причинили вред правам и законным интересам потерпевшего» [210].

09.11.2011 года в статью внесены изменения. С этого момента под неприкосновенностью частной жизни следовало понимать «незаконное

собирание сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия» [211].

Как указывалось ранее, 21.05.2013 года был принят Закон Республики Казахстан «О персональных данных и их защите». Сопутствующим с ним Законом Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам персональных данных и их защиты» внесены изменения в статью 142 Уголовного кодекса.

В частности, статья изложена в следующей редакции «Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите».

В части 1 под этим деянием следовало понимать «незаконное собирание сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо причинение существенного вреда правам и законным интересам лица в результате незаконного сбора и (или) обработки иных персональных данных».

Также введена и новая 2 часть, которая установила уголовную ответственность за «несоблюдение мер по защите персональных данных лицом, на которое возложена обязанность принятия таких мер, если это деяние причинило существенный вред правам и законным интересам лиц».

Часть 3 предусматривала уголовную ответственность за вышеуказанные «действия, совершенные лицом с использованием своего служебного положения или в целях извлечения выгод и преимуществ для себя или для других лиц или организаций, а также за распространение сведений в публичном выступлении или средствах массовой информации» [212].

В.А. Новиков, сравнивая уголовное законодательство Республики Казахстан и Российской Федерации, отметил, что в соседнем государстве в последние годы имеет место рост преступлений, совершенных с использованием персональных данных. В этой связи автор предложил в Российской Федерации использовать положительный опыт Республики Казахстан в части усиления ответственности за незаконное собирание и распространение персональных данных [213].

В.В. Вабищевич отмечает, что «Республика Казахстан первой из стран Евразийского экономического союза регламентировала уголовное наказание за непосредственное нарушение законодательства о персональных данных» [214].

Следует также отметить, что Законом Республики Казахстан от 23.04.2014 года №200-V ЗРК «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам деятельности органов внутренних дел» в Уголовный кодекс введена «Глава 7-1. Преступления против безопасности информационных технологий», в которой появилась статья 227-8, предусматривавшая ответственность за «неправомерное распространение электронных информационных ресурсов ограниченного доступа».

Исходя из диспозиции статьи, преступлением считалось «неправомерное распространение электронных информационных ресурсов, содержащих персональные данные граждан или иные сведения, доступ к которым ограничен законами Республики Казахстан, их собственником или владельцем» [215].

При принятии в 2014 году нового Уголовного кодекса указанные статьи сохранились в той же редакции. При этом статья 142 стала 147, а «Глава 7-1. «Преступления против безопасности информационных технологий» преобразовалась в «Главу 7. Уголовные правонарушения в сфере информатизации и связи» с изменением нумерации статей, а именно статья 227-8 преобразована в статью 211 [216].

24.11.2015 года Законом Республики Казахстан №419-V ЗРК «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информатизации» в Уголовный кодекс внесены изменения, статья 147 изложена в новой редакции.

Предусмотрена ответственность:

- «за несоблюдение мер по защите персональных данных лицом, на которое возложена обязанность принятия таких мер, если это деяние причинило существенный вред правам и законным интересам лиц» (часть 1);

- «незаконное собирание сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо причинение существенного вреда правам и законным интересам лица в результате незаконных сбора и (или) обработки иных персональных данных» (часть 2);

- «за эти же действия лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, либо путем незаконного доступа к электронным информационным ресурсам, информационной системе или незаконного перехвата информации, передаваемой по сети телекоммуникаций, либо в целях извлечения выгод и преимуществ для себя или для других лиц, или организаций» (часть 3);

- «за распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо причинение существенного вреда правам и законным интересам лица в результате незаконного сбора и (или) обработки иных персональных данных (часть 4) и за распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении, в средствах массовой информации или с использованием сетей телекоммуникаций» (часть 5) [217].

Содержание статьи 211 Уголовного кодекса 2014 года не отличается от статьи 227-8 Уголовного кодекса 1997 года за исключением некоторого изменения санкций.

Помимо указанного ответственность за нарушение законодательства о персональных данных может возникнуть и другим статьям Уголовного кодекса, как, например, статья 205 «Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций», статья 206 «Неправомерные уничтожение или модификация информации», статья 207

«Нарушение работы информационной системы или сетей телекоммуникаций», статья 208 «Неправомерное завладение информацией», статья 209 «Принуждение к передаче информации», статья 210 «Создание, использование или распространение вредоносных компьютерных программ и программных продуктов» и других.

Несмотря на кажущуюся на первый взгляд детальную проработку норм об ответственности за нарушение законодательства в сфере персональных данных и их защите, уровень выявляемых в этой сфере уголовных правонарушений не отражает реальной ситуации с защищенностью персональных данных в стране (таблица 4).

Таблица 4 – Статистика по уголовным делам

*Наименование статьи УК**	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024 (6 мес)
1	2	3	4	5	6	7	8	9	10	11	12	13
Нарушение непри косновенности частной жизни и законодательства о персональных данных и их защите ст.147**	1	3	37	59	22	29	34	49	35	39	66	44
	Осуждено/оправдано лиц											
	0/0	0/0	0/2	1/6	0/6	5/11	5/15	2/4	7/16	2/3	9/14	8/2
Неправомерный доступ к информа ции, в информацион ную систему или сеть телекоммуни каций. ст.205	-	-	50	44	53	28	59	3,7	46	43	32	16
	Осуждено/оправдано лиц											
	-	-	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	1/0	0/0
Неправомерные уничтожение или модификация информации. ст.206	-	-	14	9	22	13	6	9	9	15	29	35
	Осуждено/оправдано лиц											
	-	-	0/0	0/0	0/0	1/0	0/1	0/0	2/0	1/0	0/0	2/0
Нарушение работы информационной системы или сетей телекоммуникаций. ст.207	-	-	9	11	7	5	6	4	0	10	4	3
	Осуждено/оправдано лиц											
	-	-	0/0	0/0	0/0	0/0	1/0	1/0	0/0	0/0	1/0	0/0
Неправомерное завладение инфор мацией. ст.208	-	-	14	20	4	11	16	4	9	6	6	1
	Осуждено/оправдано лиц											
	-	-	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	5/0	5/0
Принуждение к передаче информации. ст.209	-	-	1	0	0	1	0	0	0	0	0	0
	Осуждено/оправдано лиц											
	-	-	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Создание, использо вание или распрост ранение вредонос ных компьютерных	-	-	61	24	11	4	4	4	4	5	4	2
	Осуждено/оправдано лиц											
	-	-	0/0	0/0	0/0	0/0	0/0	0/0	1/0	0/0	4/0	0/0

Продолжение таблицы 4

1	2	3	4	5	6	7	8	9	10	11	12	13
программ и программных продуктов. ст.210												
Неправомерное распространение электронных информационных ресурсов ограниченного доступа. ст.211	-	-	19	17	7	7	8	4	5	5	3	2
	Осуждено/оправдано лиц											
	-	-	0/0	0/0	0/0	0/0	1/0	6/0	0/0	0/0	0/0	0/0
* – в скобках указана статья в старой редакции УК; ** – ст. 142												

За более чем 10 лет (с 2013 года) по статье 147 (в утратившей силу редакции - статья 142) Уголовного кодекса за нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите зарегистрировано 418 фактов, по которым судами осуждено 39 лиц, 79 лиц оправдано, 27 уголовных дел прекращено по реабилитирующим основаниям. Более 60% возбужденных уголовных дел прекращены по реабилитирующим основаниям. За неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций по статье 205 Уголовного кодекса с 2015 года зарегистрировано 408 уголовных дел, из которых только одно дошло до суда и одно лицо было осуждено. За неправомерное уничтожение или модификацию информации по статье 206 Уголовного кодекса с 2015 года зарегистрировано 161 уголовное дело, из которых до суда дошли 9 дел, из них 1 дело прекращено, 3 возвращены прокурору, по 5 делам состоялись приговоры: 6 лиц осуждены, 1 лицо оправдано. Схожая ситуация и по статьям 207-210 Уголовного кодекса [218].

Изучение уголовных дел показало, что зачастую отсутствует надлежащая квалификация таких деяний. К примеру, в 2024 году значительный резонанс в обществе получило уголовное дело в отношении бывшего лица, которое под угрозой распространения интимных изображений своей бывшей супруги Н. требовал передать ему имущество при разводе, хотя оно было приобретено Н. до вступления в брак. Учитывая закрытый характер судебного разбирательства, основываясь на сведениях, опубликованных Н., ее бывший супруг был осужден по части 4 статьи 147 Уголовного кодекса [219]. В данном случае была необходима дополнительная квалификация деяний по пункту 2 части 3 или пункту 2 части 4 статьи 194 Уголовного кодекса, а именно за вымогательство под угрозой распространения сведений, позорящих потерпевшего с целью получения имущества в крупном размере (или в особо крупном размере).

В соответствии с пунктом 5 Нормативного постановления Верховного Суда Республики Казахстан от 23.06.2006 года №6 «О судебной практике по делам о вымогательстве» под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, оглашение которых может

причинить существенный вред интересам потерпевшего или его близких, следует понимать требование передачи чужого имущества либо права на имущество или совершения других действий имущественного характера, сопровождающееся угрозой разглашения любых сведений, которые могут нанести вред чести и достоинству потерпевшего. При этом не имеет значения, соответствуют ли действительности сведения, под угрозой разглашения которых совершается вымогательство. В то же время необходимо иметь в виду, что потерпевший стремится сохранить эти сведения в тайне, а угроза их разглашения используется виновным, чтобы принудить его к выполнению выдвинутых требований.

Существенный вред может быть причинен распространением сведений, позорящих потерпевшего. При определении существенного вреда учитывается как субъективная оценка потерпевшим тяжести причиненного ему нравственного ущерба, так и объективные данные, свидетельствующие о степени нравственных и физических страданий потерпевшего в результате вымогательства, совершенного под угрозой распространения порочащих сведений.

В данном Нормативном постановлении Верховного Суда также указано, что существенный вред может быть причинен и оглашением иных сведений, которые не являясь позорящими, способны причинить потерпевшему существенный вред, например, разглашение коммерческой тайны, влекущее причинение убытков бизнесу, разглашение тайны усыновления либо сведения, относящиеся к семейной и частной жизни и т.п. [220] Полагаем целесообразным добавить к ним и персональные данные.

Следует отметить, что распространение интимных фотографий встречается достаточно часто, но единой практики до настоящего времени не имеется. Так, в 2023 году в г. Алматы судом оправдан Д., отправивший интимные фотографии своей бывшей супруги ее родителям и родственникам. В свою очередь в 2024 году за такие же действия в Западно-Казахстансой области осужден И., а в г. Талдыкорган в 2023 году осужден Е., который отправил близким родственникам своей бывшей девушки ее фото и видео интимного характера, а также от ее имени зарегистрировался в социальных сетях, публиковал в них указанные изображения, а также объявления об оказании его бывшей девушкой интимных услуг.

Примечателен подход Российской Федерации, где прокуроры рекомендуют в таких случаях привлекать винновых к ответственности, как за нарушение неприкосновенности частной жизни, так и за незаконные изготовление и оборот порнографических материалов [139, с. 27-28]. Также следует отметить опыт Республики Узбекистан, где в Уголовном кодексе имеется статья 141.3, которой предусмотрена уголовная ответственность за распространение или угрозу распространения информации, содержащей фото и (или) видеоизображения обнаженного тела и (или) половых органов лица без его согласия, в том числе распространение в СМИ, сетях телекоммуникаций или сети Интернет [221].

Нельзя не подчеркнуть, что в настоящее время многие другие преступления совершаются под угрозой распространения интимных фотографий или видеозаписей. Так, в 2024 году резонанс получил случай в Кызылординской области, где 11 человек под угрозой распространения персональных данных в виде интимных фото и видео вовлекли несовершеннолетнюю в занятие проституцией. В этом же году в г.Туркестан 33-летний мужчина под угрозой аналогичных действий совершил изнасилование несовершеннолетней и вымогал у нее денежные средства. В целом, таких примеров немало.

Возможно включение в признаки совершения преступлений таких действий, как «под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких» в ряд статей Уголовного кодекса Республики Казахстан.

Однако более целесообразным видится внести изменения и дополнения в нормативные постановления Верховного Суда Республики Казахстан №1 от 11.05.2007 года, №4 от 11.05.2007 года, №6 от 11.04.2002 года, №6 от 23.06.2006 года, №3 от 14.05.1998 года и №7 от 28.12.2009 года, согласно которым преступления, предусмотренные статьями 105 (Доведение до самоубийства, склонение к совершению самоубийства или содействие совершению самоубийства), 123 (Понуждение к половому сношению, мужеложству, лесбиянству или иным действиям сексуального характера), 132 (Вовлечение несовершеннолетнего в совершение уголовных правонарушений), 134 (Вовлечение несовершеннолетнего в занятие проституцией, оказание иных услуг сексуального характера), 144 (Вовлечение несовершеннолетних в изготовление продукции эротического содержания), 298 (Хищение либо вымогательство наркотических средств, психотропных веществ, их аналогов), 299 (Склонение к потреблению наркотических средств, психотропных веществ, их аналогов), 308 (Вовлечение в занятие проституцией, оказание иных услуг сексуального характера), 312 (Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних либо их привлечение для участия в зрелищных мероприятиях порнографического характера), 415 (Принуждение к даче показаний), 422 (Подкуп или принуждение к даче ложных показаний или уклонению от дачи показаний, ложному заключению либо к неправильному переводу) Уголовного кодекса Республики Казахстан, могут совершаться под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.

На наш взгляд, на сегодня серьезной проблемой, препятствующей привлечению виновных к уголовной ответственности за несоблюдение мер по защите персональных данных, а также незаконный сбор и (или) обработку (за исключением распространения) персональных данных является отнесение

частей 1 и 2 статьи 147 Уголовного кодекса к делам частного обвинения. Производство по делам данной категории начинается не иначе как по жалобе потерпевшего, который является частным обвинителем по делу и поддерживает обвинение в суде. Досудебное расследование по таким делам не проводится, частное обвинение возбуждается при подаче жалобы в суд. Представление и сбор доказательств возлагается на лицо, подавшее жалобу. Однако изучение судебной практики показывает, что для доказательства факта несоблюдения мер по защите персональных данных или незаконности сбора и обработки без распространения персональных данных, как правило, требуется доступ к информационной системе, компьютерной или иной технике обвиняемого лица, что в абсолютной большинстве случаев не представляется возможным и в итоге лишает возможности представления суду доказательств.

Анализ отчетов формы № 1 «Отчет о работе судов первой инстанции по рассмотрению уголовных дел» показал, что за 2016-2023 годы и 6 месяцев 2024 года по части 1 статьи 147 Уголовного кодекса судами с вынесением приговора рассмотрено 15 уголовных дел, по которым 1 лицо осуждено, 14 оправдано. Также судами прекращено 8 дел, из которых 4 за примирением сторон и 4 по реабилитирующим основаниям.

За аналогичный период по части 2 статьи 147 Уголовного кодекса с вынесением приговора рассмотрено 46 уголовных дел, по которым 2 лица осуждены, 58 оправданы. Прекращено 29 дел, из которых 4 за примирением сторон, 24 по реабилитирующим основаниям и 1 по иным основаниям.

Таким образом, за 8,5 лет к уголовной ответственности за несоблюдение мер по защите персональных данных привлечено всего 4 лица, а за незаконное собирание сведений о частной жизни лица либо незаконный сбор и (или) обработку (за исключением распространения) персональных данных 6 лиц, то есть более чем в 80% случаев предполагаемые нарушители избежали ответственности [222].

К примеру, в 2022 году в г.Алматы на общем собрании жильцов Т. и К. сообщили, что получили через своих знакомых в органах прокуратуры сведения о привлечении к уголовной ответственности директора компании по обслуживанию дом Щ. и иные сведения относительно членов совета дома. По данному факту Щ. обратилась в суд в качестве частного обвинителя, но, не имея доступа к информационным системам органов прокуратуры, она не смогла представить доказательства своего обвинения, в результате чего Т. и К. были оправданы. В другом случае, в г. Жаркент неизвестное лицо создало профиль С. на сайтах знакомств, осуществляло от ее имени переписку интимного характера, а также рассылало ее персональные данные, в том числе номер телефона. По косвенным признакам она поняла, что эти действия осуществил ее знакомый А., в чем он ей сознался. Однако, не имея доступа к его компьютеру и телефону, в суде С. не смогла представить доказательства, что в итоге стало причиной оправдания А.

Еще одной значимой проблемой, препятствующей привлечению виновных к уголовной ответственности, за нарушение неприкосновенности

частной жизни и законодательства Республики Казахстан о персональных данных и их защите, является наличие в объективной стороне состава данного преступления обязательного признака в виде причинения существенного вред правам и законным интересам лиц. При этом в уголовном законодательстве и нормативных постановлениях Верховного Суда отсутствует толкование признака «существенный вред» относительно обработки персональных данных. Следует отметить, что схожая ситуация отмечается и других государствах, где введена уголовная ответственности за незаконную обработку персональных данных, в связи с чем данный вопрос является предмет исследования немалого количества ученных.

К.С. Захилько первичные и вторичные последствия существенного вреда правам свободам и законным интересам граждан в контексте анализируемого вида преступлений. Вред, который вызывается незаконной обработкой персональных данных или распространением сведений о частной жизни является первичным последствием преступления. При этом существенность первичного последствия (нарушение прав на защиту от незаконного вмешательства в частную жизнь и защиту персональных данных) предлагает определять из совокупности таких обстоятельств, как значимость информации для личности, вид информации и объем данных, возможность восстановления конфиденциальности сведений, негативное влияния конфиденциальной информации на честь и достоинство личности, утрата контроля над информацией о себе (в том числе в результате широкой публикации, включения ее в банки данных для обработки искусственным интеллектом и т.д.). Вред, который нанесен нарушением прав на защиту персональных данных или распространения сведений о частной жизни является вторичным последствием преступления. Существенность нарушения таких прав может подтверждаться причинением гражданину морального и социального вреда, а также имущественного ущерба [223].

А.А. Пухов указывает, что «объективная сторона состава преступления (незаконные действия в отношении информации о частной жизни и персональных данных) состоит из деяния (незаконные сбор и предоставление), общественно опасных последствий (причинение существенного вреда правам, свободам и законным интересам гражданина) и причинной связи между ними». Также, по мнению А.А. Пухова, «состав преступления материальный. Преступление признается оконченным с момента причинения существенного вреда правам, свободам и законным интересам гражданина. Такой вред может иметь как имущественный, так и неимущественный характер. Это может быть выражено в опорочивании деловой репутации, моральных либо психических переживаниях, заболевании, отказе в приеме на работу, упущенной выгоде от незаключенной сделки и т.п.» [224].

В Республике Казахстан под существенным вредом правам и законным интересам лиц в результате несоблюдения мер по защите и незаконной обработки персональных данных предлагается понимать нарушение права на защиту персональных данных, чем потерпевшему лицу причинен

имущественный и (или) неимущественный ущерб. Под имущественным ущербом следует понимать затраты лица на восстановление конфиденциальности персональных данных, утраченную выгоду и другие негативные последствия финансового характера. Под неимущественным ущербом следует понимать нравственные и физические страдания, моральные или психические переживания и другие негативные последствия, в том числе влияющие на честь, достоинство и деловую репутацию. При определении существенного вреда следует учитывать субъективную оценку потерпевшим тяжести причиненного ему ущерба, а также объективные данные о значимости, виде и объеме незащищенных или обработанных персональных данных, стоимости устранения последствий этих действий.

В некоторых исследованиях указывается об отсутствии в законодательстве ряда дефиниций касающихся уголовных правонарушений, совершенных в сети Интернет, а именно таких, как «компьютерная программа», «компьютерная система», «компьютерная сеть», «сеть телекоммуникаций» [225], что также может быть применимо и к персональным данным, поскольку их похищение чаще всего происходит с использованием сети Интернет.

В целом, уголовная ответственность за несоблюдение мер по защите и незаконную обработку персональных данных вызывает множество вопросов и дискуссий, что еще раз подтверждает необходимость проведения органами прокуратуры анализов в данной сфере.

К примеру, Е.Н. Рязанова обращает внимание, что в законодательстве зарубежных стран введена уголовная ответственность за кражу персональных данных и под этим понимается умышленная передача или использование персональных данных с целью совершения или способствования совершению преступных деяний [226]. В.В. Вабищевич предлагает разграничение уголовно-правовой охраны информации о частной жизни и персональных данных с учетом объекта, объективной стороны и предмета преступных посягательств путем разделения ответственности за разглашение информации о частной жизни и нарушение законодательства о персональных данных в отдельные статьи Уголовного кодекса Республики Беларусь [227]. Следует отметить, что в Республике Узбекистан нарушение неприкосновенности частной жизни и нарушение законодательства о персональных данных уже разделены в Уголовном кодексе на 2 отдельных состава преступления (статьи 141.1 и 141.2).

Еще одним важным направлением для проведения прокурорами анализа состояния законности является соблюдение средствами массовой информации законодательства при сборе и обработке персональных данных, поскольку средствами массовой информации нередко допускается сбор и публикация персональных данных граждан без их согласия.

К примеру, в 2022 году журналист М. обратился к сотруднику военной полиции К. для оказания содействия в получении персональных данных нескольких лиц, в отношении которых он осуществлял ряд публикаций негативного характера. К., используя доступ к информационным системам, осуществил незаконный сбор персональных данных (об адресе регистрации,

месте жительства, находящихся в собственности автотранспортных средствах, используемых номерах телефонов, документах, удостоверяющих личность и другие) и передал их журналисту М., который в дальнейшем использовал эти в своих публикациях для создания негативного образа в отношении лиц, данные которых получил. В 2023 году Военным судом Алматинского гарнизона журналист М. и сотрудник военной полиции К. осуждены.

Между тем, в средствах массовой информации имеется немало других публикаций, в содержании которых упоминаются персональные данные граждан, происхождение которых остается неизвестным.

Имеют место явные нарушения законодательства. К примеру, начиная с марта 2024 года, во многих масс-медиа опубликована информация, что сын одного из акимов района Павлодарской области избил в школе одну из учениц. В публикациях размещены фото и видеоизображения предполагаемого правонарушителя, сведения о месте работы его обоих родителей. При этом в соответствии с подпунктом 2 пункта 3-4 статьи 14 Закон «О средствах массовой информации» запрещается распространение в средствах массовой информации или сетях телекоммуникаций персональных и биометрических данных лица, включая информацию об его родителях и иных законных представителях, иной информации, позволяющей установить личность, о несовершеннолетних, подозреваемых и (или) обвиняемых в совершении административных и (или) уголовных правонарушений. 19.06.2024 года данный закон утратил силу ввиду принятия нового Закона «О масс-медиа», в котором впрочем аналогичная норма сохранилась [228, 229].

В целом, вопрос использования и размещения в продукции масс-медиа персональных данных, а в особенности изображений лиц вызывает множество вопросов.

Статьей 145 Гражданского кодекса Республики Казахстан закреплено право на собственное изображение, предполагающее невозможность использования изображения какого-либо лица без его согласия или согласия наследников в случае смерти лица [230]. Однако фото и видео изображения многих лиц публикуются в средствах массовой информации практически бесконтрольно. Четкая позиция имеется лишь относительно публикации изображения лица без согласия в продукции масс-медиа, а именно пунктом 2 статьи 14 Закона Республики Казахстан «О масс-медиа» определены случаи, когда такие действия допускаются. Следует отметить, что данная норма не всегда положительно воспринимается лицами, чье изображение публикуется без согласия, в особенности лицами, совершившими правонарушения. К примеру, в 2023 году гр. Н., ранее осужденный за совершение особо тяжкого преступления к пожизненному лишению свободы и изображение которого было опубликовано в средствах массовой информации, обратился в Конституционный Суд для признания нормы неконституционной. Однако, Конституционным Судом каких-либо противоречий не выявлено, за средствами массовой информации признано право публикации изображений преступников

в целях защиты конституционного строя, охраны общественного порядка, прав и свобод человека, здоровья и нравственности населения.

В свою очередь, в некоторых государствах данный вопрос урегулирован законодательно. Например, в пункте 2 статьи 31 Конституции Болгарии указано, что никто не может быть подвергнут наблюдению, сфотографирован, снят на пленку, записан или подвергнут каким-либо иным аналогичным действиям без его ведома или вопреки его выраженному несогласию, за исключением случаев, предусмотренных законом [231].

Отдельного изучения требует вопрос публикации фото и видеоизображений государственных служащих, поскольку в настоящее время нередко журналисты провоцируют их на грубость, а также пытаются выставить их некомпетентными. К примеру, С.В. Адаховской изучен вопрос защиты сотрудников полиции от незаконного распространения их персональных данных в средствах массовой информации [232].

Анализа требует деятельность блоггеров, которыми нередко распространяются персональные данные. К примеру, в 2022 году Талдыкорганским городским судом Алматиснкой области осужден блоггер А., который на своих страницах с аудиторией более 120 тысяч человек распространил сведения о том, что К. состоит на учете в психоневрологическом диспансере. Е.Н. Бегалиев относительно института блоггинга отмечает, что необходимо нормативное правовое урегулирование и определение единых стандартов деятельности в этой сфере, ведение реестра блоггеров, а также усиление прокурорского надзора в этом направлении [233].

Отдельного анализа требует вопрос недопущения нарушения законодательства о персональных данных и их защите при применении в Казахстане OSINT-инструментов. Н.Н. Романова и В.В. Грызунов отмечают, что «обнаружены следующие угрозы для безопасности персональных данных при использовании злоумышленниками OSINT: сбор информации/обнаружение конфиденциальной информации; социальная инженерия; нарушение конфиденциальности; кибершпионаж; фишинг; утечка данных; обнаружение уязвимостей информационных систем. Определены средства защиты для персональных данных пользователя от атак с использованием OSINT: межсетевые экраны (файрволлы); средства мониторинга сети; средства обнаружения попыток несанкционированного доступа (вторжения); нейронные сети; организационные методы; настройка приватности; сильные пароли и двухфакторная аутентификация; шифрование данных; использование VPN; резервное копирование данных» [234].

Следует проанализировать обоснованность использования гражданами Казахстана большого количества абонентских номеров телефонов. К примеру, по данным Роскомнадзора, в Российской Федерации количество абонентов, в распоряжении которых находится более 50 SIM–карт, составляет 22,7 тысяч, более 100 – 7,3 тысяч, более 200 – 2,7 тысяч, более 500 – 747, более 1000 – 268. Количество таких фактов в Казахстане неизвестно. При этом существующий порядок позволяет регистрацию абонентов без подтверждения личности, в

результате чего многие номера могут использовать другими лицами, а лица, числящиеся владельцами номеров, даже не знают об этом.

В сфере государственной правовой статистики, как указывалось в правила использования СИО ПСО внесены изменения, согласно которым теперь для входа в систему необходимо прохождение многофакторной аутентификации, включая проверку ЭЦП и биометрии пользователя (отпечатков пальцев либо Face ID), либо подтверждение личности через SMS-код, что направлено на решение имевшихся проблем.

В то же время подобные изменения не внесены в «Правила и оснований получения правоохранительными органами из системы информационного обмена правоохранительных, специальных государственных и иных органов информации, необходимой для проведения негласных следственных действий и оперативно-розыскной деятельности, а также для решения иных возложенных на них задач», утвержденные совместным приказом Генерального Прокурора от 21.12.2015 года №150 и Министра внутренних дел Республики Казахстан от 31.12.2015 года №1119 и Министра финансов Республики Казахстан от 30.12.2015 года №733 и Министра по делам государственной службы Республики Казахстан от 30.12.2015 года №21. Так, согласно пункту 16 данных Правил работа в СИО ПСО начинается с прохождения пользователем Системы процедуры аутентификации, которая осуществляется средствами ЭЦП пользователя [235]. Аналогично не внесены изменения в «Правила и основания получения органами государственных доходов из системы информационного обмена правоохранительных, специальных государственных и иных органов информации, необходимой для осуществления налогового и таможенного контроля в форме налоговых и таможенных выездных проверок», совместным приказом Генерального Прокурора Республики Казахстан от 26.01.2023 года №41 и Заместителя Премьер-Министра - Министра финансов Республики Казахстан от 26.01.2023 года №69. Согласно пункту 5 данных Правил вход в СИО ПСО начинается с прохождения пользователем процедуры аутентификации, которая осуществляется посредством ЭЦП [236]. Данные противоречия требуют устранения.

Также следует внести требования о двухфакторной аутентификации в другие правовые акты, регулирующие порядок входа и использования ЕРДР, ЕРАП и других информационных систем органов прокуратуры. Вместе с тем имеет целесообразность рассмотрения вопроса предоставления доступа к информационным системам органов прокуратуры только через верифицированные IP-адреса для исключения возможности передачи права доступа посторонним лицам, с посторонних компьютеров или устройств.

При этом следует проводить периодические проверки по вопросу соблюдения конфиденциальности сведений, получаемых при использовании СИО ПСО, ЕРДР, ЕРАП и других информационных систем органов прокуратуры.

Результаты проверок и анализов следует использовать в работе органов прокуратуры по межведомственному взаимодействию в сфере защиты

персональных данных, для проведения заседаний Координационного совета по обеспечению законности, правопорядка и борьбы с преступностью по вопросам совершения преступлений в отношении охраняемой законом информации, а также преступлений, совершенных с использованием похищенных персональных данных, проведения коллегий по вопросам защиты персональных данных.

Целесообразно также подписание меморандумов с ведущими организациями в области цифрового права и защиты персональных данных.

Результаты проверок, анализов, а также оценки, актов вступивших в законную силу, было бы эффективным использовать и для участия прокурора в нормотворческой деятельности в целях совершенствования законодательства о персональных данных и их защите.

Таким образом, в целях совершенствования прокурорского надзора в сфере персональных данных и их защите необходимо использование всего арсенала правых средств прокурора, а основными правовыми инструментами буду являться проверка, анализ и оценка актов, вступивших в силу.

Проверки могут быть предметные, то есть по соблюдения непосредственно законодательства о персональных данных и их защите, а также тематические, то есть с выключением в предмет проверки вопроса защиты персональных данных

Предметные проверки могут проводиться:

1. В деятельности уполномоченного органа в сфере защиты персональных данных.

2. В деятельности государственных органов и их должностных лиц по вопросам соблюдения законодательства о персональных данных и их защите.

3. В деятельности местных исполнительных органов по вопросам реализации их компетенции.

4. В деятельности квазигосударственных организаций, государственных учреждений (школы, больницы и т.д.), коммунальных предприятий, других организаций.

5. В деятельности собственников и операторов баз, содержащих персональные данные.

6. В деятельности правоохранительных, специальных и иных государственных органов относительно законности получения пользователями сведений из СИО ПСО, ЕРДР, ЕРАП и других информационных систем органов прокуратуры.

7. В иных случаях, в том числе по поручениям Президента и Генерального Прокурора Республики Казахстан.

Тематические проверки с выключением в предмет проверки вопроса защиты персональных данных могут проводиться по всем отраслям и направлениям прокурорского надзора. При этом полагаем, что упор должен быть на неопределенный круг лиц, защиту прав уязвимых слоев, несовершеннолетних и лиц, которые не могут себя защитить.

Оценке подлежат нормативные правовые акты в сфере персональных данных и их защиты акты центральных государственных органов, правовые акты уполномоченного органа, акты операторов и собственников баз данных об утверждении перечней персональных данных, необходимых и достаточных для выполнения осуществляемых ими задач, а также определяющие политику в отношении сбора, обработки и защиты персональных данных и другие акты в данной сфере.

Повышению эффективности прокурорского надзора в сфере защиты персональных данных препятствует несовершенство уголовного законодательства.

Видится целесообразным перевод частей 1 и 2 статьи 147 Уголовного кодекса в категорию дел частно-публичного обвинения, поскольку в настоящее время они относятся к категории дел частного обвинения, которые не предполагают проведение досудебного расследование, а также возлагают обязанности по сбору и предоставлению суду доказательств на частных обвинителей, что в условиях отсутствия их доступа к служебной документации, информационным системам, компьютерной или иной технике обвиняемого лица в большинстве случаев лишает возможности представления суду доказательств и в итоге влечет оправдание лиц даже по реальным фактах несоблюдения мер по защите персональных данных, а также незаконного сбора и (или) обработки (за исключением распространения) персональных данных.

В Республике Казахстан под существенным вредом правам и законным интересам лиц в результате несоблюдения мер по защите и незаконной обработки персональных данных предлагается понимать нарушение права на защиту персональных данных, чем потерпевшему лицу причинен имущественный и (или) неимущественный ущерб. Под имущественным ущербом следует понимать затраты лица на восстановление конфиденциальности персональных данных, утраченную выгоду и другие негативные последствия финансового характера. Под неимущественным ущербом следует понимать нравственные и физические страдания, моральные или психические переживания и другие негативные последствия, в том числе влияющие на честь, достоинство и деловую репутацию. При определении существенного вреда следует учитывать субъективную оценку потерпевшим тяжести причиненного ему ущерба, а также объективные данные о значимости, виде и объеме незащищенных или обработанных персональных данных, стоимости устранения последствий этих действий.

Кроме того, назрела необходимость введения уголовной ответственности за распространение или угрозу распространения без его согласия лица фото и (или) видеоизображений его обнаженного тела и (или) половых органов, а также видится целесообразным внесение изменений и дополнений в нормативные постановления Верховного Суда Республики Казахстан №1 от 11.05.2007 года, №4 от 11.05.2007 года, №6 от 11.04.2002 года, №6 от 23.06.2006 года, №3 от 14.05.1998 года и №7 от 28.12.2009 года, согласно которым преступления, предусмотренные ст.ст. 105, 123, 132, 134, 144, 194,

298, 299, 308, 312, 415, 422 Уголовного кодекса Республики Казахстан, могут совершаться под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.

Выводы по разделу

1. Во многих зарубежных государствах, особенно в Европе, на сегодня скоплен значительный опыт в области защиты персональных данных, внедрение которого целесообразно и в Казахстане. Европейское законодательство, а также принятые в Европе международные документы являются правовым ориентиром для всех остальных государств. При этом ряд государств уже признали право на защиту персональных данных конституционным правом, отдельным от права на неприкосновенность частной жизни, что в обозримом будущем возможно и в Казахстане. Значительный вклад в защиту персональных данных за рубежом вносит и практика ЕСПЧ. Вместе с тем в последние годы значительное внимание зарубежными государствами уделяется законодательному урегулированию применения искусственного интеллекта, в том числе в контексте персональных данных.

2. Органам прокуратуры Казахстана в целях повышения эффективности прокурорского надзора в сфере защиты персональных данных следует активизировать работу. Необходимо проведение тематических проверок по вопросам защиты персональных данных, а также такие вопросы целесообразно включать при проведении проверок в области медицины, защиты прав несовершеннолетних, трудового, банковского и другого законодательства. Важным также является проведение качественного анализа судебно-следственной практики расследования и рассмотрения уголовных дел по фактам нарушения законодательства в сфере персональных данных и их защиты. Не менее важным является проведение оценки актов, предполагающих сбор и обработку персональных данных граждан.

ЗАКЛЮЧЕНИЕ

По результатам исследования, проведенного в рамках докторской диссертации, обобщения научных трудов по теме, анализа отечественного и зарубежного законодательства по проблематике, авторы работы, достигнув поставленных целей и решив соответствующие задачи исследования, пришли к следующим выводам.

Текущая ситуация в мире свидетельствует о тенденции постоянного роста количества собираемых, обрабатываемых и хранящихся данных, непрекращающихся попытках злоумышленников похитить эту информацию, в том числе персональные данные, которые содержаться в базах данных государственных органов, банков, различных организаций, а также на устройствах пользователей сети Интернет. Число успешных кибератак остается на высоком уровне, они наносят существенный вред, как государствам, различным организациям, так и простым гражданам, чьи персональные данные похищаются и используются в противоправных целях.

По прогнозам специалистов ситуация в сфере информационной безопасности длительное время будет оставаться сложной, а также не исключается ее ухудшение, поскольку злоумышленниками используются все новые способы совершения противоправных действий, в том числе с применением технологий искусственного интеллекта.

В Республике Казахстан с последние годы также зафиксировано немало фактов массовых утечек персональных данных граждан. В определённой степени на это влияет активная цифровизация практически всех сфер общественных отношений, от предоставления государственных услуг, до перевода бизнесом своих решений в цифровой формат. В ближайшей перспективе предполагается массовая интеграция государственных и частных сервисов, что повышает угрозы защищенности персональных данных.

Согласно данным социологических опросов граждане Казахстана постоянно сталкиваются со случаями интернет-мошенничества и не чувствуют свои персональные данные защищенными.

На сегодня в Республике Казахстан сформировано законодательство о персональных данных и их защите, однако его несовершенство и отсутствие отдельных понятий, в том числе общепризнанных и применяемых в зарубежных странах является сдерживающим фактором эффективной защиты персональных данных, в том числе прокурорского надзора в этой сфере. Кроме того, Республика Казахстан не является участником общепризнанных международных правовых актов, регулирующих вопросы защиты персональных данных.

Государственными органами проводится работа по защите информационных ресурсов государственных органов и критически важной информационной инфраструктуры, отражению кибераткак, предотвращению звонков с подменных номеров и защите персональных данных. В этой работе принимают участие и органы прокуратуры.

При этом прокурорский надзор в сфере защиты персональных данных возник только в 2013 году и является достаточно молодым и малоизученным направлением. При этом до 2020 года прокуратура являлась фактически единственным государственным органом, наделенным надзорными полномочиями в сфере защиты персональных данных. В 2020 году в Казахстане появился уполномоченный орган по защите персональных данных, но за органами прокуратуры по-прежнему сохранился высший надзор за соблюдением законности в сфере персональных данных и их защиты. После появления уполномоченного органа в сфере защиты персональных данных важным является определение роли и места прокуратуры в сфере защиты персональных данных. При этом необходимо отметить, что появление уполномоченного органа и недостаточное законодательное урегулирование полномочий прокуратуры в отраслевом законе не говорит о том, что надзор в данном направлении должен сужаться или не осуществляться вовсе.

Следует отметить, что органы прокуратуры наделены не только надзорной функцией, но и осуществляют сбор и обработку персональных данных, являясь одновременно и надзорным органом и оператором значительного числа баз, содержащих персональные данные, в том числе биометрических и чувствительных, таких как сведения о судимости.

Несмотря на отсутствие правовых актов, руководящих указаний Генерального Прокурора, ведомственных актов и достаточной официальной информации о результатах, достигнутых органами прокуратуры Казахстана в сфере защиты персональных данных, значительная работа в этом направлении все же проводится, но тактика и методика, отражающие характер и специфику прокурорского надзора в сфере защиты персональных данных, еще окончательно не выработаны.

Деятельность органов прокуратуры в Республике Казахстан основана на общих принципах, закрепленных Конституцией и Конституционным законом «О прокуратуре», которые применимы абсолютно ко всем отраслям, направлениям и видам прокурорского надзора, в том числе в сфере защиты персональных данных. При этом надзор в каком-либо определенном направлении, к примеру, в сфере защиты персональных данных может осуществляться по всем отраслям прокурорского надзора. Иными словами прокурор может уделять внимание вопросу защиты персональных данных, осуществляя надзор как за законностью деятельности государственных органов и иных организаций, а так и за законностью производства по делам об административных правонарушениях, досудебного расследования, исполнительного производства и другим отраслям прокурорского надзора.

При этом для эффективной реализации прокурорского надзора в сфере защиты персональных данных важно определение характерных именно для данного направления принципов.

Для защиты персональных данных прокуроры наделены обширным арсеналом правовых средств, к которым можно отнести правовые средства прокурорского надзора, правовые средства представления интересов

государства в суде, правовые средства уголовного преследования от имени государства, правовые средства по координации и взаимодействию, а также правовые средства реализации иных полномочий прокурора.

Основными правовыми средствами и инструментами прокурорского надзора в сфере защиты персональных данных являются проверка соблюдения законности, анализ состояния законности, а также оценка, актов вступивших в законную силу. При этом для защиты персональных данных целесообразно применение всего потенциала правовых средств прокурора, в том числе по координации, межведомственному сотрудничеству и участию в нормотворческой деятельности.

Органы прокуратуры Казахстана достаточно активно используют в работе современные технологии, их применение для осуществления надзора в сфере защиты персональных данных имеет значительные перспективы, в особенности для исключения «человеческого фактора» при использовании информационных систем и баз персональных данных, противодействия телефонным звонкам с подменных номеров, выявления и пресечения деятельности приложений и сайтов, целью которых является незаконный сбор или похищение персональных данных.

Основываясь на результатах проведенного исследования, можно сделать вывод, что прокурорский надзор в сфере защиты персональных данных в Республике Казахстан является важным направлением прокурорской деятельности и эффективным правовым инструментом, направленным на защиту персональных данных и недопустимость необоснованного вмешательства в частную жизнь.

В завершении следует отметить, что поставленные цели достигнуты в полном объеме, а вытекающие из них задачи успешно решены. Полученные результаты докторской диссертации могут стать основой для продолжения научного исследования вопроса защиты персональных данных и прокурорского надзора. Результаты значимы для дальнейшего совершенствования законодательства Республики Казахстан. Работа может быть использована докторантами, магистрантами и студентами юридических факультетов в качестве дополнительного пособия при изучении курса прокурорского надзора, информационной безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 К 2025 году в мире будет храниться 200 зеттабайт данных // https://newsletter.radensa.ru/archives/5781. 20.09.2024.

2 Top 10 Cybersecurity Predictions And Statistics For 2024 // https://cybersecurityventures.com/top-5-cybersecurity-facts-figures. 18.05.2024.

3 Air Astana и «Казахтелеком» заплатят штрафы за утечку персональных данных казахстанцев // https://kz.kursiv.media/2024-04-01/pnkr-shtrf/. 05.06.2024.

4 Сообщается о новой масштабной утечке персональных данных казахстанцев // https://kaztag.kz/ru/news/soobshchaetsya-o-novoy.a: 08.08.2024.

5 Утечки конфиденциальных данных из организаций – 1-е полугодие 2024 // https://www.ptsecurity.com/ru-ru/research/analytics/utechki. 10.08.2024.

6 Digital 2023: Kazakhstan // https://datareportal.com/reports. 20.03.2023.

7 UN E-Government Knowledgebase // https://publicadministration. 24.09.2023.

8 Рейтинг электронного правительства ООН (EGDI) // https://www.tadviser.ru/index.php. 02.10.2023.

9 Указ Президента Республики Казахстан. О Государственной программе формирования «электронного правительства» в Республике Казахстан на 2005-2007 годы: утв. 10 ноября 2004 года, №1471 (утратил силу) // https://adilet.zan.kz/rus/docs/U040001471_. 12.03.2024.

10 Более 20 миллионов госуслуг получили казахстанцы через eGov и eGov Mobile за первую половину 2024 года // https://www.nitec.kz/index.php/ru/news/bolee-20-millionov-gosuslug. 09.09.2024.

11 Smart Bridge // https://www.nitec.kz/ru/proekty/smart-bridge. 10.07.2024.

12 Результаты анализа защищенности веб-ресурсов государственных организаций Республики Казахстана (2020) // https://cert.kz. 10.02.2024.

13 В Казахстане заявили об отражении 163,4 млн. кибератак на ресурсы госорганов с начала года // https://tass.ru/mezhdunarodnaya-panorama. 12.10.2023.

14 Identity Fraud Losses Total $52 Billion in 2021, Impacting 42 Million U.S. Adults // https://www.globenewswire.com/news-release. 18.09.2023.

15 Имангалиев Н.К., Темиржанова Л.А. Актуальные проблемы выявления и раскрытия уголовных правонарушений, совершаемых в сети Интернет // Л.Н. Гумилев атындағы Еуразия ұлттық университетінің Хабаршысы. - 2022. - №1(138). – С. 124-132.

16 Издержки цифровизации: кибермошенничество // https://t.me/s/socioexpert_01.12.2023.

17 Постановление Правительства Республики Казахстан. Об утверждении Концепции развития искусственного интеллекта на 2024-2029 годы: утв. 24 июля 2024 года, №592 // https://adilet.zan.kz/rus/docs/P2400000592. 10.10.2024.

18 Identity Fraud Report 2024 // https://onfido.com/landing. 18.06.2024.

19 Добробаба М.Б. Дипфейки как угроза правам человека // Lex Russica. – 2022. - №11(192). – С. 112-119.

20 Частное постановление Алмалинского районного суда г. Алматы №1-673/2019 от 02.04.2019 года. – Алматы, 2019 (ДСП).

21 Ендольцева А.В., Ендольцева Ю.В. Механизм противодействия бесконтрольному распространению персональных данных, способствующему совершению преступных посягательств на права и законные интересы субъектов персональных данных // Вестник Уфимского юридического института МВД России. - 2023. - №3(101). - С. 67-73.

22 Конституция Республики Казахстан: принят 28 января 1993 года (утратила силу) // https://adilet.zan.kz/rus/docs/K930001000_. 12.06.2024.

23 Конституция Республики Казахстан: принят 30 августа 1995 года // https://adilet.zan.kz/rus/docs/K950001000_. 12.07.2024.

24 Неприкосновенность частной жизни / под ред. Г.К. Шушиковой. – Нур-Султан, 2020. – 195 с.

25 Закон Республики Казахстан. О персональных данных и их защите: принят 21 мая 2013 года, №94-V // https://adilet.zan.kz/rus/docs. 24.02.2023.

26 Комаров С.А., Мицкая Е.В. Правовое регулирование обеспечения информационной безопасности и защиты персональных данных: монография. – СПб., 2018. - 168 с.

27 Высокоуровневый сравнительный анализ правовых режимов обработки и защиты персональных данных в государствах-членах ЕАЭС // https://rppa.ru/analitika/pdn_v_eaehs. 12.06.2023.

28 Chart of signatures and ratifications of Treaty 108 // https://www.coe.int/en/web/conventions/full-list?module=signatures-by. 2.05.2023.

29 Амиров А.М. К вопросу о современном состоянии законодательства в сфере защиты персональных данных (по материалам Республики Казахстан) // Расследование преступлений: проблемы и пути их решения. – 2023. – №1(39). – С. 143-151.

30 Постановление Правительства Республики Казахстан. Об утверждении Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023-2029 годы: утв. 28 марта 2023 года, №269 // https://adilet.zan.kz/rus/docs. 20.10.2024.

31 Сикач М.С. Особенности правового регулирования международной правовой помощи по административным вопросам в странах СНГ // Регулирование правоотношений: проблемы теории и практики: матер. 11-й всеросс. науч.-практ. конф. аспир., соиск., магистр. и мол. учен. в режиме видео-конф.-связи. – М., 2022. – С. 98-106.

32 Петрыкина Н.И. Персональные данные личности: учеб. пос. – М., 2012. – 98 с.

33 Акилов С.А. Международно-правовая регламентация защиты персональных данных в глобальной сети Интернет // Журнал правовых исследований. - 2023. - №1. - С. 88-97.

34 Сравнение законодательства о защите персональных данных в России и за рубежом // https://drc.law/blog/sravnenie-zakonodatelstva. 17.11.2023.

35 Иванский В.П. Правовое регулирование персональных данных в законодательстве зарубежных государств // Вестник Российского университета дружбы народов. Серия: Юридические науки. - 2012. - №1. – С. 156-168.

36 Дудко М.О. Понятие «персональные данные» в современном праве // Вестник Гродненского государственного университета имени Янки Купалы. Серия 4. Правоведение. - 2020. - №10(3). – С. 14-22.

37 Писарев В.В. Эволюция правового регулирования оборота персональных данных в США на примере штата Нью-Йорк // Право: история, теория, практика: сб. матер. 4-й междунар. очно-заоч. науч.-практ. конф. – М., 2022. – С. 78-87.

38 Омурчиева Э.М., Саудабаева Д.Е. Проблемы применения законодательства Республики Казахстан о персональных данных: риски для работодателя // Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan. – 2024. - №2(77). - С. 111-121.

39 Гаджиева К.А. Гармонизация правового поля стран ЕАЭС в области защиты персональных данных // Бизнес. Образование. Право. - 2021. - №2(55). - С. 258-262.

40 Добробаба М.Б. Понятие персональных данных: проблема правовой определенности // Вестник Университета имени О.Е. Кутафина. - 2023. - №2(102). – С. 42-52.

41 Рузанова В.Д.. Персональные данные как гражданско-правовая категория // Правовое государство: теория и практика. – 2022. - №3(69). – С. 77-83.

42 Жетписов С.К., Алибаева Г.А., Дубовицкая О.Б. Цифрландыру дәуіріндегі дербес деректерді қорғау: конституциялық-құқықтық аспект // Вестник Института законодательства и правовой информации Республики Казахстан. – 2023. - №3(74). – С. 68-76.

43 Ответ Министра внутренних дел Республики Казахстан от 7 декабря 2019 года на вопрос от 26 ноября 2019 года, №582584 // https://online.zakon.kz/Document/?doc_id=35885019. 05.08.2024.

44 Закон Республики Казахстан. О дактилоскопической и геномной регистрации: принят 30 декабря 2016 года, №40-VI ЗРК // https://adilet.zan.kz/rus/docs/Z1600000040. 10.10.2024.

45 Федеральный закон Российской Федерации. О персональных данных: принят 27 июля 2006 года, №152-ФЗ // https://www.consultant.ru. 28.05.2023.

46 Указ Президента Российской Федерации. Об утверждении Перечня сведений конфиденциального характера: утв. 6 марта 1997 года, №188 // https://www.consultant.ru/document/cons_doc_LAW_13532/. 30.05.2023.

47 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data // https://www.coe.int/en/web. 24.03.2024.

48 Алихаджиева И.С. Судимость как персональные данные и основание общеправовых ограничений // Известия Юго-Западного государственного университета. Серия: История и право. - 2024. - №1(14). - С. 65-79.

49 Singh G., Bhardwaj G., Singh S.V., Garg V. Biometric Identification System: Security and Privacy Concern // Artificial Intelligence for a Sustainable Industry 4.0. – 2021. – Pp. 245-264.

50 De Keyser A., Bart Y., Gu X., Liu S.Q., Robinson S.G., Kannan P.K. Opportunities and challenges of using biometrics for business: Developing a research agenda // Journal of Business Research. – 2021. - № 136. – Pp. 52-62.

51 Ioannou A., Tussyadiah I., Lu Y. Privacy concerns and disclosure of biometric and behavioral data for travel // https://www.sciencedirect.com. 15.04.2023.

52 Smith M., Miller S. The ethical application of biometric facial recognition technology // AI & Soc. – 2022. - №37. – P. 167-175.

53 Закон Республики Казахстан. О платежах и платежных системах: принят 26 июля 2016 года, №11-VI // https://adilet.zan.kz/rus/docs. 24.10.2024.

54 Закон Республики Казахстан. О банках и банковской деятельности в Республике Казахстан: принят 31 августа 1995 года, №2444 // https://adilet.zan.kz/rus/docs/Z950002444_. 25.10.2024.

55 Закон Республики Казахстан. О микрофинансовой деятельности: принят 26 ноября 2012 года, №56-V // https://adilet.zan.kz/rus. 20.10.2024.

56 Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка. Об утверждении Правил проведения биометрической идентификации банками, организациями, осуществляющими отдельные виды банковских услуг, и микрофинансовыми организациями: утв. 16 августа 2024 года, №56 // https://adilet.zan.kz/rus/docs/V2400034950. 10.10.2024.

57 Постановление Правительства Республики Казахстан. Об утверждении Соглашения о сотрудничестве в создании государственных информационных систем паспортно-визовых документов нового поколения и дальнейшем их развитии и использовании в государствах-участниках СНГ: утв. 30 марта 2009 года, №430 // https://adilet.zan.kz/rus/docs/P090000430_. 08.09.2024.

58 Кодашева Г.С. Удаленная биометрическая идентификация в банковской сфере Казахстана как часть цифровой инфраструктуры // Сб. матер. междунар. науч.-практ. конф. «Финансовые аспекты третьей модернизации экономики Казахстана». – Нур-Султан, 2021. - С. 405-413.

59 Грушин Ф.В., Сивцова А.Ю. Фотоизображение и описание примет осужденных к лишению свободы как вид персональных данных, подлежащих обработке в уголовно-исполнительной системе России // Вестник Самарского юридического института. - 2022. - №1(47). - С. 45-51.

60 Бахтеев Д.В., Леднёв И.В. Понятие и свойства криминалистического профилирования личности и поведения неизвестного преступника // Юрид. наука и правоохранительная практика. - 2020. - №3(53). – С. 110-118.

61 Закон Республики Казахстан. Об онлайн-платформах и онлайн-рекламе: принят 10 июля 2023 года, №18-VIII ЗРК // https://adilet.zan.kz/rus/docs/Z2300000018. 12.02.2024.

62 Проект постановления Правительства Республики Казахстан. Об утверждении Программы создания Национальной платформы цифровой биометрической идентификации на 2022-2024 годы // https://legalacts.egov.kz/npa/view?id=14023459. 09.09.2024.

63 Письмо Комитета по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 6 мая 2024 года, №ЖТ-2023-03797577 // https://online.zakon.kz/Document/?doc_id=32359056. 5.08.2024.

64 Журсимбаев С.К. Прокурорский надзор в Республике Казахстан. – Изд. 3-е, перер. и доп. – Алматы, 2020. – 336 с.

65 Особенности организации прокурорского надзора в чрезвычайных и иных кризисных ситуациях: монография / под ред. Г.К. Шушиковой. – Косшы, 2022. – 164 с.

66 Настольная книга прокурора: в 14 т. / под ред. С.Г. Кехлерова, О.С. Капинус. – М., 2013. – Т. 2. – 271 с.

67 Толеубекова Б.Х., Хведелидзе Т.Б. Функции прокуратуры и их дифференциация по законодательству Республики Казахстан // Журнал зарубежного законодательства и сравнительного правоведения. - 2021. - №17(5). - С. 16-22.

68 Ахметова А.Б. Конституционно-правовые основы организации и деятельности прокуратуры в Российской Федерации и Республики Казахстан: сравнительно-правовой анализ: автореф. … канд. юрид. наук: 12.00.02. – М., 2015. – 26 с.

69 Статус прокуратуры в государствах-участниках Содружества Независимых Государств: монография / под ред. Г.К. Шушиковой. – Алматы, 2024. – 154 с.

70 Прокуратура в зарубежных странах: учеб. пос. / сост. М.К. Адильханов и др. – Алматы, 2019. – 210 с.

71 Закон Республики Казахстан. О Прокуратуре: принят 21 декабря 1995 года, №2709 (утратил силу) // https://adilet.zan.kz/rus/docs. 18.12.2022.

72 Закон Республики Казахстан. О Прокуратуре: принят 30 июня 2017 года, №81-VI // https://adilet.zan.kz/rus/docs/Z1700000081. 28.12.2022.

73 Конституционный закон Республики Казахстан. О прокуратуре: принят 5 ноября 2022 года, №155-VII ЗРК // https://adilet.zan.kz. 03.03.2023.

74 Винокуров Ю.Е. и др. Прокурорский надзор: учеб. – Изд. 6-е, перер. и доп. – М.: Высшее образование, 2006. – 460 с.

75 Хведелидзе Т.Б., Толеубекова Б.Х. Принцип законности в организации и деятельности органов прокуратуры Республики Казахстан // Юриспруденция в теории и на практике: актуальные вопросы и современные аспекты: сб. ст. 8-й междунар. науч.-практ. конф. – Пенза, 2021. – С. 61-64.

76 Алибеков А.Е. Принципы участия прокурора в гражданском процессе (на примере Республики Казахстан) // Юридическая наука. - 2021. - №3. – С. 110-116.

77 Воронин О.В. О сущности современного прокурорского надзора // Уголовная юстиция. - 2018. - №11. – С. 183-189.

78 Сулейманов Т.А. Прокурорский надзор в пенитенциарной сфере - особый вид правоохранительной деятельности государственного аппарата // Modern Science. – 2022. – №5-3. – С. 198-203.

79 Бородина А.В. К вопросу об организации прокурорского надзора за исполнением законов // Вопросы росс. юстиции. – 2022. – №18. – С. 503-510.

80 Челпанова М.М. Правовое регулирование осуществления прокурорского надзора за исполнением законодательства об охране окружающей среды // Крымские юридические чтения. Прокуратура России: в преддверии 300-летия: сб. матер. всеросс. науч.-практ. конф. – Симферополь, 2021. – С. 197-202.

81 Закон Республики Казахстан. О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий: принят 25 июня 2020 года, №347-VI ЗРК // https://adilet.zan.kz/rus/docs/Z2000000347. 28.04.2023.

82 Постановление Правительства Республики Казахстан. О внесении изменений и дополнений в некоторые решения Правительства Республики Казахстан: утв. 18 января 2021 года, №12 // https://adilet.zan.kz/rus. 20.04.2023.

83 Баканов К.С., Шпорт С.В. Полномочия прокуратуры по допуску к сведениям о состоянии здоровья водителей транспортных средств // Социальная и клиническая психиатрия. - 2021. - №31(3). – С. 96-103.

84 Саушкин С.О. Органы прокуратуры в системе защиты права граждан на неприкосновенность частной жизни при обработке персональных данных // Цифровая наука. – 2020. - №5. - С. 251-257.

85 Структура органов прокуратуры / Генеральная прокуратура Российской Федерации // https://epp.genproc.gov.ru/web/gprf/. 20.11.2022.

86 Бессчасный С.А. Цифровая трансформация органов прокуратуры Российской Федерации // Прокуратура: история и современность - 300 лет прокуратуре России (Сухаревские чтения). – М., 2022. – С. 16-25.

87 Идрышева С.К. О Цифровом кодексе Казахстана // Право и государство. - 2022. - №3(96). – С. 72-87.

88 Приказ Генерального Прокурора Республики Казахстан. О некоторых вопросах организации прокурорского надзора и контроля в сфере правовой статистики и специальных учетов: принят 5 января 2022 года, №4 // https://adilet.zan.kz/rus/docs/V2200026483. 28.09.2023.

89 Закон Республики Казахстан. О государственной правовой статистике и специальных учетах: принят 22 декабря 2003 года, №510 // https://adilet.zan.kz/rus/docs/Z030000510_#z1. 20.09.2023.

90 Приказ Генерального Прокурора Республики Казахстан. Об утверждении Инструкции по информационно-справочному обслуживанию физических и юридических лиц органами правовой статистики и специальных учетов: утв. 5 января 2023 года, №7 // https://adilet.zan.kz/rus/docs. 22.09.2023.

91 Махьянова Р.М. Методологические подходы к формированию концепции тактики прокурорского надзора // Юридическая наука. - 2024. - №7. – С. 72-75.

92 Воронин О.В. О современном понимании понятий «правовые средства прокурорского надзора» и «формы реализации правовых средств прокурорского надзора» // Вестник Томского государственного университета. Право. - 2021. - №39. – С. 5-14.

93 Ергашев Е.Р., Габышева Е.А. Правовые средства прокурора: проблемы осмысления, применения и правового регулирования // Российское право: образование, практика, наука. - 2018. - №5(107). – С. 38-44.

94 Ахметова А.Б. Сравнительный анализ конституционно-правового статуса прокуратуры в Республике Казахстан и Российской Федерации // Известия высших учебных заведений. Поволжский регион. Общественные науки. - 2014. - №1(29). – С. 61-67.

95 Абдиров Н.М. Координация органами прокуратуры деятельности правоохранительных и иных государственных органов по обеспечению законности, правопорядка и борьбы с преступностью в Республике Казахстан: учеб. пос. – Караганда, 2024. – 195 с.

96 О работе прокурора по надзору за законностью в социально-экономической сфере. Раздел 1. Правовая статистика: стат. отчеты // https://qamqor.gov.kz/crimestat/statistics. 02.11.2024.

97 Приказ Генерального Прокурора Республики Казахстан. О некоторых вопросах организации прокурорского надзора: утв. 17 января 2023 года, №32 // https://adilet.zan.kz/rus/docs/V2300031753. 18.10.2023.

98 Майлыбаев А.С. Нормативно-правовые акты как основа прокурорского надзора // Передовое развитие современной науки: опыт, проблемы, прогнозы: сб. ст. 9-й междунар. науч.-практ. конф. – Петрозаводск, 2022. – С. 64-69.

99 Сейткасимова И.Н., Кенбаев Д.Х., Елемесов Ж.Ф. и др. Методические рекомендации по расследованию финансовых аспектов преступной деятельности (проведение параллельного финансового расследования). – Косшы, 2022. – 33 с.

100 Уголовно-процессуальный кодекс Республики Казахстан: принят 4 июля 2014 года, №231-V ЗРК // https://adilet.zan.kz/rus/docs. 06.11.2023.

101 Кодекс Республики Казахстан об административных правонарушениях: принят 30 января 2001 года, №155 (утратил силу) // https://adilet.zan.kz/rus/docs/K010000155_. 12.06.2023.

102 Кодекс Республики Казахстан об административных правонарушениях: принят 5 июля 2014 года, №235-V ЗРК // https://adilet.zan.kz/rus/docs/K1400000235. 18.08.2023.

103 Более 1400 жалоб поступило от граждан в МЦРИАП РК // https://www.gov.kz/memleket/entities/mdai/press/news/details/724283?. 20.03.2024.

104 Закон Республики Казахстан. О связи: принят 5 июля 2004 года, №567 // https://adilet.zan.kz/rus/docs/Z040000567_#z1. 20.04.2024.

105 Что такое Кибернадзор? // https://drfl.kz/ru/cybernadzor/. 5.02.2024.

106 Потапова Л.В., Британов А.И. Проверочное мероприятие как инструмент надзорной деятельности прокуратуры: нормативно-правовой анализ // Юридическая наука. - 2023. - №9. – С. 59-61.

107 Потапова Л.В. К вопросу о прокурорской проверке исполнения законов: матрица аспектов восприятия // Право и государство: теория и практика. - 2021. - №11(203). - С. 163-165.

108 Солдатова В.И. Защита персональных данных в условиях применения цифровых технологий // Lex russica. – 2020. – №2(159). – С. 33-43.

109 Введение Face ID в поликлиниках: в Минздраве заявили о снижении количества приписок // https://www.kt.kz/rus/medicine/vvedenie_. 20.10.2024.

110 Шабаров Д.В. Анализ состояния законности в прокурорской деятельности: теория и практика // Ленинградский юридический журнал. – 2022. – №2(68). – С. 158-169.

111 Карпышева Ю.О. Результаты анализа состояния законности как основание проведения прокурорской проверки исполнения законов // Проблемы совершенствования прокурорской деятельности и правоприменительной практики: сб. ст. – Иркутск, 2020. – Вып. 10. – С. 25-32.

112 Представление прокурора Балхашского района Алматинской области об устранении нарушений законности в адрес акима Балхашского района Алматиснкой области от 28.03.2023 года №2-04-23-00275. – Балхаш, 2024 (ДСП).

113 Пузиков Р.В., Абишев Б.С. Роль прокурора в вопросах нормотворческой деятельности на региональном уровне // Право и государство: теория и практика. – 2023. – №11(227). – С. 32-35.

114 Телина Ю.С. Конституционное право гражданина на неприкосновенность частной жизни, личную и семейную тайну при обработке персональных данных в России и зарубежных странах: дис. … канд. юрид. наук: 12.00.02. – М., 2016. – 267 с.

115 Тлесова Э.Б. Цифровизация здравоохранения в Республике Казахстан // Россия и Азия. – 2020. – №5(14). – С. 6-13.

116 Аубакирова Г.М., Исатаева Ф.М. Цифровизация промышленных предприятий Казахстана: потенциальные возможности и перспективы // Вопросы инновационной экономики. – 2020. – №4(10). – С. 2251-2268.

117 Пашков С.В. Цифровизация земледелия в Казахстане: региональный опыт // Географический вестник. – 2021. – №4(59). – С. 27-41.

118 Сарпеков Р.К. Цифровизация правового пространства // Вестник Института законодательства и правовой информации Республики Казахстан. – 2020. – №4(62). – С. 12-24.

119 Воробьев А.Е. Цифровизация нефтяной отрасли Казахстана // Проблемы недропользования. – 2018. – №1(16). – С. 66-75.

120 Сарсенбиева Н.Ф. Цифровизация образования в Республике Казахстан // Мир педагогики и психологии. – 2021. – №1(54). – С. 33-37.

121 Синкевич В.В. Цифровизация уголовного процесса: зарубежный и отечественный опыт // Вестник Волгоградской академии МВД России. – 2022. – №1(60). – С. 129-134.

122 Указ Президента Республики Казахстан. Об утверждении Стратегического плана развития Республики Казахстан до 2025 года и признании утратившими силу некоторых указов Президента Республики Казахстан»: утв. 15 февраля 2018 года, №636 (утратил силу) // https://adilet.zan.kz/rus/archive/docs/U1800000636/15.02.2018. 10.10.2024.

123 Президент Республики Казахстан К.-Ж. Токаев. Справедливый Казахстан: закон и порядок, экономический рост, общественный оптимизм: послание народу Казахстана // https://www.akorda.kz/ru. 10.09.2024.

124 Тлембаева Ж.У. О некоторых вопросах правового регулирования использования технологии искусственного интеллекта в условиях цифровой трансформации // Вестник Воронежского государственного университета. Серия: Право. – 2021. – №4(47). – С. 331-349.

125 Грачева Ю.В., Арямов А.А. Роботизация и искусственный интеллект: уголовно-правовые риски в сфере общественной безопасности // Актуальные проблемы российского права. – 2020. – №6(115). – С. 169-178.

126 Дулатбеков Н.О., Бачурин С.Н. Теоретические предпосылки применения инструментов искусственного интеллекта при реализации трехзвенной модели судебной и правоохранительной деятельности в Республике Казахстан // Bulletin of the Karaganda University “Law Series”. – 2024. – №3(11529). – С. 59-69.

127 Глава государства принял Генерального прокурора Берика Асылова // https://www.akorda.kz/ru/glava-gosudarstva-prinyal-generalnogo. 06.06.2024.

128 В Алматы и Атырау внедрили «умные» камеры с ИИ // https://digitalbusiness.kz/2024-08-06/v-almati-i-atirau-vnedrili-umnie. 14.08.2024.

129 Гречаный С.А. Распознавание лиц в современных системах видеонаблюдения: на примере оборудования ТМ // Охрана, безопасность, связь. – 2020. – №5-1. – С. 63-68.

130 Лукьянчиков А.И. Принцип работы систем распознавания лиц и особенности их применения при обработке видеопотока в реальном времени // Информатика и вычислительная техника и управление. Серия: Естественные и технические науки. – 2023. – №5. – С. 76-83.

131 Яцуценко В.В. Проблемы и перспективы внедрения цифровых технологий в деятельность органов прокуратуры // Актуальные проблемы российского права. – 2021. – №11(132). – С. 187-193.

132 Карпышева Ю.О. О возможностях использования искусственного интеллекта и иных информационных технологий в деятельности прокурора по надзору за исполнением законов // NB: Административное право и практика администрирования. – 2023. – №4. – С. 15-23.

133 Махьянова Р.М. Использование технологий искусственного интеллекта при осуществлении надзорной деятельности прокуратуры // Юридическая наука. – 2024. – №1. – С. 195-199.

134 Результаты проверки в правоохранительных и государственных органах на предмет законности и обоснованности получения данных из информационной системы СИО ПСО. – Астана, 2023 (ДСП).

135 Приказ Генерального Прокурора Республики Казахстан. Об утверждении Правил формирования, доступа, использования, хранения, защиты и уничтожения сведений из системы информационного обмена правоохранительных, специальных государственных и иных органов: утв. 13 января 2023 года, №21 // https://adilet.zan.kz/rus/docs. 30.08.2024.

136 Амиров А.М., Бегалиев Е.Н., Баймаханов А.А. и др. Обеспечение защиты персональных данных путём чипирования отдельных категорий лиц: научный обзор // Судебная медицина. – 2024. – №1(10). – С. 56-67.

137 Пахомов В.Н. Проблемы защиты интеллектуальной собственности в Интернете // Актуальные проблемы становления и развития правовой системы российской Федерации: сб. докл. 6-й всеросс. науч.-практ. конф. студ., магистр. и аспир. – Сыктывкар, 2022. – С. 140-143.

138 Сырбу А.В. Организация и производство судебно-компьютерной экспертизы: учеб. пос. – Караганда. 2010. – 114 с.

139 Аристархов А.Л., Камчатов К.В. и др. Прокурорский надзор за исполнением законов органами предварительного расследования при выявлении и расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий: науч.-практ. пос. – М., 2023. – 122 с.

140 Сычева А.В. О способах совершения мошенничеств посредством социальной инженерии в современных условиях и методах их предупреждения // Вест. Волгоградской академии МВД России. – 2022. – №4(63). – С. 127-132.

141 Карабеков К.О. Состояние и тенденции киберпреступности в Российской Федерации и Республике Казахстан // Научный вестник Омской академии МВД России. – 2024. – №30(2(93). – С. 106-112.

142 О запуске Антифрод-центра по обмену данными о мошеннических транзакциях // https://nationalbank.kz/ru/news. 12.09.2024.

143 Проект приказа «Об утверждении правил оказания услуг связи» // https://legalacts.egov.kz/npa/view?id=15183499. 22.10.2024.

144 Warren S.D., Brandeis L.D. The Right to Privacy // Harvard Law Review. – 1890. – Vol. 5, Issue 4. – P. 193-220.

145 Всеобщая декларация прав человека: утв. резолюцией Генеральной Ассамблеи ООН от 10 декабря 1948 года // https://www.un.org/ru/. 02.05.2024.

146 Конвенция о защите прав человека и основных свобод от 4 ноября 1950 года // https://www.echr.coe.int/documents/d/echr/Convention_. 03.05.2024.

147 Международный пакт о гражданских и политических правах: утв. резолюцией Генеральной Ассамблеи ООН от 16 декабря 1966 года // https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml. 03.05.2024.

148 Privacy, Data Protection and Cybersecurity: Germany – Lexology https://thelawreviews.co.uk/title/the-privacy-data-protection-and. 02.04.2024.

149 U.S. Privacy Laws: The Complete Guide // https://www.varonis.com/blog/us-privacy-laws. 04.03.2024.

150 Data Protection in Austria – GDPRhub // https://gdprhub.eu/Data_Protection_in_Austria. 04.04.2024.

151 Конституция Словацкой Республики // https://legalns.com. 01.03.2024.

152 Конституция Чешской Республики // https://legalns.com. 01.03.2024.

153 О защите физических лиц при обработке персональных данных и о свободном обращении таких данных: директива: утв. Европейским парламентом и Советом Европейского Союза от 24 октября 1995 года, №95/46/ЕС // https://online.zakon.kz/Document/?doc_id=31067635. 4.042024.

154 Хартия Европейского союза об Основных правах // https://eulaw.ru/treaties/charter/. 24.03.2024.

155 General Data Protection Regulation // https://ogdpr.eu/ru. 18.05.2024.

156 Важорова М.А. Соотношение понятий «Информация о частной жизни» и «Персональные данные» // Вест. СГЮА. – 2012. – №4(87). – С. 55-59.

157 Оганесян Т.Д. Право на защиту персональных данных: исторический аспект и современная концептуализация в эпоху Big Data // Журнал зарубежного законодательства и сравнительного правоведения. – 2020. – №2. – С. 48-63.

158 Исследование ООН / Электронное правительство 2022 // https://desapublications.un.org/sites/default/files/publications/2023-02. 02.10.2024.

159 Исмагилова О.Д., Хаджи К.Р. Мировой опыт регулирования защиты, передачи и хранения данных // Экономическая политика. – 2020. – №15(3). – С. 152-175.

160 General Personal Data Protection Act of Brazil // https://lgpd-brazil.info/. 18.04.2023.

161 Souza J. et al. The General Law Principles for Protection the Personal Data and their Importance // In Computer Science & Information Technology (CS & IT). – 2020. – Vol. 11, Issue 10. – P. 109-120.

162 Özkan Ö., Şahinol M. Reflections on Turkish Personal Data Protection Law and Genetic Data in Focus Group Discussions // NanoEthics. – 2023. – №16. – P. 297-312.

163 Klosowski T. The State of Consumer Data Privacy Laws in the US (And Why It Matters) // https://www.nytimes.com/wirecutter/blog/state-of. 20.05.2023.

164 Case of Amann v. Switzerland, App. No.27798/95 (1992, march) // http://hudoc.echr.coe.int/eng?i=001-58497. 21.11.2023.

165 Case of Leander v. Sweden, App. No.9248/81 (1987, march) // http://hudoc.echr.coe.int/eng?i=001-57519. 28.11.2023.

166 Case of Rotaru v. Romania, App. No.28341/95 (1995, february) // http://hudoc.echr.coe.int/eng?i=001-58586. 11.11.2023.

167 Амиров А.М. О некоторых подходах зарубежных государств к вопросу защиты персональных данных // Вестник Академии правоохранительных органов. – 2024. – №2(32). – С. 253-261.

168 Mangku D. et al. The personal data protection of internet users in Indonesia // Journal of Southwest Jiatong University. – 2020. – Vol. 1. – P. 202-209.

169 Fibrianti N., Holish A. Consumer Personal Data Protection: Between Expectations and Reality // https://www.academia.edu/82613948. 24.112023.

170 Tataru G., Tataru S. Human resources and personal data protection: an indissoluble relationship // Journal of Public Administration, Finance and Law. – 2021. – Vol. 9, Issue 18. – P. 303-311.

171 Mittelstadt B. Personal Data Protection // https://www.academia.edu. 11.01.2024.

172 Justickis V. Balancing Personal Data Protection with Other Human Rights and Public Interest: Between Theory and Practice // Baltic Journal of Law & Politics. – 2020. – Vol. 13. – P. 140-162.

173 Labadie C., Legnera C. Personal data management inside and out // https://www.researchgate.net/publication/346507194_Personal_data_. 18.11.2023.

174 Sun Z., Liu Z. Inadequacy and Improvement of Legal Protection of Sensitive Personal Information // SHS Web of Conferences. – 2023. – Vol. 157. – P. 03006-1-03006-4.

175 Carvalho R. et al. Protecting Citizens' Personal Data and Privacy: Joint Efort from GDPR EU Cluster Research Projects // SN Computer Science. – 2020. – Vol. 1, Issue 217. – P. 1-16.

176 Obiagwu W. How the GDPR protects personal data in the digital age // ELSA Austria Law Review. – 2022. – Vol. 7. – P. 25-31.

177 Grafenstein M., Jakobi T., Stevens G. Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-Centred UX-design methods // Computer Law & Security Review. – 2022. – Vol. 46. – P. 1-22.

178 Quach S. Digital technologies: tensions in privacy and data // Journal of the Academy of Marketing Science. – 2022. – №50. – P. 1299-1323.

179 Ducato R. Data protection, scientific research, and the role of information // Computer Law & Security Review. – 2020. – Vol. 37. – P. 1-16.

180 Mateeva Z. Principles of personal data protection // Audit 2. – 2020. – Vol. 28. – P. 95-104.

181 Соколова М.Е. Первые успехи нового европейского общего Регламента по защите персональных данных // Современная Европа. – 2020. – №2. – С. 56-66.

182 Бисалиев М., Шакиров К. Цифровые следы как фактор безопасности оборота персональных данных в сети Интернет // Вестник Евразийского Национального университета имени Л.Н. Гумилева. – 2023. – №1. – С. 81-98.

183 Прокопенко А.Н. Борьба с утечками персональных данных – поможет ли ужесточение ответственности? // Вестник Казанского юридического института МВД России. – 2024. – №15((56). – С. 48-56.

184 Семейный кодекс Украины: принят 10 января 2002 года №2947-III // https://online.zakon.kz/Document/?doc_id=30418309&pos. 30.10.2024.

185 Чекулаев С.С. Медицинское обследование лиц, вступающих в брак // Аллея науки. – 2018. – Т. 2, №1(17). – С. 619-624.

186 Из-за чего в Казахстане каждая шестая семья разводится // https://tengrinews.kz/kazakhstan_news/iz-za-chego-v-kazahstane. 29.10.2024.

187 Нетрадиционная сексуальная ориентация одного из супругов вошла в топ 5 причин разводов в Казахстане // https://www.nur.kz/society. 29.10.2024.

188 Кодекс Республики Казахстан. О браке (супружестве) и семье: принят 26 декабря 2011 года, №518-IV // https://adilet.zan.kz/rus/docs. 30.10.2024.

189 Максутов Б.М. Деятельность независимого органа по защите персональных данных в Республике Казахстан // International scientific review of the problems of law, sociology and political science: col. of scient. artic. 9th internat. correspond. scient. special. conf. – Boston, 2019. – С. 56-68.

190 Каирбаева Л.К. Защита персональных данных в международном и европейском праве // Вестник Института законодательства и правовой информации Республики Казахстан. – 2020. – №5(63). – С. 168-174.

191 Халиков А.Н. Институт негласных следственных действий в уголовно-процессуальном законе России и стран ближнего зарубежья (сравнительно-правовое исследование) // Правовое государство: теория и практика. – 2024. – №1(75). – С. 142-150.

192 Захарцев С.И., Кирюшкина Н.О. Основы организации прокурорского надзора за оперативно-розыскной деятельностью // Юридическая наука: история и современность. – 2015. – №8. – С. 137-148.

193 Приговор районного суда №2 Алматинского района города Нур-Султан № 7116-20-00-1/456 от 22.12.2020 года (текущее делопроизводство).

194 Халиуллина Э.Т. Коррупционные проявления в сфере противодействия преступлениям, совершаемым с использованием персональных данных // Регулирование правоотношений в условиях цифровизации в период пандемии: современное состояние и перспективы развития: сб. ст. – Казань, 2021. – С. 434-438.

195 Бут Н.Д. и др. Прокурорский надзор за соблюдением прав граждан на охрану здоровья и медицинскую помощь: науч.-практ. пос. – М., 2022. – 132 с.

196 Иванченко Е.А. Содержание предмета прокурорского надзора за соблюдением законодательства в сфере организации фармацевтической деятельности // Современные проблемы экономики, права и бизнеса посткороновирусного кризиса: сб. науч. тр. междунар. науч.-практ. онлайн-конф. – Р-на-Д., 2020. – С. 12-16.

197 В Алматы пациентов психбольницы на Каблукова похищали и убивали, а их квартиры продавали за бесценок // https://orda.kz/v-almaty-pacientov-psihbolnicy-pohischali-i-ubivali-a-ih-kvartiry-prodavali-za. 28.09.2024.

198 Нурмагамбетов А.М., Жумабаева А.Б. Влияние искусственного интеллекта на трудовые отношения // Вестник ЕНУ имени Л.Н. Гумилева. – 2022. – №4(141). – С. 114-122.

199 Унижаев Н.В. Особенности моделирования угроз безопасности персональных данных для обеспечения достаточного уровня защищенности // Вопросы инновационной экономики. - 2022. - №12(1). – С. 95-110.

200 Ахамбаев Р., Ахметова Ж. Рекомендации и нормы по защите персональных данных в корпоративных информационных системах // Вестник КазАТК. - 2019. - №2. – С. 156-162.

201 Сырлыбаева Ф. Некоторые вопросы защиты информационных прав работника // Вестник ЕНУ имени Л.Н. Гумилева. – 2022. – №3. – С. 72-80.

202 Справка Генеральной прокуратуры по защите прав детей-сирот и детей, оставшихся без попечения родителей, от 22.09.2021 года. – Астана, 2021 (ДСП).

203 Ережепалиев Д.И., Огурцова М.Л. Прокурорский надзор за соблюдением прав несовершеннолетних, пребывающих в организациях для детей сирот и детей, оставшихся без попечения родителей: пос. – М., 2020. – 114 с.

204 Нарушения в Центрах оказания специальных услуг: растрата пособий и незаконные действия // https://www.gov.kz/memleket/entities. 12.09.2024.

205 Координационный совет прокуратуры области Абай: окончено расследование уголовного дела в отношении директора, эксплуатировавшего недееспособных лиц // https://www.gov.kz/memleket/entities. 06.09.2024.

206 Приговор Абайского районного суда Карагандинской области от 17.10.2022 года № 3532-22-00-1/46. – Караганда, 2024 (ДСП).

207 Результаты анализа защищенности веб-ресурсов банков второго уровня Республики Казахстан 2021 // https://cert.kz/files/reports/kz. 10.10.2024.

208 Банкуют все // https://vsekz.org/index.php?threads/depozity. 26.04.2024.

209 В Астане сотрудник банка сорвал спецоперацию силовиков // https://tengrinews.kz/kazakhstan_news/v-astane-sotrudnik-banka-sorval. 06.06.2024.

210 Уголовный кодекс Республики Казахстан: принят 16 июля 1997 года, №167 (утратил силу) // https://adilet.zan.kz/rus/archive/docs. 12.08.2023.

211 Закон Республики Казахстан. О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам совершенствования правоохранительной деятельности и дальнейшей гуманизации уголовного законодательства: принят 9 ноября 2011 года, №490-IV // https://adilet.zan.kz/rus/docs/Z1100000490#z77. 14.08.2023.

212 Закон Республики Казахстан. О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам персональных данных и их защиты: принят 21 мая 2013 года, №95-V // https://adilet.zan.kz/rus/docs/Z1300000095. 13.08.2023.

213 Новиков В.А. Уголовная ответственность за нарушение неприкосновенности частной жизни по законодательству Российской Федерации и Республики Казахстан // Вестник Института законодательства и правовой информации Республики Казахстан. – 2015. – №3(39). – С. 145-149.

214 Вабищевич В.В. Опыт уголовно-правовой охраны персональных данных Казахстана и Германии // Борьба с преступностью: теория и практика: тез. докл. 8-й междунар. науч.-практ. конф. – Могилев, 2020. – С. 22-25.

215 Закон Республики Казахстан. О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам деятельности органов внутренних дел: принят 23 апреля 2014 года, №200-V // https://adilet.zan.kz/rus/docs/Z1400000200. 28.08.2023.

216 Уголовный кодекс Республики Казахстан: принят 3 июля 2014 года, №226-V ЗРК // https://adilet.zan.kz/rus/archive/docs/K1400000226/. 22.08.2023.

217 Закон Республики Казахстан. О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информатизации: принят 24 ноября 2015 года, №419-V ЗРК // https://adilet.zan.kz/rus/docs/Z1500000419. 01.10.2023.

218 Отчет о работе судов первой инстанции по рассмотрению уголовных дел. Правовая статистика: стат. отчеты // https://qamqor.gov.kz/crimestat. 02.08.2024.

219 Журналист Дана Нуржигит засудила бывшего мужа за публикацию интим фото- и видео // https://kaztag.kz/ru/news/zhurnalist-dana. 12.10.2024.

220 Нормативное постановление Верховного Суда Республики Казахстан. О судебной практике по делам о вымогательстве: утв. 23 июня 2006 года, №6 // https://adilet.zan.kz/rus/docs/P06000006S_. 20.10.2024.

221 Уголовный кодекс Республики Узбекистан: принят 22 сентября 1994 года // https://online.zakon.kz/Document. 20.1 октября 2024.

222 Правовая статистика: стат. отчеты // https://qamqor.gov.kz. 10.10.2024.

223 Захилько К.С. Существенный вред как признак уголовной противоправности незаконных действий в отношении информации о частной жизни и персональных данных // Журнал Белорусского государственного университета. Право. – 2022. – №2. – С. 58-68.

224 Пухов А.А. Уголовно-правовая защита неприкосновенности частной жизни и персональных данных в свете изменений уголовного закона // Право.by. – 2021. – № 4(72). – С. 85-92.

225 Вопросы расследования уголовных правонарушений, совершенных в сети Интернет: теоретические и практические аспекты: монография / под ред. Г.К. Шушиковой. – Косшы, 2022. – 110 с.

226 Рязанова Е.Н. Ответственность за распространение персональных данных как способ противодействия правонарушениям в сфере информационно-коммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. – 2022. – №3(95). – С. 118-123.

227 Вабищев В.В. Уголовно-правовая охрана персональных данных: автореф. …канд. юрид. наук: 12.00.08. – Минск, 2024. – 25 с.

228 Закон Республики Казахстан. О средствах массовой информации: принят 23 июля 1999 года, №451-I (утратил силу) // https://adilet.zan. 20.09.2024.

229 Закон Республики Казахстан. О масс-медиа: принят 19 июля 2024 года, №93-VIII ЗРК // https://adilet.zan.kz/rus/docs/Z2400000093. 10.09.2024.

230 Гражданский кодекс Республики Казахстан: принят 27 декабря 1994 года, №268-XIII // https://adilet.zan.kz/rus/docs/K940001000_. 08.07.2024.

231 Конституция Республики Болгарии // https://legalns.com. 10.09.2024.

232 Адаховская С.В., Кобленков А.Ю. Защита персональных данных сотрудника полиции от видеозаписи и незаконного распространения в средствах массовой информации // Юридическая наука и практика. – 2020. – №3(51). – С. 79-83.

233 Бегалиев Е.Н. О некоторых вопросах правового регулирования института блоггинга // Вестник Восточно-Сибирского института МВД России. – 2021. – №1. – С. 70-77.

234 Романова Н.Н., Грызунов В.В. Исследование методом расширенного систематического обзора литературы E-SLR проблемы обеспечения безопасности персональных данных при использовании OSINT // Вестник Дагестанского государственного технического университета. Технические науки. – 2024. – №3(51). – С. 130-144.

235 Совместный приказ Генерального Прокурора Республики Казахстан от 21 декабря 2015 года №150 и Министра внутренних дел Республики Казахстан от 31 декабря 2015 года №1119 и Министра финансов Республики Казахстан от 30 декабря 2015 года №733 и Министра по делам государственной службы Республики Казахстан от 30 декабря 2015 года №21 «Об утверждении Правил и оснований получения правоохранительными органами из системы информационного обмена правоохранительных, специальных государственных и иных органов информации, необходимой для проведения негласных следственных действий и оперативно-розыскной деятельности, а также для решения иных возложенных на них задач» // https://adilet.zan.kz/rus. 06.06.2024.

236 Совместный приказ Генерального Прокурора Республики Казахстан от 26 января 2023 года №41 и Заместителя Премьер-Министра - Министра финансов Республики Казахстан от 26 января 2023 года №69 «Об утверждении Правил и оснований получения органами государственных доходов из системы информационного обмена правоохранительных, специальных государственных и иных органов информации, необходимой для осуществления налогового и таможенного контроля в форме налоговых и таможенных выездных проверок» // https://adilet.zan.kz/rus/docs/V2300031785. 06.06.2024.

ПРИЛОЖЕНИЕ А

Анкета

Уважаемые анкетируемые!

Благодарим Вас за проявленный интерес и уделенное время для ответа на наши вопросы. Собранные данные будут использоваться только в обобщенном виде без указания личных анкетных данных опрашиваемых лиц.

При ответах на вопросы выберете один из наиболее подходящих вариантов, который в большей степени соответствует Вашему мнению.

1. *Укажите Ваш возраст:*

а) 18-30 лет;

б) 26-40 лет;

в) 41-55 лет;

г) 56 и более лет.

2. *Укажите Ваш текущий статус занятости:*

а) учусь;

б) работаю (в т.ч. государственная или правоохранительная служба, предпринимательство, самозанятость и др.);

в) не работаю;

г) на пенсии.

3. *Укажите уровень Ваших познаний в сфере юриспруденции:*

а) низкий;

б) средний;

в) высокий.

4. *Укажите насколько Вы ориентированы в вопросах обеспечения и защиты прав граждан:*

а) слабо;

б) средне;

в) достаточно глубоко;

г) вообще не интересуюсь этим вопросом;

д) занимаюсь защитой прав лично.

5. *Знакомо ли Вам понятие «персональные данные» и его обозначение:*

а) знакомо понятие и его обозначение;

б) понятие знакомо, но точное обозначение не известно;

в) понятие знакомо, имеется общее представление об обозначении;

г) затрудняюсь ответить.

6. *Известно ли Вам, какие именно виды сведений относится к персональным данным помимо фамилии, имени и отчества:*

а) да;

б) скорее да, чем нет;

в) в общих чертах;

г) нет;

д) скорее нет, чем да.

7. *Известно ли Вам, что согласно нормам законодательства к персональным данным относятся более 100 различных видов сведений:*

а) да;

б) нет;

в) частично (знаю некоторые виды персональных данных);

г) впервые узнал(а) об этом.

8. *Знакомо ли Вам понятие «неприкосновенность частной жизни»:*

а) да;

б) нет;

в) затрудняюсь ответить.

9. *Сталкивались ли Вы со случаями несогласованного распространения Ваших персональных данных, персональных данных Ваших близких, родственников или знакомых, в т.ч. через Интернет:*

а) часто;

б) редко;

в) никогда;

г) нет, но слышал(а) или читал(а) о таких фактах.

10. *Сталкивались ли Вы со случаями несогласованного распространения Ваших номеров контактных телефонов (домашний, рабочий, мобильный), адреса места жительства и места прописки либо этих же данных членов Вашей семьи:*

а) часто;

б) редко;

в) никогда;

г) нет, но слышал(а) или читал(а) о таких фактах.

11. *Сталкивались ли Вы со случаями несогласованного Вами распространения данных документа, удостоверяющего Вашу личность (номера, даты выдачи и срока действия удостоверения личности или паспорта, в т.ч. с приложением фотографии):*

а) часто;

б) редко;

в) никогда;

г) нет, но слышал(а) или читал(а) о таких фактах.

12. *Сталкивались ли Вы со случаями несогласованного Вами распространения сведений о совершенных сделках по отчуждению имущества (недвижимость, транспорт, доли участия в юридических лицах, акции и др.), в т.ч. путем обращения после совершения сделки в Ваш адрес организаций, оказывающих страховые и другие услуги:*

а) часто;

б) редко;

в) никогда;

г) нет, но слышал(а) или читал(а) о таких фактах.

13. *Сталкивались ли Вы со случаями несогласованного Вами распространения сведений о результатах медицинских заключений, диагнозов либо другой информации касательно Вашего здоровья:*

а) часто;

б) редко;

в) никогда;

г) нет, но слышал(а) или читал(а) о таких фактах.

14. *Сталкивались ли Вы со случаями несогласованного Вами распространения работодателями или коллегами сведений о Ваших доходах, заработной плате, должностном окладе, его размере, надбавках, премиях, налоговых и пенсионных отчислениях и т.д.:*

а) часто;

б) редко;

в) никогда;

г) нет, но слышал(а) или читал(а) о таких фактах.

15. *Сталкивались ли Вы, Ваши родственники или знакомые со случаями, когда посторонние лица, используя чужие персональные данные, оформляли на этих лиц кредиты, микро займы либо использовали их в иных противозаконных целях:*

а) часто;

б) редко;

в) никогда;

г) нет, но слышал(а) или читал(а) о таких фактах.

16. *Известно ли Вам, что к персональным данным относятся и Ваши биометрические данные (вес, рост, ДНК, отпечатки пальцев, фото- и видео изображения, характеристики биологических жидкостей и продуктов жизнедеятельности человека):*

а) да;

б) частично известно;

в) нет;

г) нет, но слышал(а) или читал(а) о таких фактах.

17. *Поступали ли в Ваш адрес звонки от лиц, представлявшихся сотрудниками банков или государственных органов, из разговора с которыми Вам становилось понятно о наличии у них Ваших персональных данных:*

а) часто;

б) очень часто;

в) редко;

г) никогда;

д) нет, но слышал(а) или читал(а) о таких фактах.

18. *Опасаетесь ли Вы утечки Ваших персональных данных и их последующего несанкционированного распространения:*

а) да;

б) скорее да, чем нет;

в) скорее нет, чем да;

г) нет.

19. *Принимаете ли Вы меры по защите своих персональных данных:*

а) принимаю всегда;

б) принимаю в некоторых случаях;

в) отношусь к этому безразлично;

г) задумываюсь об этом.

20. *Известно ли Вам понятие «добровольное киберстрахование»:*

а) да;

б) что-то слышал(а) или читал(а) об этом;

в) впервые слышу;

г) затрудняюсь ответить.

21. *Задумывались ли Вы о добровольном киберстраховании в целях возмещения имущественного вреда, вызванного возможной утечкой и/или распространением персональных данных:*

а) да;

б) нет;

в) затрудняюсь ответить;

г) планирую изучить этот вопрос.

22. *Известно ли Вам о наличии административной ответственности за нарушение законодательства Республики Казахстан о персональных данных и их защите и нарушение законодательства Республики Казахстан об информатизации:*

а) да;

б) да, но какие это именно статьи КоАП и какая предусмотрена ответственность мне не известно;

в) нет.

23. *Известно ли Вам о наличии уголовной ответственности за нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите:*

а) да;

б) да, но какие это именно статьи УК и какая предусмотрена ответственность мне не известно;

в) нет.

24. *Известен ли Вам механизм защиты своих персональных данных и действий в случае нарушения законодательства о персональных данных и их защите:*

а) известен;

б) известен в общих чертах

в) не известен;

г) никогда не сталкивался(-ась) с этим вопросом;

д) об этом нет никакой доступной информации.

25. *Известен ли государственный орган, который является уполномоченным по защите персональных данных;*

а) известен;

б) известен в общих чертах

в) не известен;

26. *В случае необоснованного сбора или распространения Ваших персональных данных либо иных нарушений законодательства о персональных данных в какой государственный орган Вы обратитесь:*

а) акимат;

б) полиция.

в) прокуратура;

г) Министерство цифрового развития, инноваций и аэрокосмической промышленности;

д) органы национальной безопасности;

е) Министерство информации и общественного развития;

ж) Министерство по чрезвычайным ситуациям;

з) Министерство юстиции;

и) суд;

к) НАО «Правительство для граждан».

27. *Известны ли Вам случаи, когда государство защитило персональные данные конкретного лица или большого числа граждан:*

а) защищены мои личные права, права моих родственников или знакомых;

б) известно о таких фактах из СМИ;

в) ничего не слышал(а) об этом;

г) затрудняюсь ответить.

28. *Известны ли Вам случаи защиты персональных граждан, восстановление прав которых осуществили органы прокуратуры:*

а) защищены мои личные права, права моих родственников или знакомых;

б) известно о таких фактах из СМИ;

в) ничего не слышал(а) об этом;

г) затрудняюсь ответить.

29. *На Ваш взгляд, насколько эффективно защищены персональные данные в Республике Казахстан:*

а) достаточно;

б) недостаточно;

в) вообще не защищены;

г) затрудняюсь ответить;

защищены только отдельные виды данных.

30. *Как Вы относитесь к разделению персональных данных на общедоступные и конфиденциальные с установлением различного порядка их сбора и распространения:*

а) положительно;

б) отрицательно;

в) нейтрально;

г) безразлично;

д) затрудняюсь ответить.

31. *Считаете ли Вы, что сами должны определять какие персональные данные подлежат публичному распространению, а какие нет:*

а) да;

б) скорее да, чем нет;

в) нет;

г) скорее нет, чем да;

д) затрудняюсь ответить.

32. *Сталкивались ли Вы с фактами, когда кто-либо в работе использовал чужую электронно-цифровую подпись (в т.ч.в государственных органах, ЦОНе и т.д.):*

а) часто;

б) редко;

в) никогда;

г) нет, но слышал(а) или читал(а) о таких фактах.

33. *Допускаете ли Вы направление своей электронно-цифровой подписи по электронной почте другим лицам, установления ее на общедоступные компьютеры, установление легких паролей (123…, Qwerty и т.д.):*

а) часто;

б) редко;

в) никогда;

г) нет, но слышал(а) или читал(а) о таких фактах.

34. *На Ваш взгляд из каких источников наиболее часто утекают персональные данные граждан:*

а) банковская сфера;

б) частная сфера;

в) государственные органы;

г) НАО «Правительство для граждан».

35. *Ясно ли Вам в чем отличие законного и незаконного сбора, обобщения и распространения персональных данных, сумеете ли определить противоправные действия:*

а) да;

б) скорее да, чем нет;

в) нет;

г) скорее нет, чем да;

д) вообще не понятно.

36. *Как Вы относитесь к фактам несогласованной съемки и размещения в Интернете фото или видеоизображений посторонних людей (к примеру, продавцов, кассиров, соседей при конфликтах, людей, попавших в неловкую ситуацию, и т.д.):*

а) считаю, что человек вправе снимать и публиковать, что хочет;

б) безразлично;

в) считаю, что это возможно только с согласия этих людей, а несогласованная публикация нарушает их права;

г) считаю это недопустимым, когда такие фото или видео могут способствовать идентифицированию личности человека или причинить ему вред;

д) полагаю, что этот вопрос требует законодательного урегулирования;

е) полагаю, что человек, производящий фото или видеосъемку, обязан спросить разрешение на публикацию.

37. *Знаете ли Вы определения понятия «неприкосновенность частной жизни» и что понимается под «частной жизнью»:*

а) да;

б) скорее да, чем нет;

в) нет;

г) скорее нет, чем да.

38. При заполнении в банках и других организациях согласий на сбор и обработку персональных данных обращаете ли Вы внимание на содержание данных документов:

а) редко;

б) бегло просматриваю;

в) никогда полностью и внимательно не читаю;

г) всегда внимательно читаю;

д) отказываюсь от подписания.

39. *Считаете ли Вы, что в банках и других организациях в согласиях на сбор и обработку персональных данных должен быть указан точный перечень видов собираемых и обрабатываемых персональных данных:*

а) да;

б) скорее да, чем нет;

в) нет;

г) скорее нет, чем да;

д) меня это не беспокоит.

40. *Считаете ли Вы, что в банках и других организациях в согласиях на сбор и обработку персональных данных должен быть указан точный срок и порядок хранения собираемых и обрабатываемых данных:*

а) да;

б) скорее да, чем нет;

в) нет;

г) скорее нет, чем да;

д) меня это не беспокоит.

ПРИЛОЖЕНИЕ Б

Таблица Б.1 – Проект Сравнительной таблицы по внесению изменений и дополнений в правовые акты Республики Казахстан

Структурный элемент	Действующая редакция	Предлагаемая редакция	Обоснование
1	2	3	4
Уголовно-процессуальный кодекс Республики Казахстан			
Пункт 2 статьи 32	Дела об уголовных правонарушениях, предус мотренных статьями 114 (частями первой и вто рой), 123 (частью пер вой), 131, *147 (частями первой и второй),* 149 (частью первой), 150 (частью первой), 198 (частью первой), 199 (частью первой), 321 (частью первой) Уголов ного кодекса Республики Казахстан, а также ста тьей 152 (частями первой и второй) Уголовного кодекса Республики Казахстан, за исключе нием случая, предусмот ренного частью третьей настоящей статьи, счита ются делами частного обвинения. Производство по этим делам начи нается	Дела об уголовных правонарушениях, предусмотренных статьями 114 (частями первой и второй), 123 (частью первой), 131, 149 (частью первой), 150 (частью первой), 198 (частью первой), 199 (частью первой), 321 (частью первой) Уголовного кодекса Республики Казахстан, а также статьей 152 (частями первой и второй) Уголовного кодекса Республики Казахстан, за исключением случая, предусмотренного частью третьей настоящей статьи, считаются делами частного обвинения. Производство по этим делам начинается не иначе как по жалобе потерпевшего и подлежит прекращению за примирением его с обвиняемым, подсудимым.	Анализ показывает, что серьезной проблемой, препятствующей привлечению виновных к уголовной ответственности за несоблюдение мер по защите персональных данных, а также незаконный сбор и (или) обработку (за исключением распространения) персональных данных является отнесение частей 1 и 2 статьи 147 Уголовного кодекса к делам частного обвинения. Производство по делам данной категории начинается не иначе как по жалобе потерпевшего, который является частным обвинителем по делу и поддерживает обвинение в суде. Досудебное расследование по таким делам не проводится, частное обвинение возбуждается при подаче жалобы в суд. Представление и сбор доказательств возлагается на лицо, подавшее жалобу. Однако изучение судебной практики показывает, что для доказательства факта несоблюдения мер по защите персональных данных или незаконности сбора и обработки без распространения персональных данных, как правило, требуется доступ к информационной системе, компьютерной или иной технике обвиняемого лица, что в абсолютной большинстве случаев не представляется возможным и в итоге лишает возможности представления суду доказательств. Изучение отчетов формы № 1 «Отчет о работе судов первой инстанции по рассмотрению уголовных дел»

Продолжение таблицы Б.1

1	2	3	4
	не иначе как по жалобе потерпевшего и подлежит прекращению за примирением его с обвиняемым, подсудимым.		показало, что за 2016-2023 годы и 6 месяцев 2024 года по части 1 статьи 147 Уголовного кодекса судами с вынесением приговора рассмотрено 15 уголовных дел, по которым 1 лицо осуждено, 14 оправдано. Также судами прекращено 8 дел, из которых 4 за примирением сторон и 4 по реабилитирующим основаниям.
Пункт 3 статьи 32	Дела об уголовных правонарушениях, предусмотренных статьями 108-1 (частью первой), 109-1 (частью первой), 110 (частью первой), 115, 120 (частью первой), 121 (частью первой), 121-1, 126 (частью первой), 138, 139, 145, 148 (частью первой), 152 (частью третьей), 153 (частью первой), 154, 155 (частью первой), 157 (частью первой), 158 (частью первой), 159, 187, 189 (частями первой и второй), 190 (частью первой), 195 (частью первой), 198 (частью второй), 199 (частью второй), 201 (частью	Дела об уголовных правонарушениях, предусмотренных статьями 108-1 (частью первой), 109-1 (частью первой), 110 (частью первой), 115, 120 (частью первой), 121 (частью первой), 121-1, 126 (частью первой), 138, 139, 145, *147 (частями первой и второй),* 148 (частью первой), 152 (частью третьей), 153 (частью первой), 154, 155 (частью первой), 157 (частью первой), 158 (частью первой), 159, 187, 189 (частями первой и второй), 190 (частью первой), 195 (частью первой), 198 (частью второй), 199 (частью второй), 201 (частью первой), 202 (частью первой), 204, 205 (частью первой), 206 (частью первой), 207 (частью первой), 208 (частью первой), 209 (частью первой), 211 (частью первой), 223 (частями	За аналогичный период по части 2 статьи 147 Уголовного кодекса с вынесением приговора рассмотрено 46 уголовных дел, по которым 2 лица осуждены, 58 оправданы. Прекращено 29 дел, из которых 4 за примирением сторон, 24 по реабилитирующим основаниям и 1 по иным основаниям. Таким образом, за 8,5 лет к уголовной ответственности за несоблюдение мер по защите персональных данных привлечено всего 4 лица, а за незаконное собирание сведений о частной жизни лица либо незаконный сбор и (или) обработку (за исключением распространения) персональных данных 6 лиц, то есть более чем в 80% случаев предполагаемые нарушители избежали ответственности. К примеру, в 2022 году в г.Алматы на общем собрании жильцов Т. и К. сообщили, что получили через своих знакомых в органах прокуратуры сведения о привлечении к уголовной ответственности директора компании по обслуживанию дом Щ. и иные сведения относительно членов совета дома. По данному факту Щ. обратилась в суд в качестве частного обвинителя, но, не имея доступа к информационным системам органов прокуратуры, она не смогла представить доказательства своего обвинения, в

Продолжение таблицы Б.1

1	2	3	4
	первой), 202 (частью первой), 204, 205 (частью первой), 206 (частью первой), 207 (частью первой), 208 (частью первой), 209 (частью первой), 211 (частью первой), 223 (частями первой и второй), 248 (частью первой), 250, 251 (частью первой), 317 (частью первой), 319 (частями первой и второй), 321 (частью второй), 345 (частью первой), 389 (частью первой) Уголовного кодекса Республики Казахстан, а также статьей 152 (частью первой), если оно связано с неисполнением решения суда о восстановлении на работе, считаются делами частно-публичного обвинения. Производство по этим делам начинается не иначе как по жалобе потерпевшего и подлежит	первой и второй), 248 (частью первой), 250, 251 (частью первой), 317 (частью первой), 319(частями первой и второй), 321 (частью второй), 345 (частью первой), 389 (частью первой) Уголовного кодекса Республики Казахстан, а также статьей 152 (частью первой), если оно связано с неисполнением решения суда о восстановлении на работе, считаются делами частно-публичного обвинения. Производство по этим делам начинается не иначе как по жалобе потерпевшего и подлежит прекращению за примирением его с подозреваемым, обвиняемым, подсудимым лишь в случаях, предусмотренных статьей 68 Уголовного кодекса Республики Казахстан.	результате чего Т.и К. были оправданы. В другом случае, в г.Жаркент неизвестное лицо создало профиль С. на сайтах знакомств, осуществляло от ее имени переписку интимного характера, а также рассылало ее персональные данные, в том числе номер телефона. По косвенным признакам она поняла, что эти действия осуществил ее знакомый А., в чем он ей сознался. Однако, не имея доступа к его компьютеру и телефону, в суде С. не смогла представить доказательства, что в итоге стало причиной оправдания А.

Продолжение таблицы Б.1

1	2	3	4
	прекращению за примирением его с подозреваемым, обвиняемым, подсудимым лишь в случаях, предусмотренных статьей 68 Уголовного кодекса Республики Казахстан.		
Уголовный кодекс Республики Казахстан			
Статья 147	Отсутствует	Примечание. В настоящей статье под существенным вредом правам и законным интересам лиц в результате несоблюдения мер по защите и незаконной обработки персональных данных следует понимать нарушение права на защиту персональных данных, чем потерпевшему лицу причинен имущественный и (или) неимущественный ущерб.	Значимой проблемой, препятствующей привлечению виновных к уголовной ответственности, за нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите, является наличие в объективной стороне состава данного преступления обязательного признака в виде причинения существенного вред правам и законным интересам лиц. При этом в уголовном законодательстве и нормативных постановлениях Верховного Суда отсутствует толкование признака «существенный вред» относительно обработки персональных данных. Следует отметить, что схожая ситуация отмечается и других государствах, где введена уголовная ответственности за незаконную обработку персональных данных, в связи с чем данный вопрос является предмет исследования немалого количества ученных. Исходя из мнения ученых, в Республике Казахстан под существенным вредом правам и законным интересам лиц в результате несоблюдения мер по защите и незаконной обработки персональных данных предлагается понимать

Продолжение таблицы Б.1

1	2	3	4
			нарушение права на защиту персональных данных, чем потерпевшему лицу причинен имущественный и (или) неимущественный ущерб. Под имущественным ущербом следует понимать затраты лица на восстановление конфиденциальности персональных данных, утраченную выгоду и другие негативные последствия финансового характера. Под неимущественным ущербом следует понимать нравственные и физические страдания, моральные или психические переживания и другие негативные последствия, в том числе влияющие на честь, достоинство и деловую репутацию. При определении существенного вреда следует учитывать субъективную оценку потерпевшим тяжести причиненного ему ущерба, а также объективные данные о значимости, виде и объеме незащищенных или обработанных персональных данных, стоимости устранения последствий этих действий.
Статья 147-1	Отсутствует	Распространение или угроза распространения, без согласия лица, фото и (или) видеоизображений его обнаженного тела и (или) половых органов.	Изучение показывает, что распространение интимных фотографий встречается достаточно часто, но единой практики до настоящего времени не имеется. Так, в 2023 году в г.Алматы судом оправдан Д., отправивший интимные фотографии своей бывшей супруги ее родителям и родственникам. В свою очередь в 2024 году за такие же действия в Западно-Казахстансой области осужден И., а в г.Талдыкорган в 2023 году осужден Е., который отправил близким родственникам своей бывшей девушки ее фото и видео интимного характера, а также от ее имени зарегистрировался в социальных сетях, публиковал в них указанные изображения, а также объяв ления об оказании его бывшей девушкой интимных услуг.

Продолжение таблицы Б.1

1	2	3	4
			Кроме того, в настоящее время многие другие преступления совершаются под угрозой распространения интимных фотографий или видеозаписей. Так, в 2024 году резонанс получил случай в Кызылординской области, где 11 человек под угрозой распространения персональных данных в виде интимных фото и видео вовлекли несовершеннолетнюю в занятие проституцией. В этом же году в г.Туркестан 33-летний мужчина под угрозой аналогичных действий совершил изнасилование несовершеннолетней и вымогал у нее денежные средства. В целом, таких примеров немало. Некоторые государства выделили данные действия в отдельный состав преступления. К примеру, в Республике Узбекистан в Уголовном кодексе имеется статья 141.3, которой предусмотрена уголовная ответственность за распространение или угрозу распространения информации, содержащей фото и (или) видеоизображения обнаженного тела и (или) половых органов лица без его согласия, в том числе распространение в СМИ, сетях телекоммуникаций или сети Интернет
Кодекс Республики Казахстан «О браке (супружестве) и семье»			
Статья 12	Статья 12. Медицинское обследование лиц, вступающих в брак (супружество) 1. Консультирование и обследование по	Статья 12. Медицинское обследование *и обмен сведениями между лицами, вступающими в брак (супружество)* 1. Консультирование и обследование по медицинским, а	Республика Казахстан относится к числу мировых лидеров по количеству расторжений браков, причинами которых чаще всего являются алкоголизм, наркомания, бытовое насилие, лудомания, а также около 20% браков распадаются по причине невозможности зачатия и рождения детей. Социальные опросы показывают, что

Продолжение таблицы Б.1

1	2	3	4
	медицинским, а также по медико-генетическим вопросам и вопросам охраны репродуктивного здоровья лиц, желающих вступить в брак (супружество), и только с их обоюдного согласия проводятся организа циями здравоохранения. 2. Результаты обследо вания лица, вступающего в брак (супружество), составляют медицинскую тайну и могут быть со общены лицу, с которым оно намерено заключить брак (супружество), толь ко с согласия прошед шего обследование. Исключение составляют случаи, когда у лица, вступающего в брак (супружество), имеется заболевание, создающее угрозу для здоровья другого лица, вступающего в брак (супружество).	также по медико-генетическим вопросам и вопросам охраны репродуктивного здоровья лиц, желающих вступить в брак (супружество), проводятся организациями здравоохранения. 2. Результаты обследования лица, вступающего в брак (супружество), *сообщаются лицу, с которым оно намерено заключить брак (супружество).* *Обязательным является информирование в случаях,* когда у лица, вступающего в брак (супружество), имеется заболевание, создающее угрозу для здоровья другого лица, вступающего в брак (супружество) *либо представляющее угрозу для здоровья будущего потомства.* *3. Между лицами, вступающими в брак (супружество), производится обмен данными, предусмотренными Паспортом персональных данных.*	нередко браки расторгаются по причине нетрадиционной сексуальной ориентации одного из супругов. Кодекс Республики Казахстан «О браке (супружестве) и семье» предусматривает добровольное медицинское обследование лиц, вступающих в брак (супружество), а его результаты могут быть представлены предполагаемому супругу только с согласия обследованного лица. Исключением являются случаи, когда имеется заболевание, способное создать угрозу для здоровья другого лица, вступающего в брак (супружество). Расторжению брака также может способствовать скрытая от будущего супруга информация о наличии судимости, предыдущих браков, детей, гражданстве, просроченной задолженности, имеющихся обязательствах, в том числе по алиментам, а также обман о реальном возрасте, наличии имущества, жилья и пр. Нельзя не учитывать и особенности традиций страны, особенно в части запрета и крайне негативного отношения к бракам между родственниками и лицами, близкими по родоплеменным признакам. Поэтому видится целесообразным обязательное проведение медицинского обследования лиц, вступающих в брак (супружество), а также обмен ими важными персональными данными. Для этой цели предлагается внедрить Паспорт персональных данных, который будет содержать сведения о наличии/отсутствии судимости, ВИЧ-статусе, врожденных и приобретенных заболеваниях, способных повлиять на потомство, наличии предыдущих браков,

Продолжение таблицы Б.1

1	2	3	4
			детей и обязательств перед ними, непогашенной задолженности, образовании, наличии недвижимого имущества, долей в юридических лицах и др. В дальнейшем не исключается использование, в том числе в усеченном виде данного Паспорта в иных целях, к примеру, для изучения кандидатов при трудоустройстве на работу. При этом возможна интеграция паспортов персональных данных с государственной и негосударственными системами контроля доступа к персональным данным, что даст субъекту персональных данных в каждом случае использования его Паспорта персональных данных определять перечень сведений, который он готов предоставить тому или иному лицу. Предоставление и обмен медицинскими и специальными персональными данными между лицами, планирующим вступить в брак, имеет место в других странах. К примеру, статья 30 Семейного кодекса Украины обязывает жениха и невесту сообщить друг другу о состоянии своего здоровья, а сокрытие сведений, важных для здоровья будущих потомков, может повлечь признание брака недействительным. Во Франции, Узбекистане и ряде штатов США предусмотрено обязательное медицинское обследование будущих супругов и информирование о физиологических, психических заболеваниях, отклонениях сексуальной жизни и прочих сведениях, препятствующих ведению семейной жизни.
Закон Республики Казахстан «О персональных данных и их защите»			
Подпункт 2) статьи 1	персональные данные – сведения, относящиеся к	персональные данные – сведения, совокупность информации, прямо	Положения о необходимости фиксации персональных данных на каком-либо носителе являются суживающим

Продолжение таблицы Б.1

1	2	3	4
	определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе	или косвенно относящиеся к определенному или определяемому физическому лицу, являющемуся субъектом (носителем) персональных данных	фактором и могут негативно повлиять на практике. Сравнительный анализ показывает, что в странах Европы, Новой Зеландии, Японии, Южной Корее, Бразилии и многих других государствах под персональными данными понимается любая информация, относящаяся к физическому лицу, которая может быть использована для его идентификации. Из стран СНГ схожий подход избрали Азербайджан, Армения, Белоруссия, Молдова, Россия и Таджикистан. В свою очередь, Казахстан, Кыргызстан, Узбекистан и Туркменистан законодательно закрепили положения о необходимости фиксации такой информации на каком-либо носителе. При этом многие виды персональных данных, в особенности чувствительного характера, такие как, например, сведения о религиозных и политических убеждениях, особенностях сексуального поведения в большинстве случаев не зафиксированы на каком-либо информационном носителе, что может вызвать проблемы при необходимости их защиты.
Новый подпункт 1) статьи 1	Переносится в подпункт 1-1) статьи 1	специальные персональные данные – особо личные сведения, сбор, обработка и распространение которых могут повлечь чувствительные последствия для субъекта данных, в том числе данные о судимости, расовом или национальном происхождении, родовой принадлежности, политических	Значительной проблемой казахстанского законодательства является неурегулированность вопроса обработки специальных видов персональных данных. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и законодательство большинства европейских стран относят данные о судимости лица, расовом или национальном происхождении, политических взглядах, религиозных и других убеждениях, данные о состоянии здоровья и интимной жизни к числу специальных либо

Продолжение таблицы Б.1

1	2	3	4
		взглядах, религиозных и других убеждениях, данные о состоянии здоровья и интимной жизни, смене пола и прочие.	чувствительных персональных данных. Законодательством Казахстана не предусмотрено понятие «специальные (либо чувствительные) персональные данные», сведения о расовом или национальном происхождении, политических взглядах, религиозных и других убеждениях, данные о состоянии здоровья, интимной жизни и судимости правовыми актами не отнесены к персональным данным ограниченного доступа, в связи с чем в обществе на постоянной основе возникают попытки сбора и обработки такой информации, чем ущемляются права граждан. Введение понятия специальные персональные данные в законодательство Казахстана позволит более эффективно защищать права граждан, поскольку прекратит бесконтрольный сбор чувствительных сведений.
Новый подпункт 1-1) статьи 1	биометрические данные – персональные данные, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на основе которых можно установить его личность	биометрические данные – персональные данные, которые позволяют установить личность субъекта персональных данных на основе характеризующих его физиологических, биологических признаков и поведенческих особенностей (цифровая фотография, отпечатки пальцев и (или) кистей рук, изображение радужной оболочки глаз, рисунок вен, геометрия ушных раковин, сигналы мозга, почерк, походка, динамика нажатия клавиш и	В настоящее время Законом «О дактилоскопической и геномной регистрации» закреплены два вида биометрических данных: геномная информация и дактилоскопическая информация. Геномная информация содержит сведения о ДНК, а дактилоскопическая информация об особенностях строения папиллярных узоров пальцев и (или) ладоней рук. При этом в законодательстве Казахстана уже появляются нормы о биометрической идентификации. В Социальном кодексе, законах «О платежах и платежных системах», «О банках и банковской деятельности в Республике Казахстан» и других правовых актах закреплены нормы о биометрической идентификации на основе захвата изображения лица человека.

Продолжение таблицы Б.1

1	2	3	4
		другие биометрические персональные данные)	В научной литературе к биометрическим персональным данным помимо фотографии, ДНК и папиллярных узоров также относят радужную оболочку глаз, рост, вес, видеозапись лица, рисунок вен ладони. Однако в законодательстве Казахстана такие виды биометрических персональных данных не выделяются, хотя в жизни граждан страны используются сервисы с применением технологий сбора и использования такой информации. Например, казахстанский стартап-проект «Alaqan» внедряет технологию использования рисунка вен ладони человека для входа в помещения и для оплаты услуг. По сведениям разработчиков стартапа в системе зарегистрировались уже почти сто тысяч человек. Следует отметить, что зарубежное законодательство, как правило, относит к биометрическим персональным данным не только физические и физиологические, но и поведенческие особенности физического лица, которые позволяют произвести или подтверждают однозначную идентификацию этого физического лица. В 2023 году принят Закон «Об онлайн-платформах и онлайн-рекламе», которым введены такие понятия, как профайлинг и таргетированная онлайн-реклама. Под профайлингом понимаются действия онлайн-платформ по определению предпочтений и (или) интересов пользователей, а под таргетированной онлайн-рекламой онлайн-реклама, направляемая целевым группам на основании профайлинга. Иными словами онлайн-платформам дано право сбора информации о поведенческих особенностях человека.

Продолжение таблицы Б.1

1	2	3	4
			Имеющиеся проблемы в сфере применения биометрической аутентификации планировалось решить при реализации Программы создания Национальной платформы цифровой биометрической идентификации на 2022-2024 годы, но дальше обсуждения проекта она не зашла и не была утверждена в итоге.
Нормативное постановление Верховного Суда Республики Казахстан «О квалификации некоторых уголовных правонарушений против жизни и здоровья человека» от 11 мая 2007 года N 1			
Абзац пятый пункта 29	Отсутствует	Доведение до самоубийства, в том числе посредством использования сетей телекоммуникаций, в том числе сети Интернет может осуществляться путем угроз распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.	В настоящее время многие преступления совершаются под угрозой распространения сведений, позорящих лицо, в том числе интимных фотографий, видеозаписей и иных персональных данных. При этом включение в признаки совершения преступлений таких действий, как «под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких» в большой перечень статей Уголовного кодекса Республики Казахстан является проблематичным. В этой связи видится дополнение и разъяснение в нормативных постановлениях Верховного Суда Республики Казахстан. Следует отметить, что доведение до самоубийства, склонение к совершению самоубийства или содействие совершению самоубийства нередко могут совершаться может осуществляться путем угроз распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.

Продолжение таблицы Б.1

1	2	3	4
Нормативное постановление Верховного Суда Республики Казахстан «О некоторых вопросах квалификации преступлений, связанных с изнасилованием и иными насильственными действиями сексуального характера» от 11 мая 2007 года N 4			
Абзац четвертый пункта 14-2	Отсутствует	Под понуждением к половому сношению, мужеложству, лесбиянству или иным действиям сексуального характера путем шантажа могут пониматься угрозы распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.	В настоящее время многие преступления совершаются путем шантажа. Касательно понуждения к половому сношению, мужеложству, лесбиянству или иным действиям сексуального характера путем шантажа возможно понимать угрозы распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких. В частности, нередко злоумышленники путем обмана или другими методами завладевают вышеуказанными сведениями и, шантажируя их распространением, принуждают потерпевших к половому сношению, мужеложству, лесбиянству или иным действиям сексуального характера.
Абзац пятый пункта 14-2	Отсутствует	Вовлечение в занятие проституцией, оказание иных услуг сексуального характера также могут осуществляться путем угроз распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.	В настоящее время многие преступления совершаются под угрозой распространения сведений, позорящих лицо, в том числе интимных фотографий, видеозаписей и иных персональных данных. При этом включение в признаки совершения преступлений таких действий, как «под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких» в большой перечень статей Уголовного кодекса Республики Казахстан является проблематичным. В этой связи видится дополнение и разъяснение в нормативных постановлениях Верховного Суда

Продолжение таблицы Б.1

1	2	3	4
			Республики Казахстан. Следует отметить, что Вовлечение в занятие проституцией, оказание иных услуг сексуального характера также могут осуществляться путем угроз распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.
Нормативное постановление Верховного Суда Республики Казахстан «О судебной практике по делам об уголовных правонарушениях несовершеннолетних и о вовлечении их в совершение уголовных правонарушений и иных антиобщественных действий» от 11 апреля 2002 года N 6			
Абзац первый пункта 24	Под вовлечением несовершеннолетнего в совершение уголовных правонарушений следует понимать целенаправленные действия вовлекающего по формированию у несовершеннолетнего желания (намерения, стремления) и готовности участвовать в совершении уголовных правонарушений. При этом действия взрослого должны носить активный характер и могут сопровождаться	Под вовлечением несовершеннолетнего в совершение уголовных правонарушений следует понимать целенаправленные действия вовлекающего по формированию у несовершеннолетнего желания (намерения, стремления) и готовности участвовать в совершении уголовных правонарушений. При этом действия взрослого должны носить активный характер и могут сопровождаться применением психического или физического воздействия (побои, уговоры, угрозы и запугивания, подкуп,	Вовлечение несовершеннолетних в совершение уголовных правонарушений может осуществляться различными путями, в том числе угрозами. При этом зачастую угрозы выражаются не только в вероятном применении физического насилия, а также в угрозах распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.

Продолжение таблицы Б.1

1	2	3	4
	применением психического или физического воздействия (побои, уговоры, угрозы и запугивания, подкуп, обман, возбуждения чувства мести, зависти и других низменных побуждений, уверения в безнаказанности, дача советов о месте и способе совершения или сокрытия следов уголовных правонарушений, обещание платы за совершенные действия либо оказание содействия в реализации похищенного и другие).	обман, возбуждения чувства мести, зависти и других низменных побуждений, уверения в безнаказанности, дача советов о месте и способе совершения или сокрытия следов уголовных правонарушений, обещание платы за совершенные действия либо оказание содействия в реализации похищенного и другие). *Угрозы могут выражаться в распространении сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких*	
Абзац третий пункта 26	Отсутствует	Под вовлечением несовершеннолетнего в занятие проституцией, оказание иных услуг сексуального характера путем шантажа, а также под вовлечением несовершеннолетних в изготовление продукции эротического содержания могут пониматься угрозы распространения сведений,	В настоящее время многие преступления совершаются путем шантажа. Касательно вовлечения несовершеннолетних в занятие проституцией, оказание иных услуг сексуального характера путем шантажа возможно понимать угрозы распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких. В частности, нередко злоумышленники путем обмана или другими методами

Продолжение таблицы Б.1

1	2	3	4
		позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.	завладевают вышеуказанными сведениями и, шантажируя их распространением, вовлекают несовершеннолетних в занятие проституцией, оказание иных услуг сексуального характера. Вовлечение несовершеннолетних в изготовление продукции эротического содержания может осуществляться различными путями, в том числе угрозами. При этом зачастую угрозы выражаются не только в вероятном применении физического насилия, а также в угрозах распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.
Нормативное постановление Верховного Суда Республики Казахстан «О судебной практике по делам о вымогательстве» от 23 июня 2006 года №6			
Абзац пятый пункта 5	Существенный вред мо жет быть причинен и оглашением иных сведе ний, которые не являясь позорящими, способны причинить потерпевшему существенный вред, на пример, разглашение ком мерческой тайны, влеку щее причинение убытков бизнесу, разглашение тайны усыновления либо сведения, относящиеся к семейной и частной жизни и т.п.	Существенный вред может быть причинен и оглашением иных сведений, которые не являясь позорящими, способны причинить потерпевшему существенный вред, например, разглашение коммерческой тайны, влекущее причинение убытков бизнесу, разглашение тайны усыновления либо сведения, относящиеся к семейной и частной жизни, *персональные данные* и т.п.	Изучение практики показывает, что нередко вымогательство осуществляется под угрозой распространения различных сведений, в том числе персональных данных.

Продолжение таблицы Б.1

1	2	3	4
Нормативное постановление Верховного Суда Республики Казахстан «О применении законодательства по делам, связанным с незаконным оборотом наркотических средств, психотропных веществ, их аналогов и прекурсоров» от 14 мая 1998 года №3			
Пункт 13-1	Отсутствует	Вымогательство наркотических средств, психотропных веществ, их аналогов может осуществляться путем угроз распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.	Вымогательство наркотических средств, психотропных веществ, их аналогов может осуществляться различными путями, в том числе угрозами. При этом зачастую угрозы выражаются не только в вероятном применении физического насилия, а также в угрозах распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.
Абзац первый пункта 15	Под склонением к употреблению наркотических средств или психотропных веществ, их аналогов следует понимать любые умышленные действия, направленные на возбуждение у других лиц желания к их употреблению (уговоры, предложения, дача советов, введение в заблуждение, обман, угрозы и т.п.). Уголовное	Под склонением к употреблению наркотических средств или психотропных веществ, их аналогов следует понимать любые умышленные действия, направленные на возбуждение у других лиц желания к их употреблению (уговоры, предложения, дача советов, введение в заблуждение, обман, угрозы, *в т.ч. распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить*	Склонение к употреблению наркотических средств или психотропных веществ, их аналогов может осуществляться различными путями, в том числе угрозами. При этом зачастую угрозы выражаются не только в вероятном применении физического насилия, а также в угрозах распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.

Продолжение таблицы Б.1

1	2	3	4
	правонарушение является оконченным с момента осуществления воздейст вия на лицо с целью побудить его к употреб лению наркотических средств или психотроп ных веществ, их аналогов независимо от того, упот ребило ли их склоняемое лицо либо употребление не состоялось в силу каких-либо причин (отказ склоняемого от употреб ления, вмешательство других лиц и т.п.). При этом для наступления ответственности не имеет значения, употребляло ли ранее склоняемое лицо наркотические средства или психотропные вещества, их аналоги.	*существенный вред интересам потерпевшего или его близких и т.п.).* Уголовное правонарушение является оконченным с момента осуществления воздействия на лицо с целью побудить его к употреблению наркотических средств или психотропных веществ, их аналогов независимо от того, употребило ли их склоняемое лицо либо употребление не состоялось в силу каких-либо причин (отказ склоняемого от употребления, вмешательство других лиц и т.п.). При этом для наступления ответственности не имеет значения, употребляло ли ранее склоняемое лицо наркотические средства или психотропные вещества, их аналоги.	
Нормативное постановление Верховного Суда Республики Казахстан «О применении норм уголовного и уголовно-процессуального законодательства по вопросам соблюдения личной свободы и неприкосновенности достоинства человека, противодействия пыткам, насилию, другим жестоким или унижающим человеческое достоинство видам обращения и наказания» от 28 декабря 2009 года №7			
Абзац четвер тый пункта 14	Отсутствует	Под принуждением подозрева емого, обвиняемого, потерпев шего, свидетеля к даче показаний,	Принуждение подозреваемого, обвиняемого, потерпев шего, свидетеля к даче показаний, а равно воспрепятствование лицу в добровольной даче показаний,

Продолжение таблицы Б.1

1	2	3	4
		а равно воспрепятствованием лицу в добровольной даче показаний, подаче заявления о совершенном преступлении либо принуждением к отказу от дачи показаний, либо принуждением эксперта к даче заключения путем применения угроз, шантажа могут пониматься угрозы распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.	подаче заявления о совершенном преступлении либо принуждение к отказу от дачи показаний, либо принуждение эксперта к даче заключения могут осуществляться различными путями, в том числе шантажа и угрозами. При этом зачастую шантаж и угрозы выражаются не только в вероятном применении физического насилия, а также в угрозах распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.
Абзац пятый пункта 14	Отсутствует	Принуждение свидетеля, потерпевшего к даче ложных показаний, эксперта к даче ложного заключения или переводчика к осуществлению неправильного перевода, а равно принуждение указанных лиц к уклонению от дачи показаний, соединенное с шантажом, также может осуществляться путем угроз распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.	Принуждение свидетеля, потерпевшего к даче ложных показаний, эксперта к даче ложного заключения или переводчика к осуществлению неправильного перевода, а равно принуждение указанных лиц к уклонению от дачи показаний, соединенное с шантажом может выражаться в угрозах. При этом зачастую угрозы предполагают не только вероятное применение физического насилия, а также распространение сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.

ПРИЛОЖЕНИЕ В

Проект Нормативного постановления Верховного Суда Республики Казахстан

Нормативное постановление Верховного Суда Республики Казахстан от __ _____ 20__ года № __
«О внесении изменений и дополнений в некоторые нормативные постановления Верховного Суда Республики Казахстан по уголовному законодательству»

1. Внести изменения и дополнения в следующие нормативные постановления Верховного Суда Республики Казахстан:

1. «О квалификации некоторых уголовных правонарушений против жизни и здоровья человека» от 11 мая 2007 года N 1:

1) пункт 29 дополнить абзацем пятым следующего содержания:

«Доведение до самоубийства, в том числе посредством использования сетей телекоммуникаций, в том числе сети Интернет может осуществляться путем угроз распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких».

2. «О некоторых вопросах квалификации преступлений, связанных с изнасилованием и иными насильственными действиями сексуального характера» от 11 мая 2007 года N 4:

1) пункт 14-2 дополнить абзацем четвертым следующего содержания:

«Под понуждением к половому сношению, мужеложству, лесбиянству или иным действиям сексуального характера путем шантажа могут пониматься угрозы распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.»;

2) пункт 14-2 дополнить абзацем пятым следующего содержания:

«Вовлечение в занятие проституцией, оказание иных услуг сексуального характера также могут осуществляться путем угроз распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.».

3. «О судебной практике по делам об уголовных правонарушениях несовершеннолетних и о вовлечении их в совершение уголовных правонарушений и иных антиобщественных действий» от 11 апреля 2002 года N 6:

1) пункт 24 изложить в следующей редакции:

«Под вовлечением несовершеннолетнего в совершение уголовных правонарушений следует понимать целенаправленные действия вовлекающего по формированию у несовершеннолетнего желания (намерения, стремления) и готовности участвовать в совершении уголовных правонарушений. При этом действия взрослого должны носить активный характер и могут сопровождаться применением психического или физического воздействия (побои, уговоры, угрозы и запугивания, подкуп, обман, возбуждения чувства мести, зависти и других низменных побуждений, уверения в безнаказанности, дача советов о месте и способе совершения или сокрытия следов уголовных правонарушений, обещание платы за совершенные действия либо оказание содействия в реализации похищенного и другие). Угрозы могут выражаться в распространении сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.»;

2) пункт 26 дополнить абзацем третьим следующего содержания:

«Под вовлечением несовершеннолетнего в занятие проституцией, оказание иных услуг сексуального характера путем шантажа, а также под вовлечением несовершеннолетних в изготовление продукции эротического содержания могут пониматься угрозы распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.».

4. «О судебной практике по делам о вымогательстве» от 23 июня 2006 года № 6:

1) в пункте 5 абзац пятый изложить в следующей редакции:

«Существенный вред может быть причинен и оглашением иных сведений, которые не являясь позорящими, способны причинить потерпевшему существенный вред, например, разглашение коммерческой тайны, влекущее причинение убытков бизнесу, разглашение тайны усыновления либо сведения, относящиеся к семейной и частной жизни, персональные данные и т.п.».

5. «О применении законодательства по делам, связанным с незаконным оборотом наркотических средств, психотропных веществ, их аналогов и прекурсоров» от 14 мая 1998 года № 3:

1) дополнить пунктом 13-1 следующего содержания:

«Вымогательство наркотических средств, психотропных веществ, их аналогов может осуществляться путем угроз распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.»;

2) в пункте 15 абзац первый изложить в следующей редакции:

«Под склонением к употреблению наркотических средств или психотропных веществ, их аналогов следует понимать любые умышленные действия, направленные на возбуждение у других лиц желания к их употреблению (уговоры, предложения, дача советов, введение в заблуждение,

обман, угрозы, в т.ч. распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких и т.п.).».

6. «О применении норм уголовного и уголовно-процессуального законодательства по вопросам соблюдения личной свободы и неприкосновенности достоинства человека, противодействия пыткам, насилию, другим жестоким или унижающим человеческое достоинство видам обращения и наказания» от 28 декабря 2009 года № 7:

1) пункт 14 дополнить абзацем четвертым следующего содержания:

«Под принуждением подозреваемого, обвиняемого, потерпевшего, свидетеля к даче показаний, а равно воспрепятствованием лицу в добровольной даче показаний, подаче заявления о совершенном преступлении либо принуждением к отказу от дачи показаний, либо принуждением эксперта к даче заключения путем применения угроз, шантажа могут пониматься угрозы распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.»;

2) пункт 14 дополнить абзацем пятым следующего содержания:

«Принуждение свидетеля, потерпевшего к даче ложных показаний, эксперта к даче ложного заключения или переводчика к осуществлению неправильного перевода, а равно принуждение указанных лиц к уклонению от дачи показаний, соединенное с шантажом, также может осуществляться путем угроз распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, а также персональных данных, оглашение которых может причинить существенный вред интересам потерпевшего или его близких.».

2. Согласно статье 4 Конституции Республики Казахстан настоящее нормативное постановление включается в состав действующего права, является общеобязательным и вводится в действие со дня первого официального опубликования.

Председатель Верховного Суда
Республики Казахстан _____

Судья Верховного Суда
Республики Казахстан,
секретарь пленарного заседания _____

ПРИЛОЖЕНИЕ Г

Патент

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ РЕСПУБЛИКА КАЗАХСТАН

REPUBLIC OF KAZAKHSTAN

ПАТЕНТ
PATENT

№ 8815

ПАЙДАЛЫ МОДЕЛЬГЕ / НА ПОЛЕЗНУЮ МОДЕЛЬ / FOR UTILITY MODEL

(21) 2023/1152.2

(22) 20.11.2023

(45) 02.02.2024

(54) Кірістірілген RFID - сенсоры бар компьютер тінтуірі
Компьютерная мышь со встроенным RFID - датчиком
Computer mouse with built-in RFID - sensor

(73) Бегалиев Ернар Нурланович (KZ); Амиров Алмас Муратович (KZ)
Begaliyev Yernar Nurlanovich (KZ); Amirov Almas Muratovich (KZ)

(72) Амиров Алмас Муратович (KZ) Amirov Almas Muratovich (KZ)
Бегалиев Ернар Нурланович (KZ) Begaliyev Yernar Nurlanovich (KZ)

ЭЦҚ кол қойылды
Подписано ЭЦП
Signed with EDS

Е. Оспанов
Е. Оспанов
Y. Ospanov

«Ұлттық зияткерлік меншік институты» РМК директоры
Директор РГП «Национальный институт интеллектуальной собственности»
Director of RSE «National institute of intellectual property»

РЕСПУБЛИКА КАЗАХСТАН

(19) KZ (13) U (11) 8815
(51) *G06F 3/033* (2013.01)

МИНИСТЕРСТВО ЮСТИЦИИ РЕСПУБЛИКИ КАЗАХСТАН

ОПИСАНИЕ ПОЛЕЗНОЙ МОДЕЛИ
К ПАТЕНТУ

(21) 2023/1152.2
(22) 20.11.2023
(45) 02.02.2024, бюл. №5
(72) Амиров Алмас Муратович; Бегалиев Ернар Нурланович
(73) Бегалиев Ернар Нурланович; Амиров Алмас Муратович

(54) **КОМПЬЮТЕРНАЯ МЫШЬ СО ВСТРОЕННЫМ RFID - ДАТЧИКОМ**

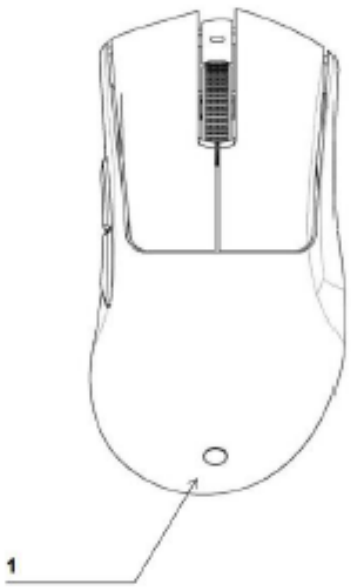
(57) Компьютерная мышь со встроенным RFID-датчиком является компьютерным аксессуаром, состоящим из компьютерной мыши и частично встроенного в ее корпус RFID-датчика.

RFID-датчик дает возможность применения компьютерной мыши лишь при взаимодействии с чипом или другими устройствами с чипом, содержащими информацию о наличии у лица права доступа к данному компьютеру. Без взаимодействия с чипом возможность использования мыши блокирует, то есть она не будет откликаться на действия пользователя. Кроме того, RFID-датчик будет фиксировать необходимые данные о работе пользователя с компьютером.

Применение полезной модели возможно лицами, имеющими доступ к государственным и частным базам данных, а также любыми другими лицами, желающими ограничить возможность использования их компьютеров посторонними.

Использование компьютерной мыши со встроенным RFID-датчиком будет способствовать повышению защищенности персональных данных, снижению количества утечек информации с государственных и негосударственных баз данных, а также позволит повысить эффективность работы уполномоченных органов при профилактике правонарушений в сферах защиты персональных данных, разглашения государственных секретов и другой информации ограниченного характера.

(19) KZ (13) U (11) 8815



Фигура 1 (вид сверху)

Полезная модель относится к компьютерным аксессуарам и предназначена для исключения фактов применения компьютеров лицами, не имеющими права использования конкретного компьютера, а также для фиксации времени, пользователя и других сведений при работе лица с компьютером, в том числе в базах данных и базах персональных данных.

В корпус компьютерной мыши частично встраивается RFID-датчик толщиной не более 2.65 мм (0.5-1 мм внутри корпуса) и шириной не более 7.5 мм., содержащий уникальный идентификационный код, электронный серийный номер, что дает возможность применения компьютерной мыши лишь при взаимодействии с чипом или другими устройствами с чипом, содержащими информацию о наличии у лица права доступа к конкретному компьютеру. Электронные компоненты частично встраиваются в корпус, не приводя к утолщению компьютерной мыши и не вызывая сложности ее использования.

Компьютерную мышь со встроенным RFID-датчиком предполагается использовать в деятельности правоохранительных и специальных органов, государственных служащих, НАО «Правительство для граждан», других организаций и лиц (частные судебные исполнители, нотариусы и др.), имеющих доступ к государственным базам данных, частных организаций, являющихся владельцами баз данных, а также любыми другими лицами, желающими ограничить возможность использования их компьютеров посторонними.

В настоящее время в результате активно реализуемой цифровизации практически во всех сферах деятельности государственных и негосударственных организаций, в том числе субъектов бизнеса, которая сопровождается массовым сбором, хранением и обобщением данных нередко возникает проблема уязвимости персональных данных граждан.

Незаконно полученные или похищенные персональные данные зачастую используются для совершения преступлений, других противоправных действий или другого причинения вреда гражданам. С 2018 по 2022 год число интернет-мошенничеств выросло с 517 до 20,6 тыс. В 2022-2023 годах ущерб от мошеннических действий составил более 30 млрд. тенге.

В рейтинге ООН Global E-Government Development Index на 2022 год по развитию электронного правительства Республика Казахстан занимает 28 место из 193 стран, а в Центральной Азии является ведущей страной по развитию электронного правительства.

Уже сейчас более 1,3 тыс. государственных услуг реализуется через НАО «Правительство для граждан» с использованием около 100 государственных баз данных. Ожидается, что количество государственных услуг и баз данных будет увеличиваться. Соответственно, будут расти количество накапливаемой на них информации и персональных данных, а также риски утери.

Стремительно растет количество негосударственных баз данных, осуществляющих сбор личных данных граждан.

Обеспечить эффективный контроль за использованием государственных баз данных более 200 тыс. человек и значительного числа лиц, имеющих доступ к негосударственным базам данных крайне проблематично.

Схожая проблема имеет место при работе с документами ограниченного доступа.

В этой связи целесообразно применение современных технологий и новых методов, одним из которых могло бы стать оснащение компьютерной мыши технологией RFID, которая даст возможность применения данного аксессуара только во взаимодействии датчика с чипом, содержащим и подтверждающим информацию о наличии у конкретного лица прав использования компьютера и доступа к базам данных.

Целью заявленной полезной модели является исключение фактов применения компьютеров, лицами, не имеющими права использования конкретного компьютера, а также фиксация времени, пользователя и других сведений при работе лица с компьютером, в том числе с документами ограниченного доступа, в базах данных и базах персональных данных.

Техническим результатом заявляемой полезной модели является:

1. Разработка компьютерной мыши со встроенным RFID-датчиком позволит исключить факты использования компьютеров лицами, не имеющим права доступа к нему, а также будет способствовать:

– снижению количества фактов необоснованного доступа лиц, не имеющих соответствующего права, к базам данных, базам персональных данных;

– безошибочному определению лица, которое в конкретное время использовало компьютер, входило в базу данных, базу персональных данных или работало с документами ограниченного характера;

- повышению защищенности персональных данных.

2. Повышение эффективности работы уполномоченных органов при профилактике правонарушений в сферах защиты персональных данных, разглашения государственных секретов и другой информации ограниченного характера, а также при выявлении и привлечения к ответственности виновных лиц.

Описанные результаты достигаются путем встраивания RFID-датчика в заднюю часть компьютерной мыши. При этом RFID-датчик дает возможность применения компьютерной мыши лишь при взаимодействии с чипом или другими устройствами с чипом, содержащими информацию о наличии у лица права доступа к данному компьютеру.

Такая компьютерная мышь особо ничем не отличается от обычных, для ее применения не требуется специальных компьютеров. Различие заключается лишь во встроенном RFID-датчике, который без взаимодействия с чипом блокирует возможность использования мыши, то есть она не

будет откликаться на действия пользователя. При этом сразу после взаимодействия датчика и чипа компьютерная мышь становиться активной, управление курсором и дача различных команд компьютеру становится возможным.

На фиг.1 показана компьютерная мышь со встроенным RFID-датчиком вид сверху (1 - RFID-датчик).

На фиг.2 показана компьютерная мышь со встроенным RFID-датчиком вид сбоку (1 - RFID-датчик).

На фиг.3 показана компьютерная мышь со встроенным RFID-датчиком вид сзади (1 - RFID-датчик).

На фиг.4 показан RFID-датчик.

В части технического обслуживания и эксплуатации не вызывает затруднений.

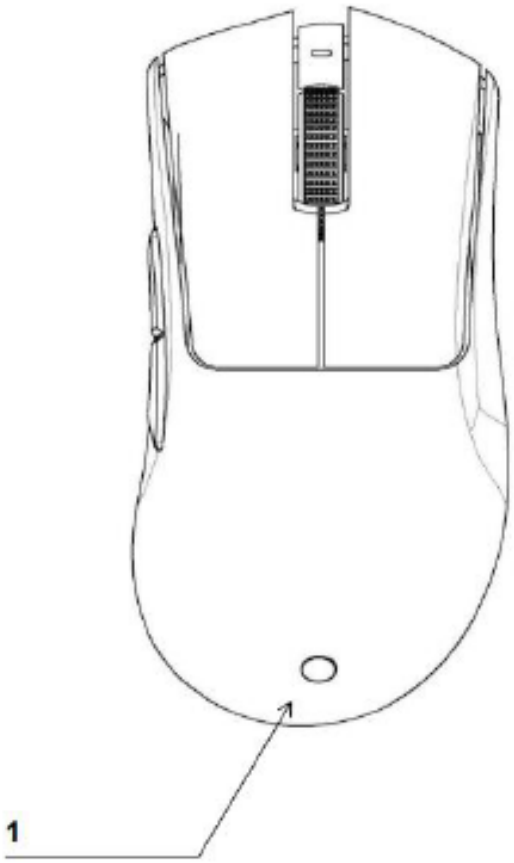
При разработке проекта приняты во внимание аспекты обеспечению максимальной функциональности, безопасности и оптимального комфорта.

Эксплуатировать компьютерную мышь со встроенным RFID-датчиком предполагается для информационной безопасности, защиты персональных данных в деятельности в деятельности правоохранительных и специальных органов, государственных служащих, НАО «Правительство для граждан», других организаций и лиц (частные судебные исполнители, нотариусы и др.), имеющих доступ к государственным базам данных, частных организаций, являющихся владельцами баз данных, а также любыми другими лицами, желающими ограничить возможность использования их компьютеров посторонними.

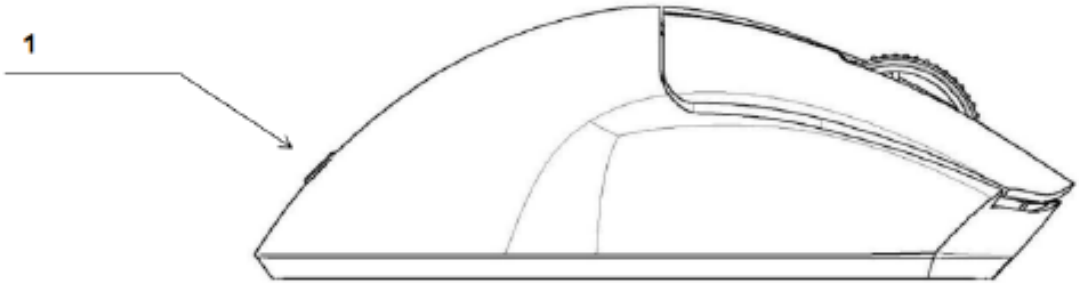
Аналогичной модели, как предлагаемая компьютерная мышь со встроенным RFID-датчиком, не существует.

ФОРМУЛА ПОЛЕЗНОЙ МОДЕЛИ

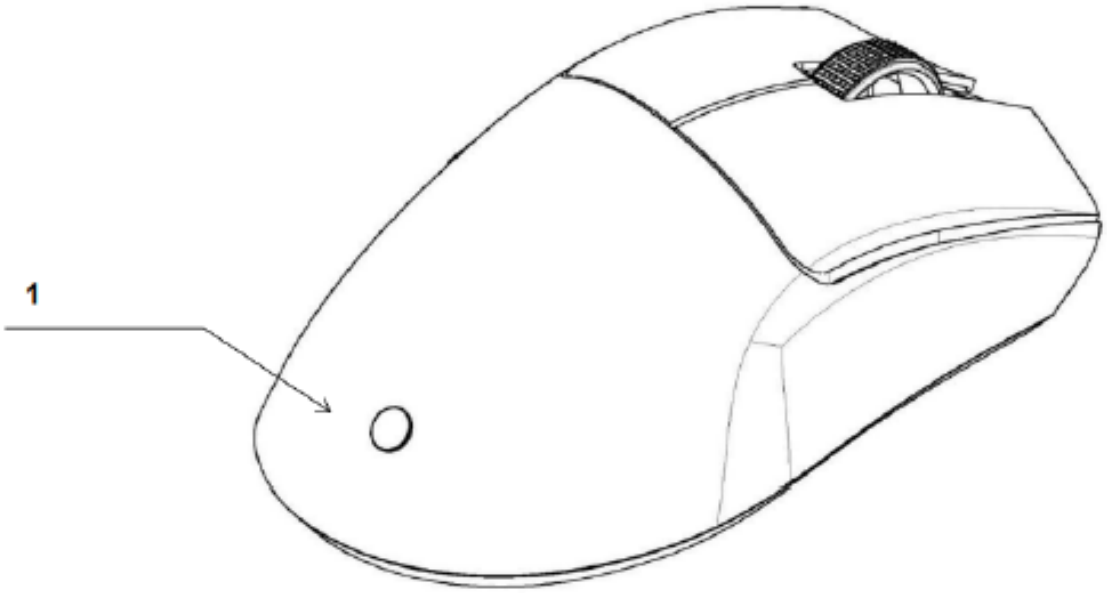
Компьютерная мышь со встроенным RFID-датчиком является компьютерным аксессуаром, состоящим из компьютерной мыши с частично встроенным в ее корпус RFID-датчиком, и данный аксессуар предназначен для фиксации всех сведений относительно пользователя компьютера, а также для предотвращения использования компьютеров лицами, не имеющими такого права.



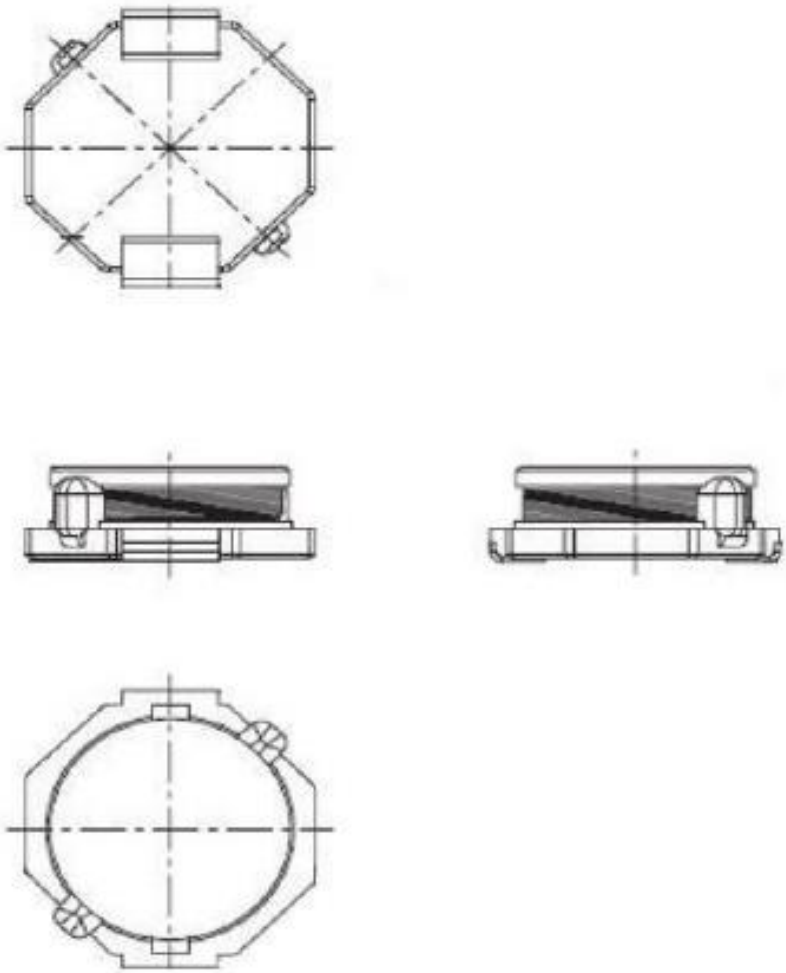
Фигура 1 (вид сверху)



Фигура 2 (вид сбоку)



Фигура 3 (вид сзади)



Фигура 4 (RFID-датчик)

Верстка Д. Женысова
Корректор Г. Косанова

ПРИЛОЖЕНИЕ Д

Проект

Паспорт персональных данных

1. Надпись на казахском и английском языках: «ҚАЗАҚСТАН РЕСПУБЛИКАСЫ» и «REPUBLIC OF KAZAKHSTAN», а также элементы национального узора;
2. Государственный Герб Республики Казахстан;
3. Надпись на казахском и английском языках: «ЖЕКЕ ДЕРЕКТЕР ПАСПОРТЫ» и «PERSONAL DATA PASSPORT»;
4. QR-код для доступа к электронной версии документа;
5. Элементы национального узора.

1. Государственный Герб Республики Казахстан, а также элементы национального узора;
2. Надпись на казахском, русском и английском языках: «Дербес деректер қорғалуға жатады, оған мемлекет кепілдік береді», «Персональные данные подлежат защите, которая гарантируется государством» и «Personal data shall be protected, as guaranteed by the state»;
3. Номер страницы;
4. Номер паспорта.

Деректер түрі
Вид данных

Фото

1. Тегі, аты, әкесінің аты / Ф.И.О.

2. Тегінді, атыңды немесе әкесінің атын өзгерту туралы ақпарат / Сведения об изменении фамилии, имени или отчества

3.Туған күн / Дата рождения

Деректер түрі
Вид данных

4. Жынысы / Пол

5. Жынысын ауыстыру туралы ақпарат / Сведения о смене пола

6. Туған жер / Место рождения

7. Тіркеу мекенжайы / Адрес прописки

8. Нақты тұрғылықты жері / Фактическое место проживания

9. Ұлты / Национальность

10. Руы / Родоплеменная принадлежность

Деректер түрі
Вид данных

11. Білім туралы ақпарат / Сведения об образовании

12. Отбасы жағдайы / Семейное положение

13. Ажыраскан некелердің болуы / Наличие расторгнутых браков

14. Балалы болу / Наличие детей

15. Алимент төлеу бойынша міндеттемелер / Наличие обязательств по уплате алиментов

16. Жылжымайтын мүліктің болуы / Наличие недвижимого имущества

Деректер түрі
Вид данных

17. Үшінші тұлғаларға, оның ішінде екінші деңгейлі банктерге қарыздың болуы / Наличие задолженности перед третьими лицами, в том числе банками второго уровня

18. Заңды тұлғаларға қатысу туралы мәліметтер / Сведения об участии в юридических лицах

19. Жұмыспен қамту туралы ақпарат / Сведения о трудоустройстве

20. Соттылықтың болуы немесе болмауы туралы мәліметтер / Сведения о наличии или отсутствии судимости

21. АҚТҚ жағдайы / ВИЧ-статус

Согласие на сбор и использование персональных данных

Я, *Ф.И.О. субъекта персональных данных* в соответствии со статьями 7, 8, 10, 24 Закона Республики Казахстан «О персональных данных и их защите» даю согласие *Ф.И.О. лица, кому предоставляются данные* на сбор и использование моих персональных данных согласно приложенному перечню без права их распространения и передачи третьим лицам (в т.ч. трансграничной) на срок до 3 месяцев, по истечении которого сведения подлежат уничтожению.

Я, *Ф.И.О. лица, кому предоставляются данные* в соответствии со статьями 7, 10, 11, 18, 22 Закона Республики Казахстан «О персональных данных и их защите» обязуюсь обеспечить конфиденциальных данных *Ф.И.О. субъекта персональных данных*, не допускать их распространения, передачи третьим лицам, а также использования вне целей сбора. При достижении целей сбора персональных данных либо по истечении 3 месяцев обязуюсь обеспечить их удаление.

Согласие составлено в двух экземплярах, имеющих одинаковую юридическую силу, и является обязательным для исполнения обоими сторонами. Нарушение условий согласия влечет установленную законодательством ответственность.

Приложение: Паспорт персональных данных на 2 листах.

Ф.И.О. _____ Ф.И.О. _____

субъект персональных данных *получатель персональных данных*

Дата _____ Дата _____

Подпись _____ Подпись _____

Таблица Д.1 - Содержание паспорта персональных данных

Вид персональных данных	Сведения субъекта персональных данных
Ф.И.О.	
Сведения об изменении фамилии, имени или отчества	
Дата рождения	
Пол	
Сведения о смене пола	
Место рождения	
Адрес прописки	
Фактическое место проживания	
Национальность	
Родоплеменная принадлежность	
Сведения об образовании	
Семейное положение	
Наличие расторгнутых браков	
Наличие детей	
Наличие обязательств по уплате алиментов	
Наличие задолженности перед третьими лицами, в том числе банками второго уровня	
Наличие недвижимого имущества	
Сведения об участии в юридических лицах	
Сведения о трудоустройстве	
Сведения о наличии или отсутствии судимости	
ВИЧ-статус	
Сведения о постановке на «Д» учет в медицинских учреждениях	
Сведения о наличии врожденных заболеваний	
Сведения о приобретенных заболеваниях, представляющих опасность для партнера и возможного потомства	
Сведения о постановке на учет в психоневрологическом и(или) наркологическом диспансере	

ПРИЛОЖЕНИЕ Е

Проект

Методические рекомендации
по организации прокурорского надзора за соблюдением законности
в сфере персональных данных и их защите

В 2013 году принят Закон Республики Казахстан «О персональных данных и их защите» (далее – Закон), статьей 28 которого на органы прокуратуры возложено осуществление высшего надзора за соблюдением законности в сфере персональных данных и их защиты.

Следует отметить, что в первоначальных редакциях Закона контрольными и надзорными функциями в сфере защиты персональных данных, была наделена только прокуратура. Аналогично и с правом возбуждения административных дел за нарушения в данной сфере. Таким образом, на тот момент прокуратура фактически являлась уполномоченным органом в данном направлении.

В 2020 году Законом Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий» введено понятие уполномоченного органа в сфере защиты персональных данных, которым определено Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан.

В соответствии с пунктом 4 статьи 5 Конституционного закона «О прокуратуре» (далее – Конституционный закон) при осуществлении надзора органы прокуратуры не подменяют функции иных государственных органов.

В этой связи важным является определение роли и места прокуратуры в сфере защиты персональных данных.

Деятельность органов прокуратуры основана на общих принципах, закрепленных Конституцией Республики Казахстан и статьей 3 Конституционного закона, которые применимы абсолютно ко всем отраслям, направлениям и видам прокурорского надзора, в том числе в сфере защиты персональных данных.

Основные отрасли прокурорского надзора определены пунктом 1 статьи 6 Конституционного закона. К ним относится надзор за законностью:

- деятельности государственных, местных представительных и исполнительных органов, органов местного самоуправления, учреждений, их должностных лиц, иных организаций независимо от форм собственности, а также принимаемых ими актов и решений;
- производства по делам об административных правонарушениях;
- досудебного расследования, уголовного преследования, оперативно-розыскной и контрразведывательной деятельности;
- исполнительного производства;
- судебных актов, вступивших в законную силу;

- исполнения уголовных наказаний и применения иных мер государственного принуждения;

- государственной правовой статистики и специальных учетов;

- соблюдения международных обязательств Республики Казахстан.

Прокурорский надзор в сфере защиты персональных данных может осуществляться по всем данным отраслям. При этом анализ законодательства, научной литературы и методики показывает, что прокурорский надзор в сфере защиты персональных построен на принципах:

- признания права неприкосновенности частной жизни, личной и семейной тайны, защиты чести и достоинства, а также права на защиту персональных данных;

- справедливости;

- беспристрастности;

- объективности;

- эффективности;

- профессионализма, компетентности и постоянного повышения профессионального уровня;

- своевременности реагирования на факты нарушения законодательства в сфере персональных данных и их защиты;

- сохранности и недопустимости разглашения документов, сведений и иной информации, полученных в ходе осуществления своей деятельности и содержащих персональные данные;

- персональной ответственность за разглашение сведений, составляющих охраняемую законом тайну и информацию;

- защиты персональных данных потерпевших и других участников уголовного процесса;

- воспрепятствования разглашению персональных данных из досудебных производств и закрытых судебных разбирательств;

- принципиальной позиции в вопросе устранения нарушений законодательства в сфере персональных данных и их защите, а также в возмещении вреда и привлечении к ответственности виновных лиц;

- принятия исчерпывающих мер по обеспечению законности, защите и восстановлению нарушенных прав и свобод человека и гражданина, охраняемых законом интересов юридических лиц, общества и государства в сфере персональных данных и их защиты.

Исходя из обширного разнообразия междисциплинарных и отраслевых основополагающих начал, охватывающих исследуемую совокупность, в качестве ключевого принципа прокурорского надзора в сфере защиты персональных данных следует определить принятие исчерпывающих мер по обеспечению законности, защите и восстановлению нарушенных прав и свобод человека и гражданина, охраняемых законом интересов юридических лиц, общества и государства в сфере персональных данных и их защиты.

Необходимо отметить, что статьей 4 Конституционного закона определены цели и задачи прокуратуры, к которым отнесены защита и

восстановление нарушенных прав и свобод человека и гражданина, охраняемых законом интересов юридических лиц, общества и государства, выявление и устранение нарушений законности, их причин, условий и последствий, координация деятельности правоохранительных и иных государственных органов по обеспечению законности, правопорядка и борьбы с преступностью, а также иные задачи, определяемые законодательством.

Таким образом, при осуществлении прокурорского надзора в сфере защиты персональных данных следует руководствоваться данными целями и задачами.

Для осуществления прокурорского надзора в сфере защиты персональных данных прокурор наделен значительным арсеналом правовых средств, к которым следует относить:

- проверку соблюдения законности в сфере защиты персональных данных;
- анализ состояния законности в сфере защиты персональных данных;
- оценку актов в сфере обработки персональных данных, вступивших в законную силу;
- рассмотрение обращений о нарушениях законодательства о персональных данных и их защите;
- инициирование досудебного расследования;
- инициирование производства по делам об административных правонарушениях по фактам нарушения законодательства в сфере персональных данных и их защиты;
- требование от уполномоченного органа в сфере защиты персональных данных проведения внеплановой проверки по конкретным фактам причинения либо об угрозе причинения вреда правам и законным интересам физических и юридических лиц, государства;
- дача уполномоченному органу в сфере защиты персональных данных обязательного для исполнения указания по вопросам внеплановой проверки, проводимой по требованию прокурора;
- требование от уполномоченного органа в области масс-медиа принятия мер по временному приостановлению доступа к объектам информатизации в виде программного обеспечения и интернет-ресурса и (или) размещенной на них информации;
- прекращение незаконных оперативно-розыскных мероприятий и негласных следственных действий;
- обеспечение конфиденциальности данных досудебных расследований и закрытых судебных разбирательств;
- назначение экспертиз, в том числе судебных технологических экспертиза, судебно-экспертных исследований средств компьютерной технологии;
- межведомственное взаимодействие в сфере защиты персональных данных, в том числе межведомственных совещаний;

- взаимодействие с Уполномоченным по правам человека по вопросам защиты персональных данных граждан;

- проведение заседаний Координационного совета по обеспечению законности, правопорядка и борьбы с преступностью по вопросам совершения преступлений в отношении охраняемой законом информации, а также преступлений, совершенных с использованием похищенных персональных данных;

- проведение коллегий по вопросам защиты персональных данных;

- подписание меморандумов с ведущими организациями в области цифрового права и защиты персональных данных;

- участие в нормотворческой деятельности в целях совершенствования законодательства о персональных данных и их защите.

Статьей 17 Конституционного закона определено, что высший надзор от имени Республики Казахстан осуществляется посредством проведения проверки соблюдения законности, анализа состояния законности, оценки актов, вступивших в силу.

Проверки соблюдения законности в сфере защиты персональных данных должны быть 2 видов: предметные, направленные на проверку соблюдения законности в сфере применения законодательства о персональных данных и их защите, а также тематические, то есть проводимое по иным вопросам, но с выключением в предмет проверки вопроса защиты персональных данных.

Предметные проверки могут проводиться:

1. В деятельности уполномоченного органа в сфере защиты персональных данных по вопросам реализации государственной политики и государственного контроля в сфере персональных данных и их защиты, организации деятельности консультативного совета по вопросам персональных данных и их защиты, а также реализации иных полномочий, предусмотренных законодательством.

2. В деятельности государственных органов и их должностных лиц по вопросам соблюдения законодательства о персональных данных и их защите. Такие проверки в большей степени будут иметь отраслевой характер, то проводиться, например, в сфере законности исполнительного производства, государственной правовой статистики, исполнения уголовных наказаний и применения иных мер государственного принуждения, по линии оперативно-розыскной и контрразведывательной деятельности и т.д. При этом особую роль, безусловно, будут иметь проверки законности оперативно-розыскной и контрразведывательной деятельности.

3. В деятельности местных исполнительных органов по вопросам реализации их компетенции, в том числе по осуществлению государственного контроля за соблюдением законодательства о персональных данных и их защите в отношении субъектов частного предпринимательства.

4. В деятельности квазигосударственных организаций, государственных учреждений (школы, больницы и т.д.), коммунальных предприятий, других организаций, в деятельности которых осуществляется сбор и обработка

большого количества персональных данных по вопросам соблюдения законодательства, в том числе в части сохранности и конфиденциальности персональных данных, недопущения их сбора в излишнем количестве.

5. В деятельности собственников и операторов баз, содержащих персональные данные, в части соблюдения предусмотренных Законом «О персональных данных и их защиты», иными законодательными актами обязательств и недопущения нарушений прав субъектов персональных данных, а также относительно надлежащей деятельности лиц, ответственных за организацию обработки персональных данных.

6. В деятельности правоохранительных, специальных и иных государственных органов относительно законности получения пользователями сведений из СИО ПСО, ЕРДР, ЕРАП и других информационных систем.

Следует отметить, что имеется множество проблем и нередки случаи доступа к персональным данных посторонних лиц.

К примеру, 22.12.2020 года в г.Нур-Султан осуждены 5 бывших и действующих сотрудников полиции, которые за вознаграждение предоставили третьим лицам право пользования базами Министерства внутренних дел и Генеральной прокуратуры, содержащим персональные данные.

7. В иных случаях, в том числе по поручениям Президента и Генерального Прокурора Республики Казахстан.

Тематические проверки с выключением в предмет проверки вопроса защиты персональных данных могут проводится по всем отраслям и направлениям прокурорского надзора. При этом что упор должен быть на неопределенный круг лиц, защиту прав уязвимых слоев, несовершеннолетних и лиц, которые не могут себя защитить.

В Казахстане отмечается значительный уклон в сторону цифрового здравоохранения, внедрен электронный паспорт здоровья, что предполагает структурирование персональных медицинских данных о состоянии здоровья физического лица и оказываемой ему медицинской помощи на протяжении всей жизни, ведется сбор большого количества персональных медицинских данных и сведений, относящихся к тайне медицинского работника.

Указанные обстоятельства, наряду с предоставлениям права доступа к персональным медицинским данным большому количеству организаций, в том числе поставщикам медицинских и фармацевтических услуг, организации, ответственной за финансовое возмещение затрат на оказание медицинской помощи, уполномоченным органам в сфере здравоохранения и в области социальной защиты населения и другим, значительно увеличивает риски утечки личной медицинской информации.

Медицинские персональные данные, в особенности лиц, которые не могут себя защитить самостоятельно, нередко используются для совершения противоправных действий. Так, в г.Алматы на протяжении 10 лет устойчивая преступная группа, имеющая в составе работников Центра психологического здоровья, используя доступ к данным пациентов, определяла одиноких людей с психическими расстройствами, у которых имелась в собственности

недвижимость. В дальнейшем эти люди похищались и содержались в неволе, а некоторые были убиты. Их собственность незаконно отбиралась и реализовывалась. В настоящее время проходит судебный процесс в отношении 22 обвиняемых лиц.

Поэтому при проверках соблюдения законодательства о здравоохранении целесообразно включать в предмет проверки защиту персональных медицинских данных пациентов. Внимание следует обращать и на работу информационных систем в сфере медицины. Например, пользователи приложения «Damumed» зачастую указывают о наличии записей о получении медицинских услуг, которые фактически не оказывались. Также допускается ошибочное указание наличия психических, неврологических и других расстройств. Не исключены факты использования персональных данных граждан для фиктивного указания и повышения объема оказанных медицинских услуг для последующего получения оплаты.

Вопрос защищенности персональных данных следует включать в проверки трудового законодательства.

В соответствии с требованием Трудового кодекса работник имеет право на обеспечение защиты персональных данных, хранящихся у работодателя, а работодатель обязан осуществлять сбор, обработку и защиту персональных данных работника в соответствии с законодательством о персональных данных и их защите.

Между тем, на практике зачастую требования не соблюдаются, персональные данные работников предоставляются третьим лицам, работодатели требуют от работников непредусмотренные законодательством персональные сведения, в том числе о наличии или отсутствии судимости и другие. В государственных учреждениях выявляются многочисленные факты фиктивной оплаты трудовой деятельности «мертвых душ» путем использования персональных данных лиц, которые не имеют никакого отношения к данной организации.

Антикоррупционной службой установлена устойчивая организованная преступная группа, которая с января 2020 года по март 2023 года на системной основе занималась хищением бюджетных средств путем перечисления заработной платы физическим лицам, фактически не работавшим в сфере образования, а также на свои личные счета. В результате преступных действий государству причинен ущерб в размере 4,3 миллиарда тенге.

В Туркестанской области органами прокуратуры выявлена преступная, которая путем манипуляций с персональными данными похитила более 4 миллиардов бюджетных средств. В частности, работниками числились одни лица, но для перечисления заработной платы были указаны реквизиты других лиц.

Таким образом, по проверкам в сфере труда возможно выявление многочисленных нарушений прав работников по защите персональных данных, в связи с чем целесообразно в предмет комплексных проверок включать и этот вопрос.

Серьезные нарушения защищенности персональных данных могут выявляться при проверках защиты прав несовершеннолетних.

По проверкам усыновления детей-сирот следует отметить, что в соответствии с пунктом 4 статьи 84 Кодекса «О браке (супружестве) и семье» дети, являющиеся гражданами Республики Казахстан, состоящие на централизованном учете в Республиканском банке данных, могут быть переданы на усыновление иностранцам только в случаях, если ребенок не может быть усыновлен родственниками, гражданами Республики Казахстан, проживающими на территории страны и за ее пределами.

По сведениям из отдельных источников, должностные лица интернатных учреждений зачастую приписывают здоровым детям серьезные заболевания, отягощённую наследственность (якобы родители алкоголики, наркоманы, психбольные и т.д.), что отпугивает потенциальных усыновителей из числа родственников и граждан Казахстана.

После отказа в усыновлении ребенка казахстанцами, они передаются на усыновление иностранцам. Однако, при повторном обследовании детей за рубежом каких-либо заболеваний не выявляют.

Поэтому в целях исключения возможных коррупционных проявлений (подарков, денежных вознаграждений от иностранных граждан), со стороны должностных лиц, за одобрение усыновления казахстанских детей, полагаем целесообразным введение практики перепроверки персональных медицинских данных и обоснованности диагнозов, выставленных детям, в особенности новорожденным и в возрасте до 3 лет.

Еще одной серьезной проблемой является ненадлежащее ведение «Черного списка усыновителей», а именно не включение в него персональных данных некоторых лиц. Прокурорами установлено 67 таких фактов. Это приводит к тому, что детей передаются ранее судимым, а также состоящим на наркологическом и психиатрическом учетах лицам.

К примеру, в 2018 году в Восточно-Казахстанской области под опеку переданы двое детей в г.Актобе семейной паре. При этом супруг был судим за изнасилование несовершеннолетней, совершенное группой лиц.

Администрация медико-социальных учреждений для детей-инвалидов, интернатов для детей-сирот и других подобных учреждений нередко, имея доступ к персональным данным воспитанников, допускает неправомерное использование их денежных средств. Схожие нарушения допускаются и в учреждения для взрослых лиц с различными заболеваниями. К примеру, в 2022 году судом Абайским районным судом Карагандинской области осуждены руководитель Центра оказания специальных социальных услуг, 2 сотрудника Медико-социального учреждения престарелых инвалидов, а также почтальон отделения АО «Казпочта», которые в группе лиц похищали денежные средства у пенсионеров и инвалидов. Так, должностные лица, имея доступ к персональным данным подопечных, в том числе к их диагнозам и сведениям о состоянии здоровья, ежемесячно формировался список, в который включались лиц, не способных самостоятельно распоряжаться своими денежными

средствами. Этот список направлялся почтальону АО «Казпочта», которая получала денежные средства за данных лиц. В дальнейшем подделывались подписи в ведомостях, а денежные средства распределялись.

Социальные работники имеют доступ к многочисленным персональным данным получателей специальных социальных услуг, информации об индивидуальных особенностях лиц, нуждающихся в специальных социальных услугах, состоянии здоровья, диагнозе заболевания, степени ограничения жизнедеятельности, что составляет профессиональную тайну социального работника. Недостаточная защищенность такой информации может повлечь существенный вред.

При проверках финансового законодательства в деятельности банков целесообразно включение вопроса защищенности персональных данных клиентов. Например, в 2024 году Алмалинским районным судом г.Алматы по уголовным делам осужден А., ранее занимавший должность заместителя директора отделения одного из банков, которым со счетов клиентов банка похищено более 200 миллионов тенге. Пользуясь наличием доступа к персональным данным клиентов, А. определял лиц, у которых на счетах имеются значительные денежные суммы. В дальнейшем в информационной системе изменялся доверенный номер клиента, что давало А. доступ к управлению счетом и возможность для вывода денежных средств на подконтрольные ему счета.

Имея доступ к персональным данным, сотрудники банков могут совершать и другие противоправные действия. К примеру, в 2024 году Межрайоным судом по уголовным делам г.Астана осужден юрисконсульт одного из банков, который в поступивших к нему документах увидел данные своего знакомого, о чем сообщил ему, чем допустил срыв специальной операции органов национальной безопасности, направленной на пресечение канала поставки огнестрельного оружия и боеприпасов.

При проведении проверок в местах лишения свободы следует применять опыт Российской Федерации по искоренению мошеннических колл-центров путем выявления с помощью радиомониторинга абонентских номеров, используемых заключенными, и их последующего блокирования.

Таким образом, в ходе комплексных проверок практически по всем направлением возможно включение в виде дополнительного вопроса соблюдение законности в сфере персональных данных и их защите.

В сфере государственной правовой статистике следует проводить периодические проверки по вопросу соблюдения конфиденциальности сведений, получаемых при использовании СИО ПСО, ЕРДР, ЕРАП и других информационных систем органов прокуратуры.

Анализ состояния законности должен проводиться по важным вопросам защищенности персональных данных.

В первую очередь, необходим глубокий и всесторонний анализ следственно-судебной практики по фактам нарушения законодательства о персональных данных.

Несмотря на кажущуюся на первый взгляд детальную проработку норм об ответственности за нарушение законодательства в сфере персональных данных и их защите, уровень выявляемых в этой сфере уголовных правонарушений не отражает реальной ситуации с защищенностью персональных данных в стране.

За более чем 10 лет (с 2013 года) по статье 147 (в утратившей силу редакции - статья 142) Уголовного кодекса за нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите зарегистрировано 418 фактов, по которым судами осуждено 39 лиц, 79 лиц оправдано, 27 уголовных дел прекращено по реабилитирующим основаниям. Более 60% возбужденных уголовных дел прекращены по реабилитирующим основаниям. За неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций по статье 205 Уголовного кодекса с 2015 года зарегистрировано 408 уголовных дел, из которых только одно дошло до суда и одно лицо было осуждено. За неправомерное уничтожение или модификацию информации по статье 206 Уголовного кодекса с 2015 года зарегистрировано 161 уголовное дело, из которых до суда дошли 9 дел, из них 1 дело прекращено, 3 возвращены прокурору, по 5 делам состоялись приговоры: 6 лиц осуждены, 1 лицо оправдано. Схожая ситуация и по статьям 207-210 Уголовного кодекса.

Изучение уголовных дел показало, что зачастую отсутствует надлежащая квалификация таких деяний. К примеру, в 2024 году значительный резонанс в обществе получило уголовное дело в отношении бывшего супруга известной тележурналистки Д.Н., который под угрозой распространения ее интимных изображений требовал передать ему имущество при разводе, хотя оно было приобретено Д.Н. до вступления в брак. Основываясь на сведениях, опубликованных Д.Н., ее бывший супруг был осужден по части 4 статьи 147 Уголовного кодекса. В данном случае была необходима дополнительная квалификация деяний по пункту 2 части 3 или пункту 2 части 4 статьи 194 Уголовного кодекса, а именно за вымогательство под угрозой распространения сведений, позорящих потерпевшего с целью получения имущества в крупном размере (или в особо крупном размере).

В соответствии с пунктом 5 Нормативного постановления Верховного Суда Республики Казахстан от 23.06.2006 года № 6 «О судебной практике по делам о вымогательстве» под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, оглашение которых может причинить существенный вред интересам потерпевшего или его близких, следует понимать требование передачи чужого имущества либо права на имущество или совершения других действий имущественного характера, сопровождающееся угрозой разглашения любых сведений, которые могут нанести вред чести и достоинству потерпевшего. При этом не имеет значения, соответствуют ли действительности сведения, под угрозой разглашения которых совершается вымогательство. В то же время необходимо иметь в виду, что потерпевший стремится сохранить эти сведения в тайне, а угроза их

разглашения используется виновным, чтобы принудить его к выполнению выдвинутых требований.

Существенный вред может быть причинен распространением сведений, позорящих потерпевшего. При определении существенного вреда учитывается как субъективная оценка потерпевшим тяжести причиненного ему нравственного ущерба, так и объективные данные, свидетельствующие о степени нравственных и физических страданий потерпевшего в результате вымогательства, совершенного под угрозой распространения порочащих сведений.

Следует отметить, что распространение интимных фотографий встречается достаточно часто, но единой практики до настоящего времени не имеется. Так, в 2023 году в г.Алматы судом оправдан Д., отправивший интимные фотографии своей бывшей супруги ее родителям и родственникам. В свою очередь в 2024 году за такие же действия в Западно-Казахстансой области осужден И., а в г.Талдыкорган в 2023 году осужден Е., который отправил близким родственникам своей бывшей девушки ее фото и видео интимного характера, а также от ее имени зарегистрировался в социальных сетях, публиковал в них указанные изображения, а также объявления об оказании его бывшей девушкой интимных услуг.

Нельзя не подчеркнуть, что в настоящее время многие другие преступления совершаются под угрозой распространения интимных фотографий или видеозаписей. Так, в 2024 году резонанс получил случай в Кызылординской области, где 11 человек под угрозой распространения персональных данных в виде интимных фото и видео вовлекли несовершеннолетнюю в занятие проституцией. В этом же году в г.Туркестан 33-летний мужчина под угрозой аналогичных действий совершил изнасилование несовершеннолетней и вымогал у нее денежные средства. В целом, таких примеров немало.

Еще одним важным направлением для проведения прокурорами анализа состояния законности является соблюдение средствами массовой информации законодательства при сборе и обработке персональных данных, поскольку средствами массовой информации нередко допускается сбор и публикация персональных данных граждан без их согласия.

К примеру, в 2022 году журналист К.М. обратился к сотруднику военной полиции К.К. для оказания содействия в получении персональных данных нескольких лиц, в отношении которых он осуществлял ряд публикаций негативного характера. К.К., используя доступ к информационным системам, осуществил незаконный сбор персональных данных (об адресе регистрации, месте жительства, находящихся в собственности автотранспортных средствах, используемых номерах телефонов, документах, удостоверяющих личность и другие) и передал их журналисту К.М., который в дальнейшем использовал эти в своих публикациях для создания негативного образа в отношении лиц, данные которых получил. В 2023 году Военным судом Алматинского гарнизона журналист К.М. и сотрудник военной полиции К.К. осуждены.

Между тем, в средствах массовой информации имеется немало других публикаций, в содержании которых упоминаются персональные данные граждан, происхождение которых остается неизвестным.

Имеют место явные нарушения законодательства. К примеру, начиная с марта 2024 года, во многих масс-медиа опубликована информация, что сын одного из акимов района Павлодарской области избил в школе одну из учениц. В публикациях размещены фото и видеоизображения предполагаемого правонарушителя, сведения о месте работы его обоих родителей. При этом в соответствии с подпунктом 2 пункта 3-4 статьи 14 Закон «О средствах массовой информации» запрещается распространение в средствах массовой информации или сетях телекоммуникаций персональных и биометрических данных лица, включая информацию об его родителях и иных законных представителях, иной информации, позволяющей установить личность, о несовершеннолетних, подозреваемых и (или) обвиняемых в совершении административных и (или) уголовных правонарушений. 19.06.2024 года данный закон утратил силу ввиду принятия нового Закона «О масс-медиа», в котором аналогичная норма сохранилась.

Анализа требует деятельность блоггеров, которыми нередко распространяются персональные данные. К примеру, в 2022 году Талдыкорганским городским судом Алматиснкой области осужден блоггер А., который на своих страницах с аудиторией более 120 тысяч человек распространил сведения о том, что К. состоит на учете в психоневрологическом диспансере.

Отдельного анализа требует вопрос недопущения нарушения законодательства о персональных данных и их защите при применении в Казахстане OSINT-инструментов.

Результаты проверок и анализов следует использовать в работе органов прокуратуры по межведомственному взаимодействию в сфере защиты персональных данных, для проведения заседаний Координационного совета по обеспечению законности, правопорядка и борьбы с преступностью по вопросам совершения преступлений в отношении охраняемой законом информации, а также преступлений, совершенных с использованием похищенных персональных данных, проведения коллегий по вопросам защиты персональных данных.

Целесообразно также подписание меморандумов с ведущими организациями в области цифрового права и защиты персональных данных.

Оценке подлежат нормативные правовые акты в сфере персональных данных и их защиты акты центральных государственных органов, правовые акты уполномоченного органа, акты операторов и собственников баз данных об утверждении перечней персональных данных, необходимых и достаточных для выполнения осуществляемых ими задач, а также определяющие политику в отношении сбора, обработки и защиты персональных данных и другие акты в данной сфере.

Результаты проверок, анализов, а также оценки, актов вступивших в законную силу, было бы эффективным использовать и для участия прокурора в нормотворческой деятельности в целях совершенствования законодательства о персональных данных и их защите.

Таким образом, в целях совершенствования прокурорского надзора в сфере персональных данных и их защите необходимо использование всего арсенала правых средств прокурора, а основными правовыми инструментами буду являться проверка, анализ и оценка актов, вступивших в силу.

ПРИЛОЖЕНИЕ Ж

Акты внедрения

БЕКІТЕМІН
Бас прокуратураның 1-Қызметінің қылмыстық заңнаманы қолдану тобының жетекшісі
Ж. Жақсылықбаева
2023 жылғы «27» 12

Диссертациялық зерттеу нәтижелерін практикаға енгізу
АКТІСІ

Комиссия құрамы:
Төраға – топ басшысы Бас прокуратураның 1-Қызметінің қылмыстық заңнаманы қолдану тобының жетекшісі **Ж. Жақсылықбаева**.
және комиссия мүшелері:
Бас прокуратураның 1-Қызметінің қылмыстық заңнаманы қолдану тобының Бас Прокурорының көмекшісі Е. Алмазұлы;
Бас прокуратураның 1-Қызметінің қылмыстық заңнаманы қолдану тобының аға прокуроры М. Джанунц;
Бас прокуратураның 1-Қызметінің қылмыстық заңнаманы қолдану тобының аға прокуроры Ә. Жүсіпов.

Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясының докторанты А.М. Әміровтің «Жеке деректер мен оны қорғау саладағы заңдылықтың сақталуын прокурорлық қадағалау» атты диссертациялық зерттеу шеңберінде зорлық-зомбылық құрбандарын бүркеншік атау ұсынысы Бас прокуратураның Сотқа дейінгі тергеп-тексерудің заңдылығын қадағалау және қылмыстық қудалау қызметі қылмыстық заңнаманы қолдану тобының практикасына енгізілгендігі жөнінде актіні жасады.

Комиссия төрағасы:
Бас прокуратураның 1-Қызметінің қылмыстық заңнаманы қолдану тобының жетекшісі **Ж. Жақсылықбаева**

Бас прокуратураның 1-Қызметінің қылмыстық заңнаманы қолдану тобының Бас Прокурорының көмекшісі **Е. Алмазұлы**

Бас прокуратураның 1-Қызметінің қылмыстық заңнаманы қолдану тобының аға прокуроры **М. Джанунц**

Бас прокуратураның 1-Қызметінің қылмыстық заңнаманы қолдану тобының аға прокуроры **Ә. Жүсіпов**

«УТВЕРЖДАЮ»
Директор Института
профессионального обучения
Абдухманов М.Ш.
«___» _____ 2024 г.

Акт
внедрения результатов диссертационного исследования докторанта Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан

Комиссия в составе:
председателя: Заведующей кафедрой прокурорского надзора Балтабаевой Ж.Б.
и членов комиссии:
1) Доцента кафедры прокурорского надзора Утепова Д.П.
2) Доцента кафедры прокурорского надзора Шаншарбаевой Л.С.

Составили настоящий акт о том, что материалы диссертационного исследования докторанта
Амирова Алмаса Муратовича
на тему Прокурорский надзор за соблюдением законности в сфере персональных данных и их защиты

внедрены в практическую деятельность, научную деятельность, учебный процесс
(подчеркнуть нужное)

1. Краткая аннотация внедрения диссертационного исследования докторанта *(указать использованный пункт, положение, главу, раздел)*
При проведении курсов первоначальной профессиональной подготовки лиц, поступающих на службу в органы прокуратуры, использованы пп. 1.2 (Основополагающие принципы и алгоритмы прокурорского надзора в сфере защиты персональных данных), 2.1 (Правовая регламентация средств прокурорского надзора в сфере защиты персональных данных), 3.2 (Рекомендации по комплексному совершенствованию прокурорского надзора в сфере персональных данных и их защите), а также 3, 4 и 6 положения диссертации

2. Форма внедрения диссертационного исследования докторанта:
12.11.2024 года докторантом Амировым А.М. прочитаны 4 лекции на тему: «Прокурорский надзор за соблюдением законности в сфере персональных данных и их защиты» для групп № 1, 2, 3 и 4 курсов первоначальной

профессиональной подготовки лиц, поступающих на службу в органы прокуратуры

(указать форму конечного продукта (законодательная инициатива, приказ, служебная записка, справка, инструкция, методическая рекомендация либо лекции, видеолекции, учебное пособие и др.) с приложением копии внедренного продукта, удостоверенного подписью уполномоченного лица (председателя комиссии), подписывающего акта.

3. Эффективность внедрения диссертационного исследования докторанта:
Актуальность диссертационного исследования и его внедрения не вызывает сомнений. Лекции Амирова А.М. содержали в себе теоретические основы и практику осуществления прокурорского надзора в сфере защиты персональных данных, что вызвало значительный интерес со стороны обучающихся на курсах первоначальной профессиональной подготовки лиц.

4. Дата внедрения диссертационного исследования докторанта: 12.11.2024 года.

Председатель: _____ Ж. Балтабаева
(подпись, Ф.И.О.)

Члены комиссии: _____ Д. Утепов
(подпись, Ф.И.О.)

_____ Л. Шаншарбаева
(подпись, Ф.И.О.)

ТОО "Центр цифровых прав Казахстан"
050022, Казахстан, г. Алматы, ул. Байзакова, 280, SmArt.Point
Тел: +7 (775) 007-81-99 E-mail: kz@drc.law www.drc.law/kz/

Исх. № 078008 20 ноября 2024

«УТВЕРЖДАЮ»
_____
Основатель Eurasian Digital Foundation
Управляющий партнер
«Digital Rights Center Qazaqstan»
Р. Дайырбеков

Акт
внедрения результатов диссертационного исследования докторанта Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан

Комиссия в составе:

председателя: Teaching professor, Заместителя директора Высшей школы права Maqsut Narikbayev University, Директора Digital Rights Center Qazaqstan в МФЦА Утеген Д.

и членов комиссии:

1) Старшего юриста Digital Rights Center Qazaqstan (DRCQ), AIFC Legal Adviser Кабышева Е.

2)Юриста DRCQ, Ожерельев В.

Составили настоящий акт о том, что материалы диссертационного исследования докторанта Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан

Амирова Алмаса Муратовича

на тему Прокурорский надзор за соблюдением законности в сфере персональных данных и их защиты

внедрены в **практическую деятельность**, научную деятельность, учебный процесс

(подчеркнуть нужное)

ТОО "Центр цифровых прав Казахстан"
050022, Казахстан, г. Алматы, ул. Байзакова, 280, SmArt.Point
Тел: +7 (775) 007-81-99 E-mail: kz@drc.law www.drc.law/kz/

1. Краткая аннотация внедрения диссертационного исследования докторанта *(указать использованный пункт, положение, главу, раздел)*

Значительный интерес представил раздел 3.2 (Рекомендации по комплексному совершенствованию прокурорского надзора в сфере персональных данных и их защите) диссертации Амирова А.М. в части имеющихся правоприменительных проблем, способствующих ненадлежащей квалификации деяний, а также препятствующих привлечению к уголовной ответственности лиц за нарушение неприкосновенности частной жизни и законодательства о персональных данных и их защите. Кроме того, интерес вызывают предложенные концептуальные подходы модернизации уголовной политики по защите персональных данных, содержащиеся в 3 положении диссертации Амирова А.М.

2. Форма внедрения диссертационного исследования докторанта:

08.11.2024 года докторантом Амировым А.М. проведена гостевая лекция в рамках работы Центра практики, карьеры и трудоустройства Высшей школы права Maqsut Narikbayev University касательно соблюдения законности в сфере законодательства о персональных данных и их защите. Кроме того, Амировым А.М. компании «Digital Rights Center Qazaqstan» предоставлена справка с анализом судебно-следственной практики по статьям Уголовного кодекса, связанным с неправомерным распространением и обработкой персональных данных, которая будет использована в дальнейшей работе компании, в том числе при участии в рабочих группах по разработке и совершенствованию цифрового законодательства и законодательства о персональных данных.

(указать форму конечного продукта (законодательная инициатива, приказ, служебная записка, справка, инструкция, методическая рекомендация либо лекции, видеолекции, учебное пособие и др.) с приложением копии внедренного продукта, удостоверенного подписью уполномоченного лица (председателя комиссии), подписывающего акта.

3. Эффективность внедрения диссертационного исследования докторанта:

Актуальность диссертационного исследования и его внедрения не вызывает сомнений. Гостевая лекция Амирова А.М. содержала значительный объем полезной информации, что вызвало оживленный интерес со стороны студентов и преподавателей университета (лекцию посетили около 40 человек). Поднимаемые вопросы в справке отражают серьезные проблемы уголовно-правового механизма защиты персональных данных граждан.

4. Дата внедрения диссертационного исследования докторанта: 14.11.2024 года.

Председатель: _____ Д. Утеген
(подпись, Ф.И.О.)

Члены комиссии: _____ Е. Кабышев
(подпись, Ф.И.О.)

ТОО "Центр цифровых прав Казахстан"
050022, Казахстан, г. Алматы, ул. Байзакова, 280, SmArt.Point
Тел: +7 (775) 007-81-99 E-mail: kz@drc.law www.drc.law/kz/

Ожерельев В.
(подпись, Ф.И.О.)

С уважением,
Руслан Дайырбеков

Управляющий партнер DRCQ

«УТВЕРЖДАЮ»

И.о. Ректора Академии правосудия
при Высшем Судебном Совете
Республики Казахстан
к.ю.н., доцент
Мусин К.К.

«29» 11 2024 г.

Акт
внедрения результатов диссертационного исследования докторанта Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан

Комиссия в составе:

председателя: И.о. директора научно-образовательного центра уголовно-правовых дисциплин Академии правосудия при Высшем Судебном Совете Республики Казахстан, к.ю.н., Сембековой Б.Р.
и членов комиссии:

1) Доцента научно-образовательного центра уголовно-правовых дисциплин Академии правосудия при Высшем Судебном Совете Республики Казахстан, к.ю.н., Жаксыбековой Ф.С.

2) Доцента научно-образовательного центра уголовно-правовых дисциплин Академии правосудия при Высшем Судебном Совете Республики Казахстан, к.ю.н., Мусеновой Э.Е.

Составили настоящий акт о том, что материалы диссертационного исследования докторанта
Амирова Алмаса Муратовича
на тему Прокурорский надзор за соблюдением законности в сфере персональных данных и их защиты

внедрены в практическую деятельность, научную деятельность, **учебный процесс**
(подчеркнуть нужное)

1. Краткая аннотация внедрения диссертационного исследования докторанта *(указать использованный пункт, положение, главу, раздел)*

При проведении обучения магистрантов Академии правосудия при Высшем Судебном Совете Республики Казахстан использованы пп. 1.1 (Современное состояние и перспективы соблюдения законности в сфере персональных данных и их защите), 2.3 (Особенности применения

современных технологий в деятельности прокурора по защите персональных данных) и 3.1 (Анализ целесообразности и возможности имплементации в Республике Казахстан передового опыта защиты персональных данных) диссертации Амирова А.М.

2. Форма внедрения диссертационного исследования докторанта:

28.11.2024 года докторантом Амировым А.М. прочитана лекция в онлайн-формате на тему: «Защита персональных данных в Республике Казахстан» для магистрантов Академии правосудия при Высшем Судебном Совете Республики Казахстан (40 человек)

(указать форму конечного продукта (законодательная инициатива, приказ, служебная записка, справка, инструкция, методическая рекомендация либо лекции, видеолекции, учебное пособие и др.) с приложением копии внедренного продукта, удостоверенного подписью уполномоченного лица (председателя комиссии), подписывающего акта.

3. Эффективность внедрения диссертационного исследования докторанта:
Актуальность диссертационного исследования и его внедрения не вызывает сомнений. Лекция Амирова А.М. содержала в себе теоретические основы и практику осуществления защиты персональных данных в Республике Казахстан, что вызвало значительный интерес со стороны магистрантов Академии правосудия при Высшем Судебном Совете Республики Казахстан.

4. Дата внедрения диссертационного исследования докторанта: 29.11.2024 года.

Председатель: _____ Б. Сембекова
(подпись, Ф.И.О.)

Члены комиссии: _____ Ф. Жаксыбекова
(подпись, Ф.И.О.)

_____ Э. Мусенова
(подпись, Ф.И.О.)

ПРИЛОЖЕНИЕ И

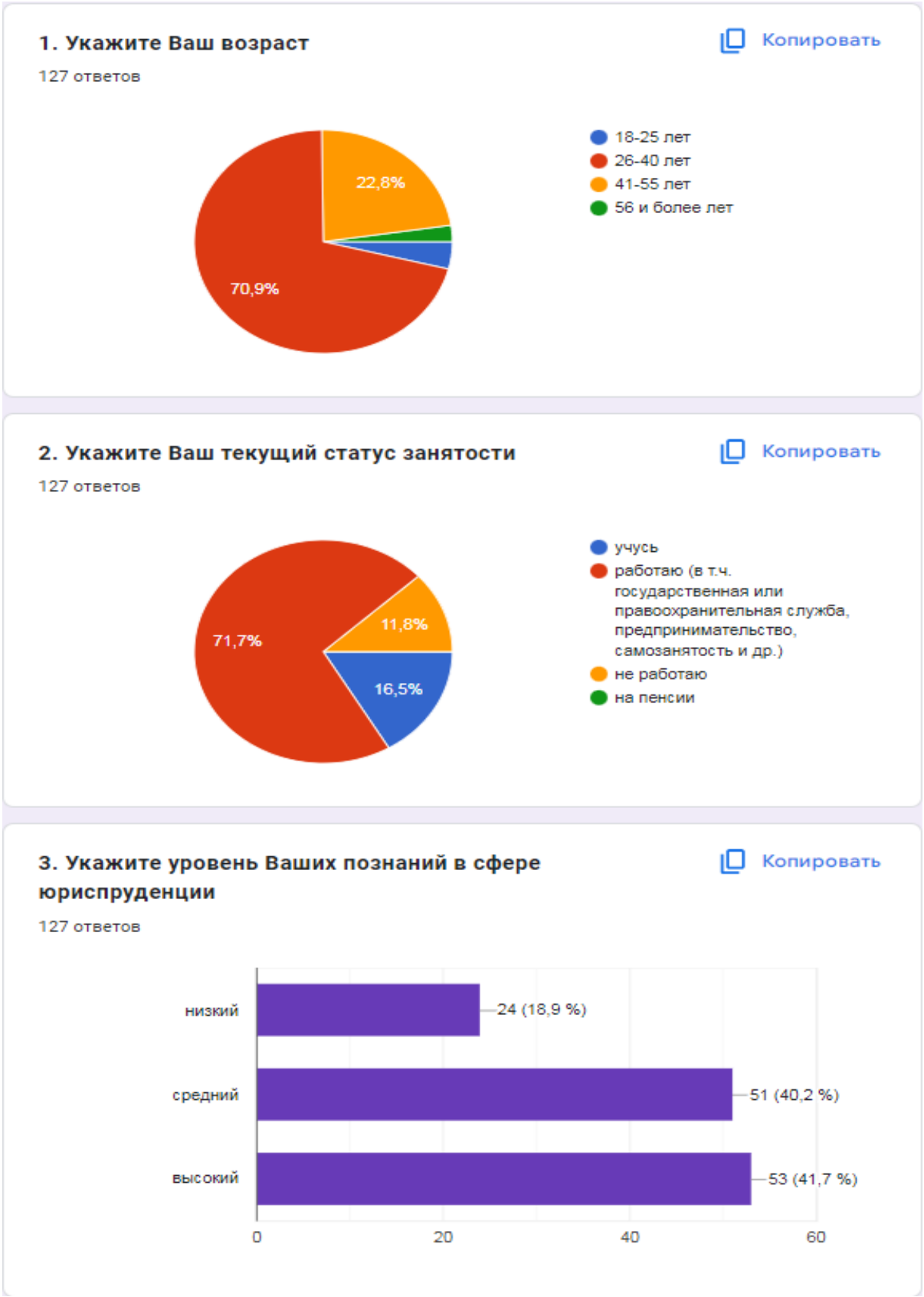
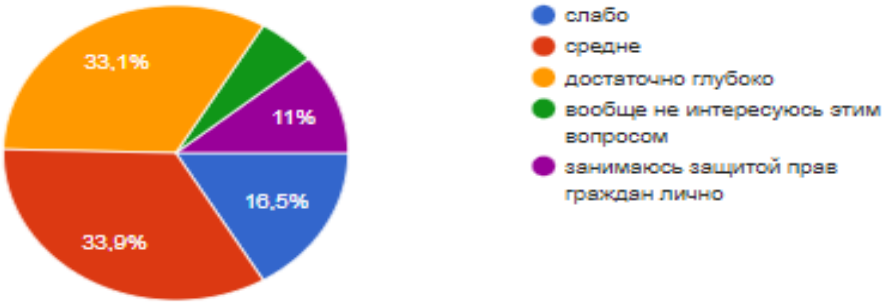


Рисунок И.1 – Сводные данные анкетирования 127 лиц по вопросам, связанным с защитой персональных данных, лист 1

4. Укажите насколько Вы ориентированы в вопросах обеспечения и защиты прав граждан

Копировать

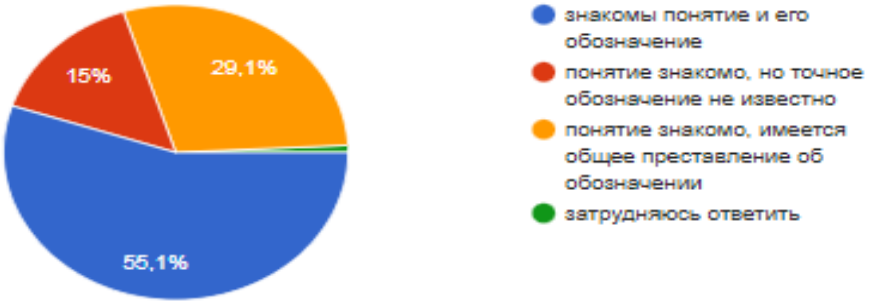
127 ответов



5. Знакомо ли Вам понятие «персональные данные» и его обозначение

Копировать

127 ответов



6. Известно ли Вам, какие именно виды сведений относится к персональным данным помимо фамилии, имени и отчества

Копировать

127 ответов

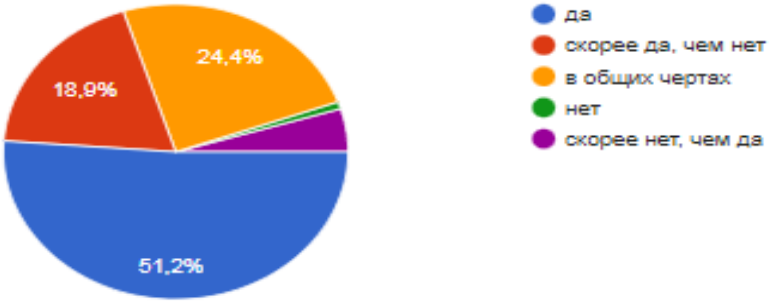
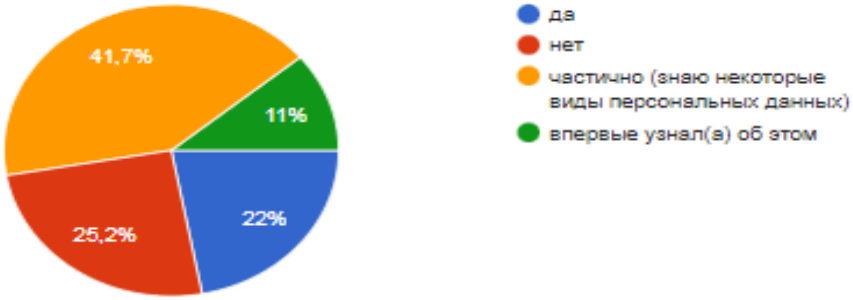


Рисунок И.1, лист 2

7. Известно ли Вам, что согласно нормам законодательства к персональным данным относятся более 100 различных видов сведений

Копировать

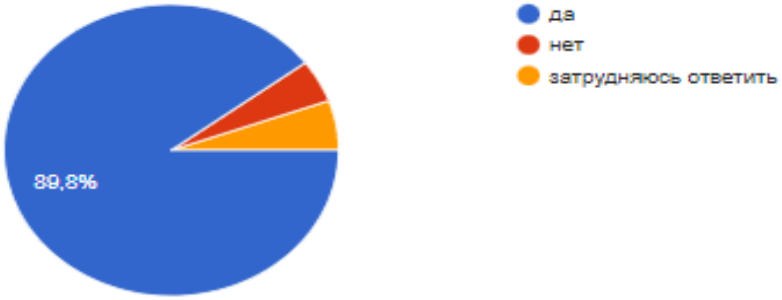
127 ответов



8. Знакомо ли Вам понятие «неприкосновенность частной жизни»

Копировать

127 ответов



9. Сталкивались ли Вы со случаями несогласованного распространения Ваших персональных данных, персональных данных Ваших близких, родственников или знакомых, в т.ч. через Интернет

Копировать

127 ответов

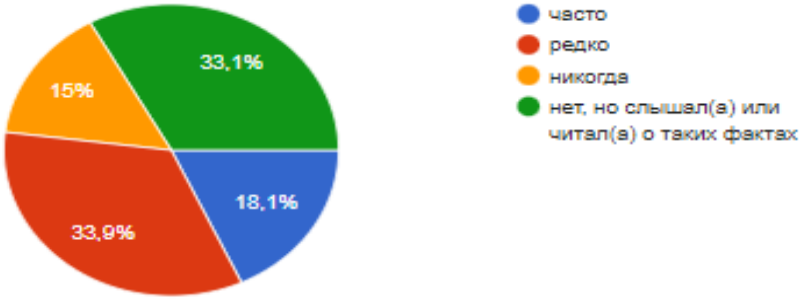


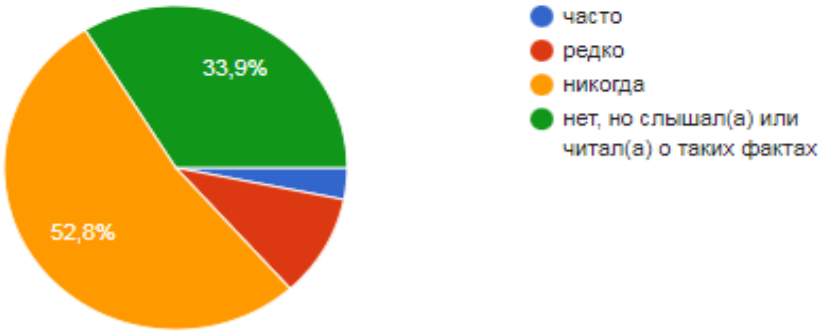
Рисунок И.1, лист 3

Рисунок И.1, лист 4

12. Сталкивались ли Вы со случаями несогласованного Вами распространения сведений о совершенных сделках по отчуждению имущества (недвижимость, транспорт, доли участия в юридических лицах, акции и др.), в т.ч. путем обращения после совершения сделки в Ваш адрес организаций, оказывающих страховые и другие услуги

Копировать

127 ответов



13. Сталкивались ли Вы со случаями несогласованного Вами распространения сведений о результатах медицинских заключений, диагнозов либо другой информации касательно Вашего здоровья

Копировать

127 ответов

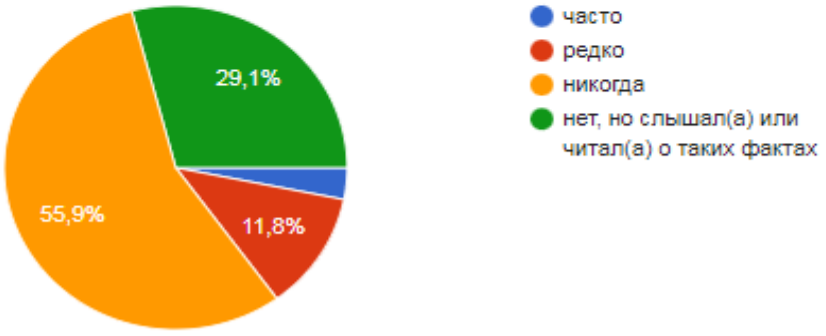
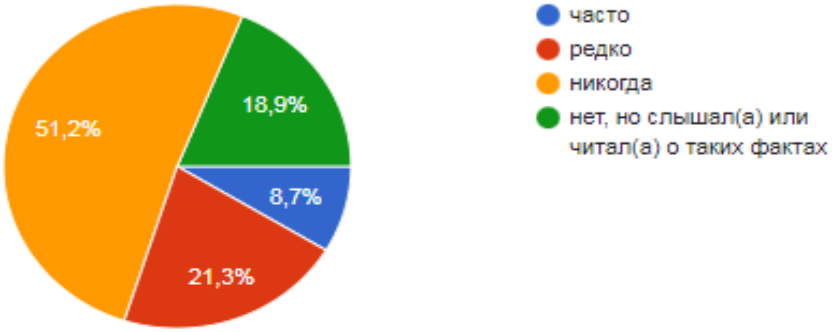


Рисунок И.1, лист 5

14. Сталкивались ли Вы со случаями несогласованного Вами распространения работодателями или коллегами сведений о Ваших доходах, заработной плате, должностном окладе, его размере, надбавках, премиях, налоговых и пенсионных отчислениях и т.д.

Копировать

127 ответов



15. Сталкивались ли Вы, Ваши родственники или знакомые со случаями, когда посторонние лица, используя чужие персональные данные, оформляли на этих лиц кредиты, микро займы либо использовали их в иных противозаконных целях

Копировать

127 ответов

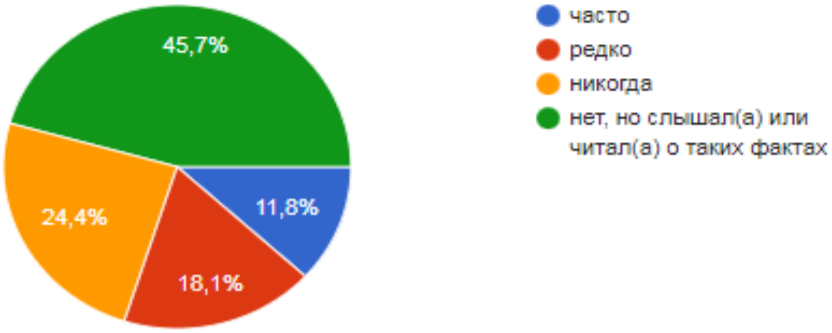
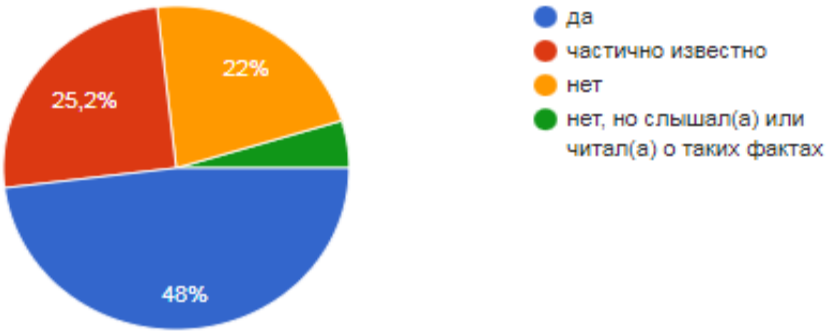


Рисунок И.1, лист 6

16. Известно ли Вам, что к персональным данным относятся и Ваши биометрические данные (вес, рост, ДНК, отпечатки пальцев, фото- и видео изображения, характеристики биологических жидкостей и продуктов жизнедеятельности человека)

Копировать

127 ответов



17. Поступали ли в Ваш адрес звонки от лиц, представлявшихся сотрудниками банков или государственных органов, из разговора с которыми Вам становилось понятно о наличии у них Ваших персональных данных

Копировать

127 ответов

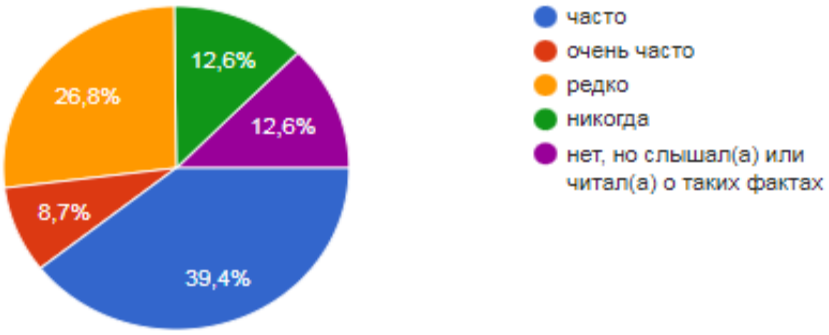
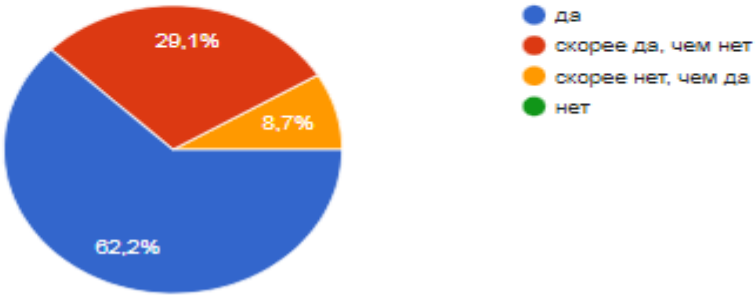


Рисунок И.1, лист 7

18. Опасаетесь ли Вы утечки Ваших персональных данных и их последующего несанкционированного распространения

Копировать

127 ответов



19. Принимаете ли Вы меры по защите своих персональных данных

Копировать

127 ответов

20. Известно ли Вам понятие «добровольное киберстрахование»

Копировать

127 ответов

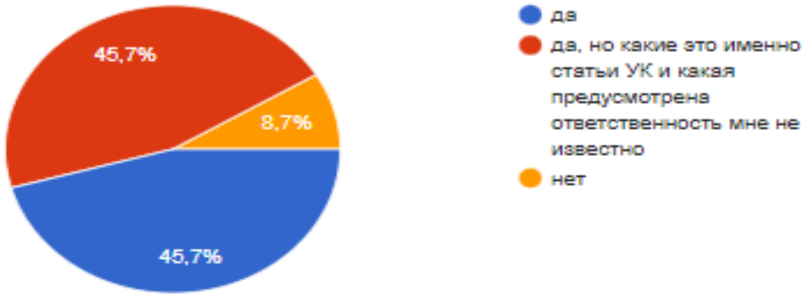
Рисунок И.1, лист 8

Рисунок И.1, лист 9

23. Известно ли Вам о наличии уголовной ответственности за нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите

Копировать

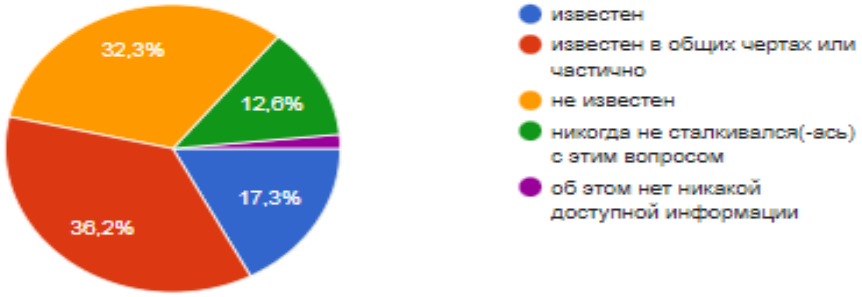
127 ответов



24. Известен ли Вам механизм защиты своих персональных данных и действий в случае нарушения законодательства о персональных данных и их защите

Копировать

127 ответов



25. Известен ли государственный орган, который является уполномоченным по защите персональных данных

Копировать

127 ответов

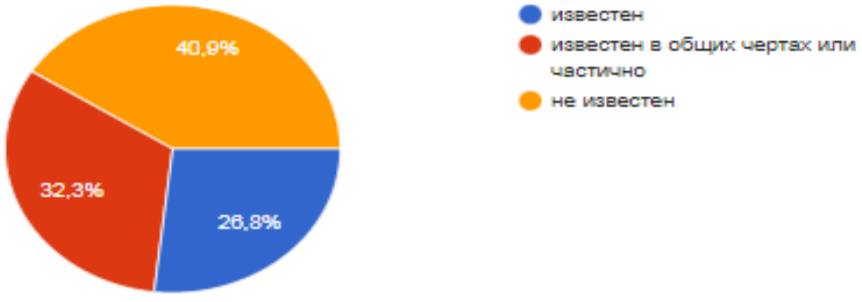
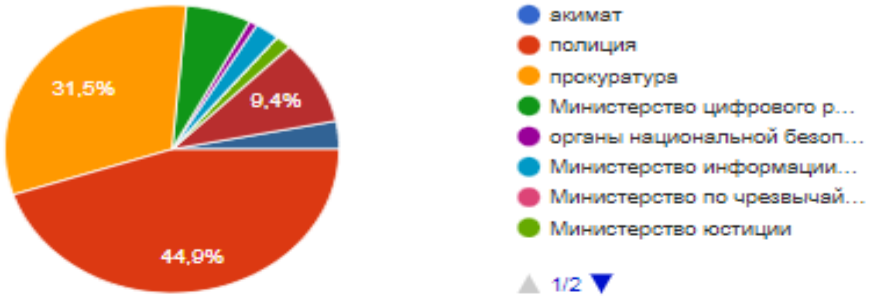


Рисунок И.1, лист 10

26. В случае необоснованного сбора или распространения Ваших персональных данных либо иных нарушений законодательства о персональных данных в какой орган Вы обратитесь

Копировать

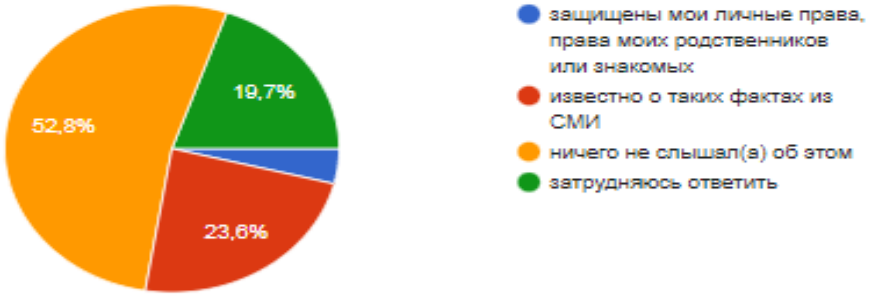
127 ответов



27. Известны ли Вам случаи, когда государство защитило персональные данные конкретного лица или большого числа граждан граждан

Копировать

127 ответов



28. Известны ли Вам случаи защиты персональных данных граждан, восстановление прав которых осуществили органы прокуратуры

Копировать

127 ответов

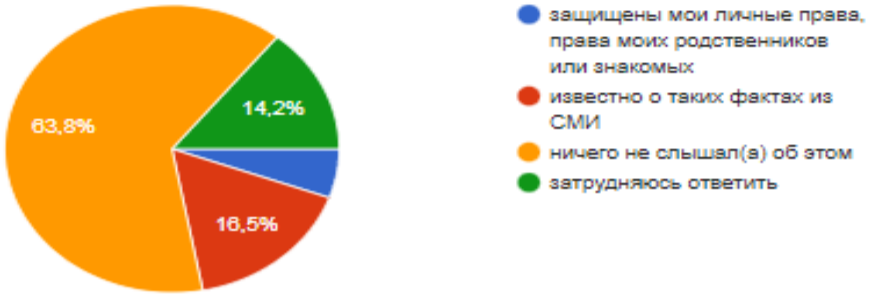
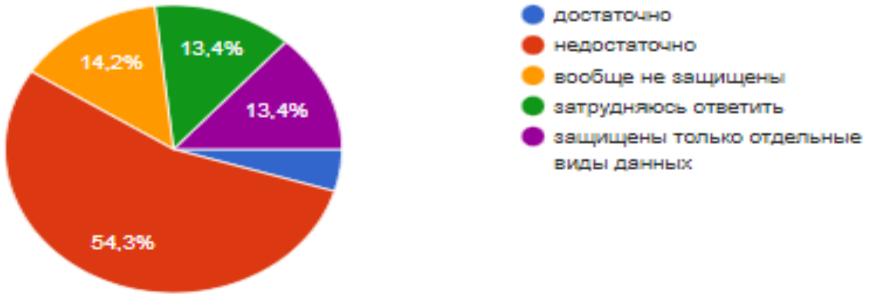


Рисунок И.1, лист 11

29. На Ваш взгляд, насколько эффективно защищены персональные данные в Республике Казахстан

Копировать

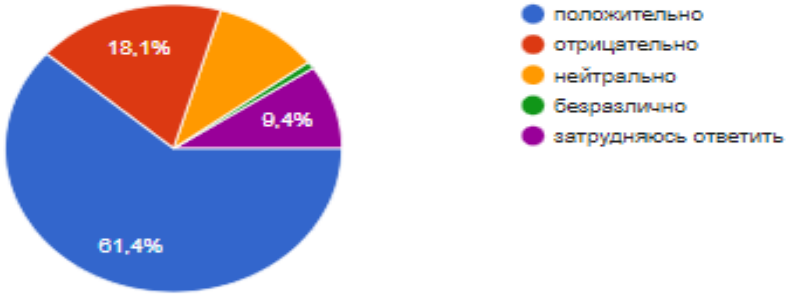
127 ответов



30. Как Вы относитесь к разделению персональных данных на общедоступные и конфиденциальные с установлением различного порядка их сбора и распространения

Копировать

127 ответов



31. Считаете ли Вы, что сами должны определять какие персональные данные подлежат публичному распространению, а какие нет

Копировать

127 ответов

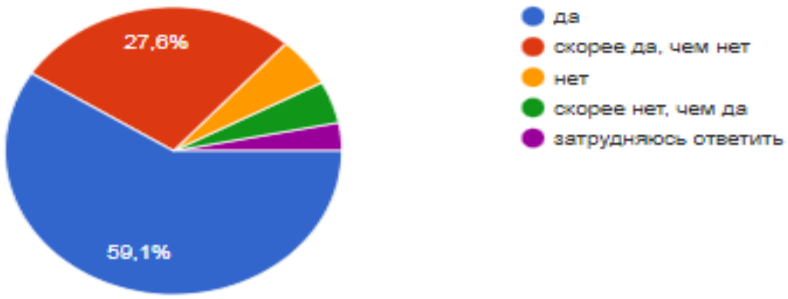
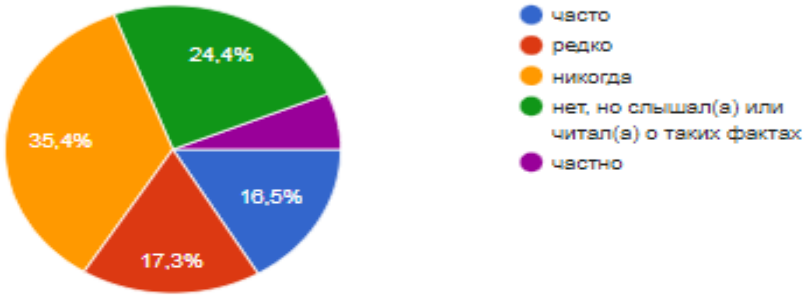


Рисунок И.1, лист 12

32. Сталкивались ли вы с фактами, когда кто-либо в работе использовал чужую электронно-цифровую подпись (в т.ч. в государственных органах, ЦОНе и т.д.)

Копировать

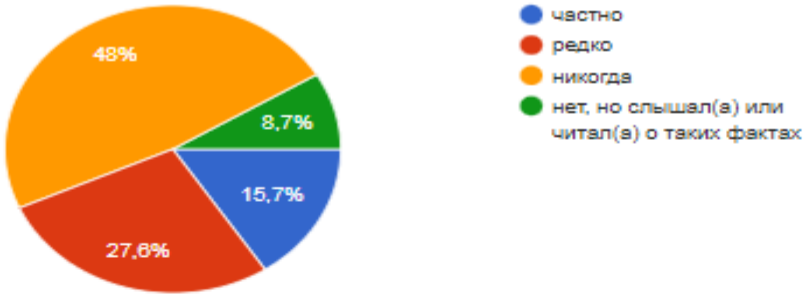
127 ответов



33. Допускаете ли Вы направление своей электронно-цифровой подписи по электронной почте другим лицам, установление ее на общедоступные компьютеры, установление легких паролей (123..., Qwerty и т.д.)

Копировать

127 ответов



34. На Ваш взгляд из каких источников наиболее часто утекают персональные данные граждан

Копировать

127 ответов

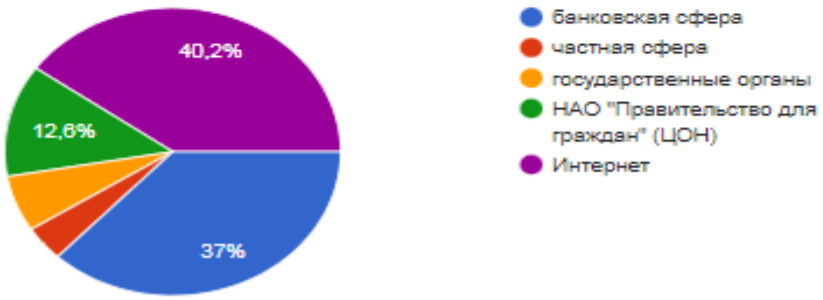
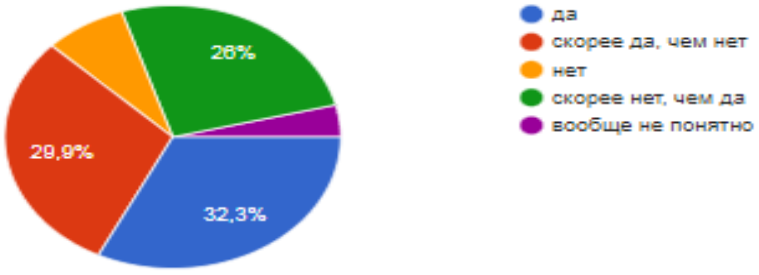


Рисунок И.1, лист 13

35. Ясно ли Вам в чем отличие законного и незаконного сбора, обобщения и распространения персональных данных, сумеете ли определить противоправные действия

Копировать

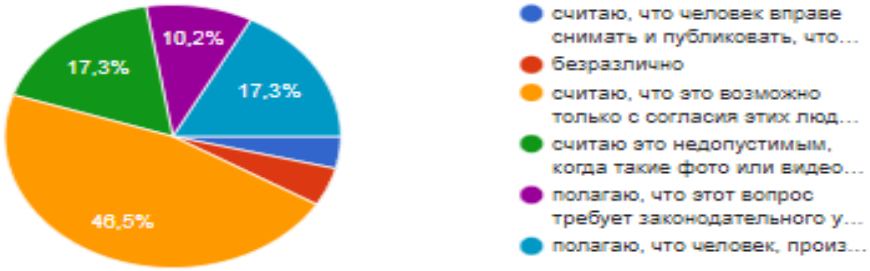
127 ответов



36. Как Вы относитесь к фактам несогласованной съемки и размещения в Интернете фото или видеоизображений посторонних людей (к примеру, продавцов, кассиров, соседей при конфликтах, людей, попавших в неловкую ситуацию, и т.д.)

Копировать

127 ответов



37. Знаете ли вы определение понятия "неприкосновенность частной жизни" и что понимается под "частной жизнью"

Копировать

127 ответов

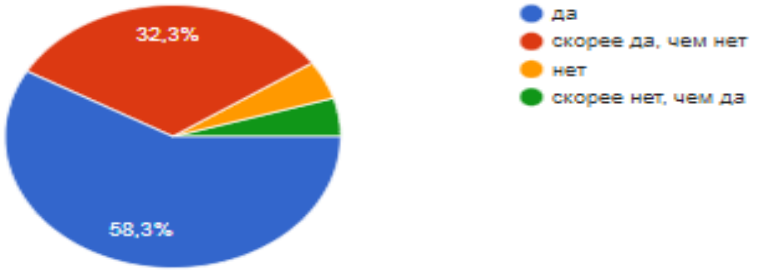
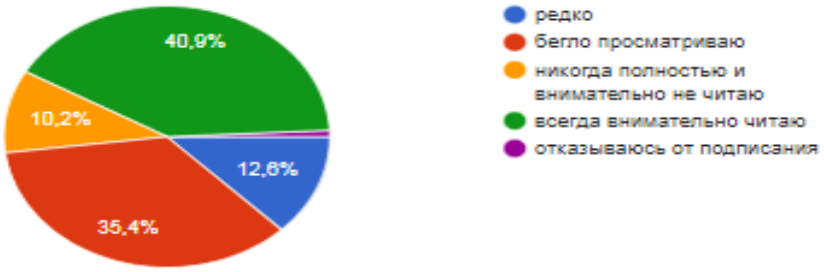


Рисунок И.1, лист 14

38. При заполнении в банках и других организациях согласий на сбор и обработку персональных данных обращаете ли Вы внимание на содержание данных документов

Копировать

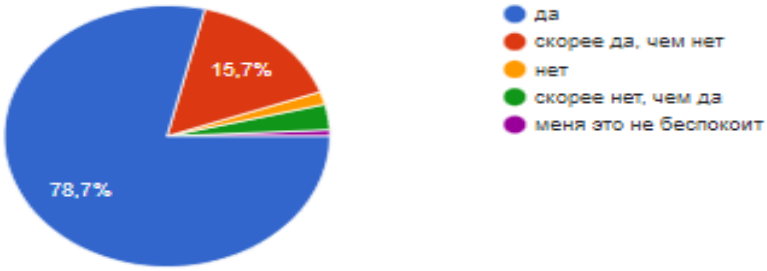
127 ответов



39. Считаете ли Вы, что в банках и других организациях в согласиях на сбор и обработку персональных данных должен быть указан точный перечень видов собираемых и обрабатываемых данных

Копировать

127 ответов



40. Считаете ли Вы, что в банках и других организациях в согласиях на сбор и обработку персональных данных должен быть указан точный срок и порядок хранения собираемых и обрабатываемых данных

Копировать

127 ответов

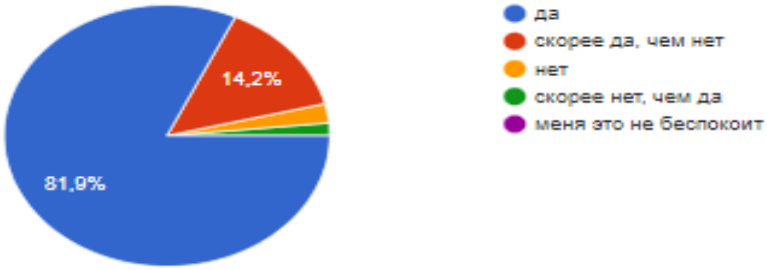


Рисунок И.1, лист 15