МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт права
(наименование института полностью)

Кафедра «Конституционное и административное право»
(наименование)

40.04.01 Юриспруденция
(код и наименование направления подготовки)

Правовое обеспечение государственного управления и местного самоуправления
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему «Защита персональных данных в законодательстве РФ: конституционно-правовой аспект»

Обучающийся Мария Анатольевна Храмцова _____
(И.О. Фамилия) (личная подпись)

Научный руководитель к.ю.н. К. П. Федякин
(ученая степень, звание, И.О. Фамилия)

Тольятти 2023

ОГЛАВЛЕНИЕ

Введение

Актуальность темы исследования. Данная тема «Защита персональных данных в законодательстве РФ: конституционно-правовой аспект» заинтересовала меня потому, что в настоящее время технические средства позволяют производить сбор и обработку существенных объемов социально значимых сведений, необходимых для эффективного функционирования государственных механизмов, протекания общественных процессов, а также реализации прав человека. Стремительное развитие информационных технологий дает возможность получать доступ и использовать различные банки данных практически любым субъектам информационных отношений. Постоянно ускоряющаяся информатизация общества и активное развитие открытых информационных систем значительно упрощают утечку и иные формы незаконного доступа к информации персонального характера, что делает задачу обеспечения ее правовой защиты особо актуальной и значимой как для российского, так и зарубежного законодательства и правовой доктрины.

Персональные данные — это очень щепетильный вопрос для каждого человека, ведь тема персональных данных, тем и важны, что это персональная личная конфиденциальная информация, касающаяся конкретного человека, это его личные данные и они должны быть неприкосновенны перед другими. Наши персональные данные должны быть защищены от несанкционированных действий других лиц.

На территории РФ ведется контроль за соблюдением прав по защите персональных данных человека. Существует множество нормативно-правовых актов, определяющих и указывающих на наши права в защите персональных данных. Развитие информационных систем усовершенствуется с каждым годом и тем самым создает большую угрозу. В таких системах возрастает спрос и появляется повышенный интерес и контроль к чужим частным персональным данным. В развитии современных технологий так же увеличивается возможность пресекать правонарушения в

сфере защиты персональных данных, но и при этом появляются такие же большие возможности для несанкционированных проникновений в базы данных. Мошенническими путями сливаются данные для дальнейшего распространения и в дальнейшем обогащения. Мошенники умышленно взламывают сервера, в связи, с чем и происходит утечка конфиденциальной информации.

Глобальные телекоммуникационные сети активно развивают свою деятельность в защите персональных данных, но все же есть не только информационная утечка базы данных, есть еще тот факт, что данные о частной жизни в повседневной жизни зависит в целом от самого человека. Человек не всегда отдает себе отчет и понимание, когда, где и кому можно распространять и предоставлять свои данные. Незнание законов не освобождает нас от ответственности, но все же на территории РФ много наивных людей преклонного возраста, которые сами распространяют свои данные, не ведая и не отдавая отчет своим действиям и их последствий. Чаще всего это конечно касается банковских денежных операций, где люди передают свои персональные коды для активации и разблокировок кредитных карт для дальнейшего процесса снятия наличных денежных средств.

Это всего лишь одна небольшая часть проблемы, есть множество других способов и вариантов для потери, утечки и распространения персональных данных. Мы имеем право на защиту наших данных и хотим чувствовать себя в безопасности, поэтому закон обязан нас защитить от несанкционированной передачи персональных данных.

С развитием общедоступности сети Интернет в стране появилось множество проблем с утечкой частной информации. Появилось много несанкционированного доступа к персональным данным, чем с большим удовольствием пользуются мошенники. Каждый день происходят незаконных операций по мошенническим действиям. Звонят «лжеоператоры» гражданам и мошенническими путями выманивают информацию о

банковских счетах, личных данных и т.д. Большинство сограждан, а чаще всего это люди в преклонном возрасте не знают свои прав и законов попадаются на уловки мошенников передавая им свои данные добровольно.

Конечно, если данные внесены компанией либо в социальные сети закрытого типа, то за эту информацию несут ответственность субъекты, которые и осуществляют непосредственно действия по обработке персональных данным с помощью информационно- телекоммуникационных сетей. На них законодательно возложена ответственность, которая регламентируется в Федеральном законе «О персональных данных» от 27.07.2006 года №152- ФЗ.

Степень научной разработанности темы исследования. По данной проблеме писали многие ученые, они основывались на анализах сравнений проводимых в законодательстве в сфере защиты персональных данных, они рассматривали эти проблемы непосредственно в конституционно – правовом аспекте – это Ветров Д.М., Волошкина Н.Н., Климович Е.В., Петрыкина Н.И., Поливанова Д.З., Савельев А.И., Серков П.П., Свирин Ю.А., Ситникова Е.Г., Терещенко Л.К., Филимонова Е.А., Цыдакова Э.А. и другие.

В данной работе мною были проанализированы несколько диссертационных работ по теме защиты персональных данных, из них я выбрала положительные и отрицательные аспекты. Эти работы были выбраны мной исключительно в сравнительном анализе мнений, в понимании теории, в понимании проблем касающихся защиты персональных данных и виды их решений.

Например:

Бураков В.В. считает, что существует большая проблема на законодательном уровне в отношении Роскомнадзора, который, по его мнению, практически имеет формальный вид и который не эффективно отвечает на требования современных правоотношений.

Карташева Т.Е. считает, что право человека на неприкосновенность частной жизни недостаточно основано для реализации и воплощения в жизни.

Кучеренко А.В. считает, что если оператора защиты персональных данных расширить в полномочиях, и он будет добросовестно выполнять свою работу, его действия и правильная трактовка законодательных норм будет обоснована законодательно, то это будет является залогом его успешной работы.

Успенский А.Р. предлагает ужесточить наказания и повысить сумму штрафа для юридических лиц и внести поправки в статью 13.11. КоАП РФ, и еще в нескольких нормативно – правовых нормах внести поправки и дополнения.

Объект исследования. Общественные правоотношения в институте персональных данных, защита неприкосновенности личной, частной жизни при хранении, передаче и обработке персональных данных в Российской Федерации.

Предметом исследования являются Теоретическая и практическая анализ научной литературы в сфере защиты персональных данных. Нормативно – правовые акты, законодательства, предусматривающие неприкосновенность частной жизни, материалы судопроизводственной практики, научные статьи, отражающие всю суть персональных данных их принципы и условия обработки, а также их защита.

Целью исследования является анализ и сравнение действующих нормативно – правовых актов в области хранения, передачи, обработке и защиты персональных данных. Выявление проблем в законодательной системе по урегулированию отношений между гражданином Российской Федерации (его персональные данные), Роскомнадзор (ответственность за обработку, хранение и утечку персональных данных), правоохранительные органы (ответственность и наказание за несоблюдение правовых норм по защите персональных данных).

Для достижения вышеуказанных целей необходимо выполнить следующие задачи:

- изучить нормативно – правовые акты по защите персональных данных;

- изложить структуру и определение персональных данных и определить степень их защиты;

- изучить правовое регулирование в области обработки и защиты персональных данных в электронных сетях;

-провести анализ научных исследований и статей в области защиты персональных данных;

- изучить проблемы и перспективы в области конституционно – правовых норм по защите персональных данных;

- проанализировать на практике судебных решений в сфере защиты персональных данных юридическую ответственность всех сторон;

- внести предложения по улучшению юридической ответственности в сфере обработке, передаче, хранении и защиты персональных данных.

Объем моей диссертационной работы на тему «Защита персональных данных в законодательстве РФ: конституционно-правовой аспект» - 71 страница. Структура данной работы состоит из: введения, основной части состоящей из 3х глав, (первая глава дает определение персональных данных, 2я глава понятие юридической ответственности за нарушение норм о персональных данных, 3я глава раскрывает проблемы в защите персональных данных, и мои рекомендации и возможные решения по совершенствованию защиты персональных данных), заключения и списка используемой литературы.

Глава 1. Понятие «Персональные данные»

1.1 Понятия персональных данных и гарантии их защиты

Персональные данные – это информация, которая несет за собой сведения, связанные напрямую с человеком. Это полная биография о человеке, его финансовое положение, образование, вид деятельности.

Обработка персональных данных — это сбор, хранение и любое использование, как при помощи информационных технологий, так и в частном порядке.

Вникая в рамки законодательного права по защите персональных данных, можно сразу понять, что в Конституции РФ нет фактического положения, которое бы четко определяло, само право на защиту персональных данных. Хотя и существуют положения, которые гарантируют нам в какой-то мере защищенность в защите персональных данных. Например, статья 23 Конституции России устанавливает право на неприкосновенность частной жизни, личную и семейную тайну. В месте с тем гарантируется право на тайну переписки, телефонных переговоров. Ограничение данного права допускается только на основании судебного решения. Положения статьи 24 Конституции РФ пересекаются с ФЗ «О персональных данных» как прямой запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия [9].

Определенно возникает много вопросов, что понятие «персональные данные» и термин «частная жизнь» значительно отличаются так, например, в Конституции РФ указывается термин «частная жизнь», но при этом он не несет за собой юридической основы. По мнению автора В.Н. Лопатина соотношение между «частной жизнью» и «персональными данными» он рассматривает как общее и частное [3] и Э. А. Цадыкова, например считает, что информация о частной жизни несет более широкое понятие, чем персональные данные [42]. А вот, например Е.В. Климович считает, что

персональные данные как раз не являются однородными, и что в их структуре, помимо идентифицирующей информации, нужно выделять данные о конкретном человеке, по ее мнению, к этому и относится вся информация о частной жизни [7]. Д.М. Ветров тоже кстати считает частную жизнь составляющей частью персональных данных [4]. А в частности, эти термины частная жизнь и персональные данные сильно отличаются между собой по содержанию. Содержание персональных данных — это вся информация прямо или косвенно относящаяся к человеку. А вот частная жизнь не несет за собой нормативно-правовых актов, оно скорее определяет образ жизни.

По моему мнению тайна частной жизни имеет достаточно объемное понимание. Ведь не всегда наши данные могут считаться тайной, так как некоторые наши персональные данные имеют общедоступный характер. Часть персональных данных можно получить непроизвольно, а случайным образом, не имея на это никакого злого умысла. Например, в социальных сетях часто можно увидеть на чьей-либо открытой страничке данные о ее владельце, такие как фамилия, имя, отчество, место работы, дата рождения, номер телефона и т.д. Такие данные не подлежат контролю так как не несут в себе противоправных действий.

Для отечественной конституционно-правовой доктрины характерно такое понимание частной жизни, в соответствии с которым к ней относится «не широкий спектр отношений, а узкая сфера интимных, бытовых и семейных отношений. Данный вывод, как представляется, находит подтверждение и в практике Конституционного Суда РФ, который рассматривает право на неприкосновенность частной жизни в качестве «фундаментального права», «в обеспечение» которого Конституция РФ закрепляет «иные личные права», в том числе право на тайну коммуникаций и право на неприкосновенность жилища» [9].

Одна из основных идей, которая имеет место во многих исследовательских работах, такова: права субъекта персональных данных

юридическая конструкция, производная от прав человека, сконцентрированная в источниках международного права. Скорее всего, необходимо различать два понятия – персональные данные и тайну частной жизни. Тайна частной жизни (личная и семейная тайна) – достаточно широкое понятие, не получившее точного нормативного закрепления и, в ряде случаев, охватывающее персональные данные. Тем не менее, отдельно взятые факты о лице, такие как фамилия, имя, отчество, место работы, адрес и т.п., а еще сведения о большинстве повседневных событий, связанных с этим лицом, не всегда могут считаться тайной. Поскольку по своему характеру эти сведения являются общедоступными и могут быть непроизвольно получены любым случайным лицом. В понятие «частная жизнь» включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она носит не противоправный характер. В противовес этому, персональные данные, как правило, являются своего рода идентификатором субъекта в человеческом обществе [10].

Федеральные законы, касающиеся частной жизни, защищают нас от любого постороннего вмешательства в личную жизнь, это касается чаще всего переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Это конкретно указано в ст. 23 Конституции РФ.

Если происходит вторжение в частную жизнь, то это либо нарушение неприкосновенности частной жизни, что карается законом, либо обработка персональных данных. Обработка персональных данных может происходить только тогда, когда гражданин добровольно передает свои персональные данные и подтверждает дальнейшие действия оператора обработки данных, это указано в ч. 1 ст. 9 Федерального закона «О персональных данных». К этому можно отнести заключение трудового договора, договора по кредитованию, либо в общедоступном варианте в социальных сетях.

Ст. 5 ФЗ «О персональных данных» предоставляет защиту прав и свобод человека и гражданина при обработке его персональных данных, в

том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. По такой формулировке следует, что институт частной жизни является составной частью института персональных данных, причем тоже в некоторой его части. Из вышеизложенного представляется, что необходимо отграничивать институт персональных данных от института неприкосновенности частной жизни [33].

В последнее время в связи с началом геополитической напряженностью в 2022 году, институт «персональных данных» пытается предпринять новые методы и решения в ряду нормативных актах по защите персональных данных. Так, например институт «персональных данных» рассматривает предложения от крупных компаний, которые предлагают альтернативу для системы наказаний, которая подразумевает уголовную ответственность за массовые утечки базы персональных данных. В этом предложение предлагается удерживать с предприятий нарушителей процент с годового оборота. За факт утечки – 1%, но если предприятие не предупредило в течение 3х дней Роскомнадзор, то выплачивать придется - 3%. В цифрах это примерно 500000-700000 рублей в государственную казну если при этом утечка данных будет свыше 1000 человек.

6 июня 2022 года Госдума приняла поправки к закону «О персональных данных», в них говорится об условиях, которые обязаны выполнять все компании при утечке информации. Они должны сообщить в Роскомнадзор в течение 24 часов, а сами результаты расследования этих утечек они должны предоставить в течение 72 часов. По мнению некоторых крупных компаний эти законы и поправки по защите персональных данных очень усложнят работу компаний. Так как всех операторов обяжут приобрести совсем не дешевое оборудование, для выполнения функций по установки безопасности, чтобы предотвратить утечку и слив информации третьим лицам.

Система безопасности по защите персональных данных должна анализировать содержимое, иметь антивирусные средства должен быть

полный мониторинг и контроль персональных данных, должна предотвращать от любых несанкционированных вторжений.

Практически все организации и предприятия РФ руководствуются законом об обеспечении персональных данных. Это для них как операторов персональных данных является прямой обязанностью. Если оператор персональных данных не соблюдает требования законам об обработке персональных данных, то на этот случай предусмотрена юридическая ответственность. Юридическая ответственность может быть применена как для предприятия в целом, даже может стать причиной для остановки основной деятельности предприятия при лишении лицензии, так и для руководителя отдельно. В совокупности в защите персональных данных мы видим сложный технологический процесс, основанный на недопущении утечки персональных данных с соблюдением конфиденциальности, безопасности их хранении в процессе деятельности организаций, предприятий и т.д.

Обязанности по организационным вопросам хранения, передачи и обработке персональных данных возложена на работодателя, он же и является оператором данного процесса. При обнаружении нарушений прав сотрудников в части передачи или утечки и вообще использование персональных данных сотрудников не по назначению, виновных привлекают к материальной, дисциплинарной, административной или уголовной ответственности.

1.2 Систематизация законодательства о персональных данных

В данное время институт «персональных данных» в России основаполагается рядом нормативных актов. При этом, как отмечают некоторые авторы, «практически во всех законах присутствуют нормы о правах граждан – субъектов персональных данных, хотя и с различной степенью разработанности. Во многих актах закреплены нормы об

ответственности за нарушения в работе с персональными данными». В первую очередь, неприкосновенность частной жизни гарантируется Конституцией Российской Федерации, а персональные данные являются важнейшей составляющей частной жизни. Основные позиции неприкосновенности частной жизни прописаны и в Конституции Российской Федерации 1993 г. (ст. 23, 24). Статья 23 Конституции гарантирует каждому «право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения». Статья 24 установила запрет на «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия».

Есть еще несколько нормативно правовых акта определяющих четкое положение и значения в обработке персональных данных. Первый это гл.14 Трудового Кодекса «Защита персональных данных». В этой главе указываются общие и четкие положения по защите, обработке, требованиям и ответственности за соблюдением всех указанных норм по защите персональных данных сотрудников. Второй правовой источник не менее важный — это ФЗ №149 «Об информации, информационных технологиях и защите информации» он указывает какие права нужно соблюдать при работе с информационными технологиями. Так же говорится об ответственности при случае утечки информации. Как правильно использовать систему информационных технологий, не нарушая права сотрудников [26].

Постановлением правительства РФ от 1 ноября 2012г. № 1119 (взамен утратившего силу постановления №781 от 17.11.2007) утверждены требования к защите персональных данных при их обработке в информационных системных персональных данных, что означает определенный порядок требований. искореняющий определенные угрозы безопасности.

В данном документе под угрозами безопасности персональных данных понимается обобщенность условий и факторов, создающих угрозу несанкционированного доступа, в том числе случайного во время их обработки информационной системой. Где в результате могут быть уничтожены, изменены, копированы, представлены иным лицам или же распространены на всеобщее обозрение. Все угрозы делятся на три типа и для обеспечения сохранности и защиты информации введены четыре уровня защищенности.

Для обеспечения защищенности персональных данных введен режим доступа в помещения, в которых расположена информационная система, препятствующий возможности неконтролируемого проникновения и доступа посторонним лицам. Создание структурного подразделения или назначение ответственного за обеспечение безопасности персональных данных в информационной системе.

Отметим, что государственные информационные системы определены в статье 13 Федерального закона от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации», как «федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов» [34].

Правовой институт регулирует общественные отношения, относящиеся к нескольким отраслям права, т.е. находящиеся на стыке отраслей, поэтому указанный правовой институт следует рассматривать как межотраслевой. В целом, несмотря на наличие ряда основополагающих документов, в существующем нормативно-правовом поле нет единых и исчерпывающих положений, связанных с организационно-правовой защитой персональных данных работников [10].

Есть противоречия между предоставлением оператором персональных данных государственным органам по их официальному запросу. Закон

основательно запрещает распространять и передавать персональные данные. В свою очередь предприятия боясь получения акта предписания от Роскомнадзора категорически отказывают государственным органам и в том числе Федеральной Антимонопольной Службе РФ в получении таких данных. Мною был найден в социальных сетях подобный описываемый случай, когда Федеральная Антимонопольная Служба сделала официальный запрос у оператора мобильной связи предоставить информацию о владельце телефонного номера, с которого исходила многочисленная информация, содержащая навязчивую рекламу. Организация сети мобильной связи отказала в выдаче информации, за что и была оштрафована за непредоставление данных. Суд постановил, что ФАС действовал на основании закона и оператор мобильной связи должен был предоставить информацию, запрашиваемую ФАС.

Такие разногласия крайне редки, но они все же встречаются. Первое такое разбирательство произошло в 2020 году, а второе в 2021году. Часто решаются судебные споры менее значимые, но имеющие значение в юридической практике, нарушения по неправомерному использованию и распространению персональных данных.

Основным законом в сфере защиты персональных данных является Федеральный закон «О персональных данных» от 27.07.2006г. №152-ФЗ.[33]

Он определяет:

- Основные понятия персональных данных – Гл.1 ст. 1,2,3,4;
- Принципы и условия обработки персональных данных – Гл.2 ст. 5,6,7,8,9,10,10.1;
- Какие имеет права субъект персональных данных – Гл. 3 ст. 14,15,16,17;
- Указывает на обязанности операторов при сборе, обработке и хранении персональных данных – Гл. 4 ст. 18,19,20,21,22,22.1;
- Устанавливает контроль за обработкой (обработка – это действия с персональными данными, а именно сбор, изменение, накопления, хранение,

распространение, обезличивание, уничтожение) персональных данных и ответственность за нарушения этих требований – Гл. 5 ст. 23,23.1,24;

В соответствии с п. 1 ст. 23 Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных» и п. 1 Положения о Федеральной службе по надзору в сфере связи и массовых коммуникаций, утвержденного постановлением Правительства Российской Федерации от 16.03.2009 года № 228, «уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям настоящего Федерального закона, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере связи и массовых коммуникаций (Роскомнадзор)»[33].

Вообще есть целый ряд нормативно правовых актов регулирующих сферу общественных отношений в защите персональных данных. Главный НПА как я уже указала выше это Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных». Этот закон я бы сказала основа основ принимающую все начальные факты из которых можно понять, что такое непосредственно «персональные данные». Но есть множества других дополняющих нашу безопасность в других отраслях обработки и передачи данных. Например, ст. 4 закона РФ №2124-1 «О средствах массовой информации». В этой статье говорится о недопущении использования разглашения сведений относящихся к гос. тайне или призывы к террористической деятельности. Этот закон по моему мнению имеет ряд не совершенствований, так как в наше время очень часто происходят утечки информации как раз по вине СМИ. Взять даже пример связанный с данными событиями на Украине по спецоперации, как мы видим через СМИ, идет много подложной(фейковой) информации про наших солдат и сограждан в целом. Отследить эти утечки почему-то для наших властей это проблема, но я считаю это можно решить при помощи наших лучших специалистов

информационных технологий, которые смогли бы создать программу для блокировки утечек ложной и несанкционированной информации.

Еще одним из основных законов это наше право, право на неприкосновенность частной жизни и всех вытекающих из нее – ст. 23 Конституции РФ:

1. «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени» [9].

2. «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения» [9].

Следующие нормативные правовые акты, относящихся к сфере деятельности человека, которые определяют состав, содержание и обработку персональных данных. К ним относят: ФЗ-27 «Об индивидуальном учете в системе обязательного пенсионного страхования», № 149-ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ-197 «Трудовой кодекс РФ», ФЗ-79 «О государственной гражданской службе РФ», ФЗ-129 «О государственной регистрации юридических лиц и индивидуальных предпринимателей» и т.п.

1.3 **Положительные аспекты**

Положительные аспекты в том, что институт «персональных данных» связи с началом геополитической напряженностью начал в 2022 году рассматривать предложения от крупных компаний, которые предлагают альтернативу для системы наказаний, которая подразумевает уголовную ответственность за массовые утечки базы персональных данных. Внесено несколько предложений по усилению защиты персональных данных.

Так же в связи с последними политическими событиями мы четко видим наши минусы и пробелы по несанкционированной утечки и ложной информации СМИ. Радует то, что мы наконец начали разрабатывать

различные программы по улучшению и внедрению разработчиков в информационных технологиях. Потому, что на них лежит большая ответственность и надежда на их умы. С их помощью можно добиться колоссальных результатов по отслеживанию утечки и нарушений неправомерного использования персональных данных как граждан, так и компаний в целом.

Так не смотря на все перечисленные положительные аспекты в защите персональных данных, мы видим пробелы, касающиеся проблем по утечке информации, ущерб от которых подчас оценивается весьма впечатляющими суммами. Отсутствие систематизации законодательства в сфере персональных данных создает состояние незащищенности от несанкционированного доступа к информации персональных данных. Обильно возрастают объем информации личного доступа персональных данных, нуждаются в особой ответственности при решении вопросов и регулирование соответствующих правоотношений. Есть законы, противоречащие друг другу. Принципом в этом должно стать обеспечение информационной безопасности человека, защита личных прав в сфере информационного общества, и урегулирования законодательных спорных вопросов.

Радует, что институт персональных данных, анализирует обстановку и предпринимают усилия при усовершенствовании безопасности защиты данных, принимают законопроекты для улучшения работы операторов. Вводят административную и уголовную ответственность за несоблюдение требований и утечку информации. Осознают важность и усиливают действия уполномоченных органов.

Еще один большой плюс в том, что часто наша информация о частной жизни и наши персональные данные передаются в тех случаях, когда от нас этого требуют сторонние организации или в электронном виде запрашивают подтверждение, даже в тех случаях, когда это абсолютно не нужно. И вот для таких не нужных действий с 1 сентября 2022 года вступили соответствующие

поправки Федеральным Законом от 01.05.2022 №135-ФЗ. Если раньше у нас требовали под любым предлогом наши номера телефонов или электронную почту, то сейчас не обязательно это сообщать, только в тех случаях, где это предусмотрено законодательством.

С 1 сентября 2022 года вступило новое правило к требованиям по обработке персональных данных с обязательными требованиями статьи 18.1 Закона № 152-ФЗ. Если раньше было «могли», то теперь четко «обязаны» назначать структурное подразделение и определить ответственное лицо за обработку персональных данных; издавать и опубликовывать в обязательном порядке политику по персональным данным; осуществлять внутренний контроль (аудит) персональных данных (способ контроля и подтверждение его проведения нужно прописать в отдельном Локально нормативном акте. Его предмет: соблюдение требований законодательства, политики, локально нормативном акте организации по защите персональных данных).

Летом этого года были приняты несколько нормативно - правовых актов, расширяющих полномочия и внесением изменений в сфере обработки биометрических персональных данных. Например таких как: Федеральный закон от 14.07.2022 № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», «отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности»»[41] (далее - Федеральный закон № 226-ФЗ); Федеральный закон от 14.07.2022 № 325-ФЗ «О внесении изменений в статьи 14 и 14-1 Федерального закона «Об информации, информационных технологиях и о защите информации» и статью 5 Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации» (далее - Федеральный закон № 325-ФЗ)[40]; Постановления правительства Российской Федерации от 15.06.2022 № 1066 «О размещении физическими лицами своих биометрических персональных данных в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и

хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица»[13] (далее - Постановление № 1066); Постановления правительства Российской Федерации от 16.06.2022 № 1089 «Об утверждении Положения о единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица»[14] (далее - Постановление № 1089); Постановления правительства Российской Федерации от 15.06.2022 № 1067 «О случаях и сроках использования биометрических персональных данных, размещенных физическими лицами в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица»[15] (далее - Постановление № 1067);

В будущем ожидается изменения к требованиям закона о персональных данных, которые вступят в силу 1 марта 2023 года. В большей степени это коснется вопросов и действий по уведомлению Роскомнадзора по работе с персональными данными, их обработке, передачи и утечек информации.

В законе 266-ФЗ предусматриваются изменения по срокам подачи уведомлений операторами, таких как:

- исключения данных из реестра операторов, если оператор отправит уведомлении о прекращении обработки ПД: само исключение – в течение 30 дней, подача заявления о прекращении – в течение 10 рабочих дней (пп. «б» п. 14 ст. 1 Закона 266-ФЗ)

- уведомления оператором в случае изменения сведений (не позднее 15 числа, следующего за месяцем, в котором возникли изменения (пп. «д» п. 14 ст. 1 Закона 266-ФЗ).

Будут применены три формы уведомления операторами:

- до начала обработки персональных данных оператором
- о прекращении обработки персональных данных оператором (такое уведомление необходимо будет подать в течение 10 рабочих дней с даты прекращения обработки персональных данных), такой срок конечно можно будет продлить еще на пять дней, но будет нужна четкая мотивация и письменное уведомление;
- об изменении данных по обработке персональных данных (такое уведомление необходимо будет подать до 15 числа следующего месяца).

Еще до 1 марта 2023 года будут установлены требования к подтверждению уничтожения персональных данных (Проект Приказа Роскомнадзора (подготовлен 19.08.2022), пп. «г» п. 13 ст. 1 Закона 266-ФЗ).

Таким образом, изменения в закон о персональных данных касаются всего порядка работы с ними: от особенностей согласия и уведомления Роскомнадзора до правил трансграничной передачи, прекращения обработки и исполнения новых сроков. За нарушение этих требований грозят не только крупные административные штрафы, но и уголовная ответственность (ст. 13.11, 13.12 и 19.7 КоАП РФ, ст. 137 и 272 УК РФ).

Такие изменения не могу не радовать и несут в себе положительное влияние на работу операторов по обработке персональных данных. Во всех нормативно правовых актах должно четко прослеживаться полное понимание и ответственность за неправомерные действия. Это будет улучшением в дисциплинарной ответственности, что скажется в лучшую сторону для организация занимающихся обработкой персональных данных.

Вывод

Анализируя выше сказанное по поводу защиты и охраны персональных данных можно утверждать, что существует множество мнений и многих авторов есть своя точка зрения по определению и классификации терминологии, информации и нормативно правовых актов. Есть два доступа к информации открытый и закрытый. К закрытому доступу относится Указ Президента «Об утверждении перечня сведений конфиденциального характера», что подразумевает под собой конфиденциальность персональных данных.

Есть определения понятия «персональных данных» и что к ним относится в ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ (ред. от 14.07.2022) "О персональных данных", в ней четко указано кто и как должны хранить и обрабатывать персональные данные. Что такое персональные данные – это имя, фамилия, дата и место рождения, паспортные данные, прописка, должность, профессия и многое другое, что относится непосредственно к физическому лицу. Кто несет ответственность, кто является оператором обработки персональных данных, что относится к уничтожению, хранению, предоставлению, блокировке и автоматизации данных.

На основании всех нормативно правовых актов понятно, что персональные данные — это конфиденциальная информация и за несоблюдение законных действий по отношению передачи, обработке и других действий, наступает юридическая ответственность.

Многие утверждают, что безопасность конфиденциальной информации носит безопасный характер на высоком уровне, с чем я крайне несогласна. Я считаю персональные данные находятся в состоянии правовой незащищенности от несанкционированного доступа. И мною были приведены примеры, в каких областях это не доработано. Если брать рабочую специфику, при устройстве на работу, то тут практически все понятно и с безопасностью и обработкой и хранением. В трудовом законодательстве гл. 14 ФЗ-197 «Трудовой кодекс РФ», пописаны четкие

условия обработки, хранения и юридическая ответственность за несоблюдение. В данной сфере легче найти нарушения и пресечь противодействия, нежели в информационной, либо в частном порядке, когда такими деяниями помышляют мошенники и наживаются на безграмотности и социально не защищенных физических лиц.

Общие нормативно правовые акты обеспечивают безопасность в защите ограниченного доступа к информации, но все равно далеки от совершенства. Вычислить утечку информации и довести до судебного определения вины с юридической ответственностью и наложением штрафа за содеянные правонарушения, крайне редкое явление.

Необходимо создать такой механизм защиты в правовых отношениях по защите персональных данных, чтобы можно было с первой подачи собственных данных по цепочке отследить несанкционированную утечку и предотвратить последствия. К этому процессу необходимо подключить информационных специалистов по разработке специальных программ блокировок по утечке несанкционированной информации. Так же усилить контроль нормативно правовыми актами и законами ужесточающее наказание и увеличение штрафов за ответственность утечки и незаконного использования персональных данных.

Замечу, что органы государственной власти не бездействуют и 6 июня 2022 года Госдума приняла поправки к закону «О персональных данных», в них говорится об условиях, которые обязаны выполнять все компании при утечке информации. К этому подключен Роскомнадзор которому операторы должны сообщить об утечке в течение 24 часов, а результаты расследования утечек они должны предоставить в течение 72 часов. Увеличились и штрафы, хотя я считаю, что сумма штрафов занижена. За факт утечки – 1%, но если предприятие не предупредило в течение 3х дней Роскомнадзор, то выплачивать придется -3%. В цифрах это примерно 500000-700000 рублей в государственную казну если при этом утечка данных будет свыше 1000 человек.

Положительные решения по обработке персональных данных касающихся изменений в законе 266-ФЗ, которые вступят в силу 1 мата 2023года.

Глава 2. Судебная и административная практика по защите персональных данных.

2.1 Юридическая ответственность за нарушения норм о персональных данных.

Проблема защиты персональных данных в наше время набирает катастрофические на мой взгляд обороты. Эта проблема очень остро ощущается на всей территории Российской Федерации. Огромная доля нашей информации касаемой частной, личной жизни – наши паспортные данные, профессия, кредитные истории, банковские счета, данные нашего здоровья (диагнозы), вся эта информация хранится в электронной базе социальных сетей, в электронных базах государственных структур, таких как налоговая, банки, больницы, паспортный стол, полиция и т.д. Эти данные должны быть строго защищены от любых посторонних вмешательств. Ведь наша защита персональных данных предусмотрена законом.

Законодательство определенно не совершенно в проблемах по защите персональных данных, они безусловно есть. Много пробелов и недостатков в сфере защиты персональных данных, но также есть законы, защищающие нас и наши данные в контроле уполномоченных органов. В Российской Федерации не мало регулирующих нормативно – правовых актов в работе с персональными данными. Основной закон по моему мнению это Федеральный Закон от 27.07.2006 года №152-ФЗ «О персональных данных». Он дает четкие понятия кто является оператором персональных данных, и кто несет ответственность по выполнению всех функций обработки, хранения уничтожения и требований по защите персональных данных. Это основа основ для других нормативно – правовых актов, таких как Гражданский кодекс Российской Федерации, Уголовный кодекс РФ, Трудовой кодекс РФ, Кодекс Российской Федерации об административных правонарушениях. Это также и муниципальные органы, юридическое и физическое лицо, государственный орган. Эти нормативно – правовые акты и законы предупреждают нас, что за несоблюдение законов по защите

персональных данных предусматривается административная и уголовная ответственность:

Например:

Административная ответственность предусмотрена при «обработке персональных данных в случаях, не предусмотренных законом» в ч. 1. Ст.13.11 КоАП РФ, для физических лиц штраф от 2000 до 6000 рублей, а при повторном нарушении штраф удваивается; для должностных (государственных служащих) предусматривается ответственность за нарушение штрафом от 10000 до 20000 рублей, при повторном нарушении штраф также удваивается; для юридических лиц сумма штрафа посущественнее от 60000 до 100000 рублей, а при повторном нарушении практически утраивается от 100000 до 300000 рублей. И это только по ч.1. ст. 13.11 КоАП РФ.

Во 2 части ст. 13.11 КоАП РФ за «обработку персональных данных без письменного согласия» штрафы куда больше – для физических лиц штраф от 6000 до 10000 рублей, при повторном нарушении от 10000 до 20000 рублей; для должностных лиц (государственных служащих) штраф от 20000 до 40000 рублей, за повторное нарушение от 40000 до 100000 рублей; для юридических лиц штраф предусмотрен от 30000 до 150000 рублей, а при повторном нарушении от 300000 до 500000 рублей.

В части 3 ст.13.11 КоАП РФ «Невыполнение обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных» штраф для физических лиц предусмотрен в сумме от 1500 до 3000 рублей; для должностных лиц штраф от 6000 до 12000 рублей; для юридических лиц штраф от 30000 до 60000 рублей, за повторные нарушения повышение штрафов к сожалению не предусмотрено.

В части 4 ст. 13.11 КоАП РФ «Невыполнение обязанности по предоставлению субъекту персональных данных информации, касающейся

обработки его персональных данных» влечет предупреждение и наложение штрафа для физических лиц в сумме от 2000 до 4000 рублей; для должностных лиц сумма штрафа составляет от 8000 до 12000 рублей; для юридических лиц эта сумма составляет от 40000 до 80000 рублей.

В части 5 ст. 13.11 КоАП РФ «Невыполнение оператором в сроки, установленные законодательством, требования об уточнении персональных данных, их блокировании или уничтожении» влечет предупреждение и наложение штрафа в виде сумм для физических лиц от 2000 до 4000 рублей, при повторном нарушении штраф в разы увеличивается от 20000 до 30000 рублей; для должностных лиц штраф предусмотрен в сумме от 8000 до 20000 рублей, а при повторном нарушении от 30000 до 50000 рублей; для юридических лиц штраф предусмотрен в виде сумм от 50000 до 90000 рублей, при повторном нарушении от 300000 до 500000 рублей.

В части 6 ст. 13.11 КоАП РФ «Невыполнение при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ» несет административного штрафа для физических лиц в сумме от 1500 до 4000 рублей; для должностных лиц штраф предусмотрен от 8000 до 20000 рублей; для юридических лиц наложение административного штрафа в сумме от 50000 до 100000 рублей.

В части 7 ст. 13.11 КоАП РФ «Невыполнение оператором, являющимся государственным или муниципальным органом, обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов по обезличиванию персональных данных» влечет так же предупреждение или наложение административного штрафа в сумме от 6000 до 12000 рублей.

В части 8 ст. 13.11 КоАП РФ «Невыполнение оператором при сборе персональных данных, в том числе посредством информационно-

телекоммуникационной сети «Интернет», предусмотренной законодательством РФ в области персональных данных обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан РФ с использованием баз данных, находящихся на территории РФ» предусматривается наказание в виде наложения штрафа в сумме для физических лиц от 30000 до 50000 рублей, при повторном нарушение наложение штрафа увеличивается от 50000 до 100000 рублей; для должностных лиц штраф предусмотрен наложением в сумме от 100000 до 200000 рублей, за повторное нарушение от 500000 до 800000 рублей; для юридических лиц наложение штрафа в сумме от 1000000 до 6000000 рублей, при повторном нарушении увеличение штрафа не предусмотрено.

Исходя из ст. 13.11 Кодекса Российской Федерации об административных правонарушениях административная ответственность зависит от тяжести правонарушения. Если нет письменного согласия субъекта, то это усугубляет положение юридических лиц и предусматривает за нарушение максимальный размер штрафа.

Если оператор либо иное лицо нарушает свои обязанности по обработке, хранению и защите персональных данных, и не законно распространяет либо собирает эти данные, то за такое правонарушение предусмотрена уголовная ответственность.

Например:

УК РФ 137 «Нарушение неприкосновенности частной жизни» влечет наказание за незаконное собирание и распространение сведений о частной жизни лица, составляющих его личную и семейную тайну. Уголовная ответственность грозит если эти действия совершены намеренно, из корыстных побуждений. Наказание ужесточается, если виновный использовал свое служебное положение.

- Ч.1 – Сбор или распространение данных, которые составляют личную или семейную тайну человека, без его согласия. За обнародование таких данных

возможны наказания – штраф, обязательные-исправительные-принудительные работы.

- Ч.2 – с использованием служебного положения – наказание в виде лишения прав на профессиональную деятельность, арест и лишение свободы.
- Ч.3 – Незаконное обнародование информации о потерпевшем, которому еще не исполнилось 16 лет влечет штраф, лишения права на профессиональную деятельность, принудительные работы, арест и лишение свободы [30].

В выше упомянутой статье полагается наказание в виде, часть 1,2 ст. 137 Уголовного кодекса РФ «Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации» для физических лиц наказание предусмотрено от наложения штрафа до 200 000 рублей или в размере заработной платы или иного дохода за период до 18 месяцев, либо обязательные работы до 360 часов, либо исправительные работы до 1 года, либо принудительные работы до 2 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового, либо арест на срок до 4 месяцев, либо лишение свободы до 2 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет.

Для должностных лиц наказание по этой статье предусмотрено в виде штрафа от 100 000 до 300 000 рублей или в размере заработной платы или иного дохода за период от 1 года до 2 лет, либо лишение права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет, либо принудительные работы до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового, либо арест до 6 месяцев,

либо лишение свободы до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет.

Часть 3 ст. 137 Уголовного кодекса РФ «Незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, Либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия» для физических лиц наказание предусмотрено в виде штрафа от 150 000 до 350 000 рублей или в размере заработной платы или иного дохода за период от 18 месяцев до 3 лет, либо лишение права занимать определенные должности или заниматься определенной деятельностью на срок от 3 до 5 лет, либо принудительные работы до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 6 лет или без такового, либо арест до 6 месяцев, либо лишение свободы до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 6 лет.

Статья 138 Уголовного кодекса РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» для физических лиц предусмотрено наказание в виде штрафа до 80 000 рублей или в размере заработной платы или иного дохода за период до 6 месяцев, либо обязательные работы до 360 часов, либо исправительные работы до 1 года. Для должностных лиц по этой же статье предусмотрено наказание в виде штрафа от 100 000 до 300 000 рублей или в размере заработной платы или иного дохода за период от 1 года до 2 лет, либо лишение права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет, либо обязательные работы до 480 часов, либо

принудительные работы до 4 лет, либо арест до 4 месяцев, либо лишение свободы на срок до 4 лет.

Ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» влечет наложение штрафа в размере до 200000 рублей, либо исправительные работы на срок до 1 года, либо ограничения свободы до 2х лет, либо принудительные работы до 2х лет. Если деяния, предусмотренные частью 1,2,3 настоящей статьи, повлекли тяжкие последствия - наказываются лишением свободы на срок до 7 лет [15]. Если быть точнее, то наказание предусмотрены по каждой части разные: в части 1ст. 272 УК РФ «Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации» предусмотрен штраф до 200 000 рублей или в размере заработной платы или иного дохода за период до 18 месяцев, либо исправительные работы до 1 года, либо ограничение свободы до 2 лет, либо принудительные работы до 2 лет, либо лишение свободы до 2 лет. В части 2 ст. 272 УК РФ «Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние причинило крупный ущерб (сумма которого превышает 1 000 000 рублей) или было совершено из корыстной заинтересованности» предусмотрен штраф от 100 000 до 300 000 рублей или в размере заработной платы или иного дохода за период от 1 года до 2 лет, либо исправительные работы от 1 года до 2 лет, либо ограничение свободы до 4 лет, либо принудительные работы на срок до 4 лет, либо лишение свободы до 4 лет. В части 3 ст. 272 УК РФ «Деяния, предусмотренные ч.1 или ч.2 ст. 272 УК РФ, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения» предусмотрено наказание для физических лиц в виде штрафа до 500 000 рублей или в размере заработной платы или иного дохода за период до 3 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет, либо ограничение свободы на срок до 4 лет,

либо принудительные работы на срок до 5 лет, либо лишение свободы до 5 лет; для должностных лиц штраф до 500 000 рублей или в размере заработной платы или иного дохода за период до 3 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет, либо ограничение свободы на срок до 4 лет, либо принудительные работы на срок до 5 лет, либо лишение свободы до 5 лет. Ну и в части 4 ст. 272 УК РФ «Деяния, предусмотренные ч. 1-3 ст. 272, если они повлекли тяжкие последствия или создали угрозу их наступления» для физических и должностных лиц наказание в виде лишения свободы сроком до 7 лет.

Так же предусмотрены наказания за нарушения требований законодательства. За невыполнение законного предписания Роскомнадзора по ст. 19.5 КоАП – максимальный штраф 500000 рублей; ст. 19.20 КоАП – срок до 90 суток при осуществлении деятельности по защите персональных данных без лицензии. Если это повлекло еще и ущерб, то ст.171 УК РФ влечет наказание в виде ареста до 6 месяцев и лишения права занимать должность сроком до 5-ти лет [44].

Штрафы и наказания предусмотренные по ст.13.11 КоАП РФ, ст. 272 УК РФ, ст. 137 УК РФ, несут за собой уверенность в защите прав человека в сфере персональных данных, но для нарушителей в таких неправомерных действиях иногда выгоднее выплатить штраф и получить большую выгоду от разглашения персональных данных. Злоумышленники изобретают новые методы для взлома и кражи персональных данных граждан, и для этого требуются новые способы защиты как организационных, программных так и технических. Законодательство в данное время не захватывает всех нюансов в данной сфере.

Безусловно требуется рассмотрение более динамичного развития законодательства в сфере защиты персональных данных. Нужно усилить контроль уполномоченных органов, которые должны четко выполнять все

действия по защите персональных данных. Необходимо обеспечивать безопасность персональных данных.

Информация о людях, ценных бумагах и т.п. имеет большую ценность. На этом и зарабатывают многие злоумышленники (например, журналисты, инсайдеры, мошенники). Уровень информационных технологий вырос до таких высот, когда защита информационных прав не так эффективна, как хотелось бы. В связи с развитием средств электронной коммерции и средств коммуникаций выросли злоупотребления, связанные с данными о человеке. Используются средства интеграции и быстрой обработки персональных данных, что создает огромную угрозу по правам и интересам человека.

Для того чтобы улучшить работу по защите персональных данных нужно привлекать специализированные компании работающих в сфере информационной безопасности, так как практика показывает, что самостоятельно реализовать данные требования по защите данных достаточно сложно. Имея опыт и квалифицированные ресурсы, такие компании способны реализовать требования законодательства. Они смогут разработать свой подход к реализации задач по защите персональных данных.

Вышеуказанные нормативно – правовые акты можно отнести к общедоступным и основным. Есть еще масса нормативно – правовых актов, защищающих наши права в области защиты персональных данных и несанкционированного их использования, но мы не будем пока углубляться в крайности.

Эти требования устанавливает законодательство, а государство создало уполномоченные контрольные органы государственной власти, которые обязаны осуществлять проверки по соблюдению правил в сфере защиты персональных данных и ответственности за их нарушения.

К контрольным уполномоченным органам относятся:

- Федеральная служба по надзору в сфере связи, информационных технологиях и массовых коммуникациях – Роскомнадзор

- Федеральная служба по техническому и экспортному контролю – ФСТЭК
- Федеральная служба безопасности Российской Федерации – ФСБ

На эти уполномоченные контрольные органы возлагаются обязанности по обеспечению контроля и надзора в правильности соблюдения всех требований в обработке персональных данных.

Уполномоченные органы, на которые возлагаются обеспечение контроля в соответствии Федерального закона от 27.07.2006 года №152 – ФЗ «О персональных данных» является федеральный орган исполнительной власти, который несет полную ответственность за соблюдение всех требований и норм в сфере связи, информационных технологиях и т.д. Уполномоченный контрольный орган обязан принимать письменные обращения граждан являющимися субъектами персональных данных для рассмотрения обращения о соответствии установленными правилами и требованиями по защите персональных данных и принять верное решение в установленных законодательством норм.

Уполномоченный контрольный орган наделяется правами и обязанностями в области защиты персональных данных, а именно имеет право:

- Осуществлять проверку общих сведений,
- Требовать от оператора обработки персональных данных предоставлять уточнения по всем областям персональных данных, в которых было воздействия незаконного характера,
- Запрашивать у физических и юридических лиц необходимую информацию для обеспечения и улучшения своих полномочий и прав, и строго на безвозмездной основе,
- Принимать меры для приостановки и прекращения обработки персональных данных в связи с нарушениями требований Федерального закона от 27.07.2006 года №152 «О персональных данных»,

- Отправлять в федеральный орган исполнительной власти, сведения связанные с мерами по обеспечению выполнения своих прямых обязанностей оператором персональных данных,
- Направлять в органы предоставляющим лицензию операторам, заявление для рассмотрения и принятия мер по приостановлению или полному прекращению своих действий лицензии,
- Направлять в правоохранительные органы для решения о возбуждении уголовного дела,
- Предлагать Правительству РФ для совершенствования улучшения или новые нормативно - правовые акты для защиты персональных данных,
- Привлекать к административной ответственности, нарушителей Федерального закона от 27.07.2006 года №152 «О персональных данных».

Проверки, как и везде осуществляются по двум типам плановая и внеплановая; документарная и выездная. Плановая проверка проводится согласно утвержденному плану и доступна на официальном сайте. План график формируется загодя и начинает свое действие с наступления нового календарного года. Например, сводный план график государственной проверки Администрации МО Всеволожского муниципального района можно увидеть на сайте Управления Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека по Ленинградской области [48].

Плановые проверки на основании ст. 9 Федерального закона от 26.12.2008 года № 294 «О защите прав юридических лиц и индивидуальных предпринимателей» проводятся для утверждения правомерности того, что юридическое лицо соблюдает все требования в процессе осуществления своей деятельности. О Проведении плановой проверки юридическое лицо уведомляет орган по управлению контролем максимум за три дня до начала проверки, заказным письмом либо вручением лично в руки. Плановые проверки проводятся не чаще одного раза в три года.

Внеплановые проверки на основании ст. 10 Федерального закона от 26.12.2008 года № 294 «О защите прав юридических лиц и индивидуальных предпринимателей» могут проводится при возникновении оснований. В первую очередь по письменной жалобе граждан о нарушении прав человека, либо по приказу государственного контроля, либо по поручению Президента РФ или Правительства РФ, а также по требованию исполнительного органа. Уведомление такой проверки должно осуществляться не позднее двадцати четырех часов до начала проверки.

Плановая и внеплановая проверки могут быть двух типов, документарная и выездная. Документарная проверка проводится для проверки сведений, содержащихся в документах для подтверждения их правомерности и подлинности. Проводится по месту нахождения государственного органа, осуществляющего контроль. Юридическое лицо обязано предоставить запрашиваемые государственным органом документы в виде копия заверенных печатью и подписью руководителя. Если будут обнаружены ошибки, их нужно устранить и исправить в течении 10 рабочих дней. Если проверка документов не удовлетворит требования государственного контроля, не представлены будут документы либо будут найдены нарушения, то государственный орган вправе произвести выездную проверку.

2.2 Судебная и административная практика по защите персональных данных.

Этот случай был взят мной из событий нашего СНТ «Спутник» в котором я непосредственно участвовала как член правления данного СНТ

В соответствии со ст. 7 ФЗ -152 «О персональных данных» получившие доступ к персональным данным операторы и другие лица не имеют права раскрывать и распространять третьим лицам персональные данные без согласия субъекта персональных данных.

Статьей 6 Закона установлено, что обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.

Члены СНТ Спутник написали коллективное заявления в правоохранительные органы на председателя данного СНТ. Из него следует, что в апреле 2022 г. в общедоступном месте на входной двери в правление СНТ « Спутник» председателем СНТ Боровским размещены персональные данные членов садоводства без их согласия, а именно: « Список членов СНТ «Спутник», не выплативших 3500 руб. за установку СИП». В списке указаны позиции, состоящие из инициалов должников и номеров участков в садоводстве. Этот список висел с 01 апреля по настоящее время. В результате чего персональные данные членов садоводства стали доступны неопределенному кругу лиц. В действиях председателя правления СНТ «Спутник», усматриваются признаки административного правонарушения, предусмотренного ст. 13.11 КоАП РФ, а именно нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

На судебном заседании председатель СНТ Спутник факт совершения правонарушения не отрицал, вину признал. Выслушав председателя рассмотрев материалы дела, мировой судья пришел к выводу, что факт совершения председателем СНТ административного правонарушения, предусмотренного ст. 13.11 КоАП РФ, и его виновность подтверждены совокупностью исследованных в судебном заседании доказательств, которые суд оценивает в соответствии с требованиями ст. 26.11 КоАП РФ.

Постановил:

Председателя правления СНТ «Спутник» признать виновным в совершении правонарушения, предусмотренного ст. 13.11 Кодекса РФ об административных правонарушениях и назначить ему наказание в виде предупреждения.

Этот случай был решен в пользу истца, но есть и такие решения, которые остаются без удовлетворения. Пытаясь найти в системе интернета судебных решений в пользу истца, оказалось плачевным, так как таких дел практически нет, зато очень много решений в пользу ответчика. Ответчику нужно только доказать, что истец дал согласие на обработку персональных данных, а чаще всего это так и есть, хотя многие истцы даже не понимают, когда дают на это согласие. Например, я нашла один из многих вариантов судебного решения, с решение неудовлетворения. Информацию использовала из судебных практик суда из базы электронного журнала "Помощник адвоката" в Консультант Плюс [47]:

Иванов К.В. 25.05.2022 года обратился в суд с уточненным иском к Николаевой К.Т. о защите прав субъекта персональных данных, с компенсацией морального вреда.

Исковые требования мотивированы тем, что стороны состояли в браке, от которого имеют несовершеннолетних детей Иванову К.А. и Иванову К.Я.

В иске истец указал что на интернет-сайте в сервисе ВКонтакте, ответчик разместила персональные данные Иванова К.В. и несовершеннолетних детей Ивановой К.А. и Ивановой К.Я., включая их изображения, однако, истец не давал согласия на обработку, включая распространение, его персональных данных и детей, законным представителем которых он является, в связи с чем ответчик нарушила положения Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

Истец, с учетом уточнений исковых требований в порядке ст. 39 ГПК РФ, просил суд признать информацию, размещенную на интернет-странице https://vk.com/, информацией, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных; обязать Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций принять меры по ограничению доступа к информации в сети "Интернет", обрабатываемой с нарушением

законодательства Российской Федерации в области персональных данных, путем внесения указателя страницы сайта https://vk.com/ информационно-телекоммуникационной сети "Интернет", содержащую информацию, обрабатываемую с нарушением законодательства в области персональных данных, в Реестр нарушителей прав субъектов персональных данных; возложить обязанность на Николаеву К.Т. удалить персональные данные Ивановой К.А., содержащиеся на интернет-страницах; взыскать с Николаевой К.Т. в его пользу компенсацию морального вреда в размере 50000 рублей.

Судом установлено и из материалов дела следует, что Иванов К.В. и Николаева К.Т. состояли в зарегистрированном браке, от брака имеют двоих несовершеннолетних детей: Иванову К.А. и Иванову К.Я.

Николаевой К.Т. принадлежит интернет-страница https://vk.com/.

Обосновывая уточненные исковые требования, истец указывал, что на указанной интернет-странице Николаевой К.Т. были размещены без его согласия его фотографии, а также фотографии несовершеннолетних детей в подтверждение чего последним был представлен протокол осмотра доказательств от 18.07.2018 г. интернет-страницы: https://vk.com/ на интернет-сайте в сервисе ВКонтакте.

Проанализировав вышеприведенные нормы материального права, оценив собранные доказательства в их совокупности, суд пришел к выводу об отказе в удовлетворении исковых требований Иванова К.В. в полном объеме, полагая, что истцом в нарушение ст. 56 ГПК РФ не предоставлены достоверные и достаточные доказательства, свидетельствующие, что ответчик незаконно использовала персональные данные его и их несовершеннолетних детей, при этом суд установил, что информация, размещенная ответчиком на интернет-странице https://vk.com/, не является информацией, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, поэтому основания для включении указанной интернет-страницы в "Реестр нарушителей прав

субъектов персональных данных", с возложением на ответчика обязанности по удалению персональных данных Ивановой К.А., содержащихся на интернет-страницах; взыскании с Николаевой К.Т. в пользу истца компенсацию морального вреда в размере 50000 рублей, отсутствуют.

При этом суд исходил из того, что Николаева К.Т., размещая в интернет-странице фотографии своих детей, будучи их матерью, однозначно высказала свое согласие на размещение их персональных данных, в соответствии с положениями семейного законодательства ответчик имела предусмотренные законом права действовать в интересах детей.

На основании изложенного, руководствуясь ст. ст. 328, 329 ГПК РФ, судебная коллегия определила:

решение Всеволожского городского суда, находящегося по адресу ул. Вахрушева 14 от 30.06.2022года оставить без изменения, апелляционную жалобу Иванова К.В., действующего в своих интересах и в интересах несовершеннолетних Ивановой К.А. и Ивановой К.Я. - без удовлетворения.

Вывод

Юридическая ответственность за нарушение норм о персональных данных, играет большую роль в исполнении соответствующих требований по выполнению юридическим и физическим лицом своих обязательств. Это дает надежду на то, что уполномоченный оператор по обработке персональных данных будет исправно и честно, не нарушая законодательство выполнять свои прямые обязанности.

Законодательство определенно не совершенно в проблемах по защите персональных данных, они безусловно есть. Много пробелов и недостатков в сфере защиты персональных данных, но также есть законы, защищающие нас и наши данные в контроле уполномоченных органов, таких как Роскомнадзор, ФСТЭК, ФСБ.

Контрольные органы проводят плановые и внеплановые проверки для соблюдения все законодательных норм. Это обеспечивает порядок и ответственность в обеспечении правильности оформления, обработки и

хранения персональных данных юридическими лицами. При нарушении своих прямых обязанностей при обработке персональных данных, таки юридические лица могут быть минимум оштрафованы, а максимум лишение лицензии на исполнения своей деятельности.

Глава 3. Проблема защиты персональных данных в Российской Федерации и их решения.

3.1 Обеспечение защиты персональных данных в сети интернет

Проблема защиты персональных данных в гло

бальной сети интернета куда сложнее, чем на бумажном носителе. Ведь эти данные мы заносим в базу данных операторов, которые работаю с обработкой персональных данных. Такие организации как банки, страховые компании, коллекторские агентства, торговые сети (выдающие карты, по которым предоставляются скидки или бонусы для физических лиц), кол-центры (обрабатывающие базы данных физических лиц), образовательные учреждения, медицинские учреждения, туристические агентства, кредитные кооперативы, гостиницы, нотариальные конторы, вносят и сохраняют наши данные в своих базах. И это важная часть защиты и охраны данных от несанкционированного использования. Но и они не всегда могут обеспечить гарантии по сохранности и конфиденциальности личных данных. Эта проблема актуальна по сей день так как защитные системы не могут нам гарантировать сто процентной гарантии защиты наших персональных данных. Есть множество степеней защиты, мы вводим пароли, шифруем свои данные, устанавливаем противовирусные программы, но этого недостаточно. Несмотря на все защитные нами действия хакеры взламывают различные сервера и информационные системы. Для решения этих поставленных целей и задач потребуется множество времени и сил.

Самый распространённый вид утечки информации в сети интернет происходит при помощи самих граждан, они сами по доброй воле чаще всего, не ведая и не отдавая отчет своим деяниям, позволяют мошенникам себя обмануть. Мошенники взламывают личные странички в социальных сетях и от имени правообладателя странички пишут другим пользователям и вымогают денежные средства при помощи обманных сообщений «якобы попал в беду», заблокировали карту и много таких изощренных ложных сообщений. В таких ситуациях они чаще просят просто перевести некоторую

сумму денег на определенный номер телефона. Также мошенники действуют другим путем, звонят якобы клиенту из банка и говорят, что с их банковской картой случилась какая-то беда и для устранения неполадок с картой нужен номер карты и код. Чаще всего на такие уловки попадаются люди преклонного возраста или просто очень доверчивые, которые не были еще в таких ситуациях. После передачи данных или перевода денежных средств, мошенники исчезают и блокируют номера своих телефонов. Отследить потом злоумышленников очень сложно так как телефонные сим карты можно приобрести в наше время без паспорта и уточнения свои персональных данных. А если идти в суд, то это тоже практически ни к чему не приведет. Правоохранительные органы чаще не берутся просто за такие дела, и они остаются «висяком», поэтому человек понимая всю сущность проблемы, не будет обращаться в правоохранительные органы и тратить свое время, а просто смирится с утратой не крупной суммы. Поэтому в данной области нужно быть самому более ответственным подходить к таким событиям настороженно, до тех пор, пока не будут созданы защитные противовирусные программы от взлома таких сетей.

В сфере ответственности и защиты утечки информации в интернет-ресурсах мы определенно должны отталкиваться от Федерального закона от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации» [34]. Вся информация согласно этому закону должна распространятся с содержанием только достоверной информации об субъекте, если эти данные распространяются без использования СМИ, а исходя из Федерального закона от 07.07.2003 года №126-ФЗ «О связи» [37], то тут операторы связи должны оберегать данные субъекта и хранить его тайну. Хотя в настоящее время идентификация пользователя стоит под большим сомнением, при этом для множества сайтов условие идентификации субъекта очень важно.

В настоящее время очень небезопасно проводить платежи через систему Интернет так, как информация сохраняется или перехватывается кибератаками и происходят незаконные списания денежных средств.

Очень уязвима информация и ее оборот, которую мы часто передаем для предоставления различных нам услуг в государственные и муниципальные органы.

Главный на данный момент по имеющимся и хранящимся нашим персональным данных является портал Государственных услуг. Этим порталом пользуется практически вся Российская Федерация и только очень малый процент, который не использует и не зарегистрирован в этом портале. Скоро этот портал заменит нам все наши документы, носящие бумажный характер, например ИНН, паспорт, СНИЛС, страховой полис, водительские права, документы об образовании, военный билет и т.д. Нам не придется ходить куда-то и получать все эти документы, все будет в электронном виде. Достаточно скинуть свое фото, как все сведения будут собраны автоматически. Мы ведь даже если заказываем любую услугу предоставляем сканы своих документов на имущество и различные документы, которые там хранятся. Там хранится информация о нашем здоровье, что тоже не мало важно для утечки информации, ведь есть список таких болезней о которых не то, что рассказывать, думать не хочется. И вот такому порталу мы должны доверь на тысячу процентов, ведь там практически вся наша документальная жизнь. Информация такого рода должна быть обеспечена гарантированной безопасностью против любого внешнего воздействия.

Есть такие порталы не государственного воздействия, например, как банк. Банки сейчас практически каждый создает свой портал. Через такие порталы очень, казалось бы, удобно оплачивать коммунальные и различные услуги. Часто такие программы устанавливают в телефоны субъекты для минимизирования времени, при посещении банков. Оформляют кредиты и ипотеку, при чем тоже при оформлении ипотеки на сайт банка через портал,

гражданин обязан скинуть множество документов в отсканированном виде. А эти документы тоже носят конвенциальный характер.

Например, недавно был случай из жизни, я хотела оформить ипотеку на вторичное жилье, обратилась в «Сбербанк». Банк мне рекомендовал для удобства установить приложение банка по ипотекам «Домклик». При посещении банка я подписала заявление об обработке передачи данных с правом передачи третьим лицам. Я не очень хотела подписывать этот документ, но без него мне бы не оформили ипотеку. Уточню, что я ходила только в этот банк и к другим банкам по данному вопросу не обращалась. Спустя несколько дней меня начали атаковать различные операторы разных банков с предложением оформить у них ипотеку. Вот и возникает вопрос от куда появилась эта информация у других банков? Я не давала согласия на распространение данной информации для других банков. Тут начинаешь задумываться, а так ли безопасен этот банк, и насколько компетентно работают в этом банке сотрудники.

Для таких программ для идентификации субъекта существует Постановление Правительства РФ от 28.11.2011 года №977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» [12] в нем указаны понятия по работе в информационной системе. Идентификация субъектов передаваемых данных определяется как «сравнение идентификатора, вводимого участником информационного взаимодействия в любую из информационных систем с идентификатором этого участника в информационных системах, содержащих уникальные сведения о гражданине Российской Федерации на ведение которых федеральные органы исполнительной власти, органы государственных внебюджетных фондов уполномочены в соответствии с федеральными

законами, актами Президента Российской Федерации и актами Правительства Российской Федерации»[12].

Еще одно определение является крайне важным, субъект авторизуясь в электронных интернет-порталах передает свои персональные сведения, тем самым дает согласие на получения прав доступа для дальнейшего использования при работе в получении государственных и муниципальных услуг в электронном формате.

Конечно, бесспорно, получение услуги в электронном виде, как говорится, не выходя из дома, не тратить время на очереди очень удобна, экономит наше время. Но эти технологии так стремительно развиваются, что наше государство не успевает отреагировать на новшества кибератак на портал услугах.

Если в социальных сетях интернета у нас есть шанс предотвратить и устранить своими силами так сказать проблему мошеннических действий, путем не реагирования и не передавать свои данные, то в базах данных компаний, в которые мы предоставляем свои персональные данные у нас доступа нет и повлиять на ход событий мы не можем. Поэтому мы доверяем и рассчитываем на оператора обработки данных на его полномочия по защите персональных данных.

Например, только за этот год было совершено несколько утечек данных клиентов, определенных компании:

Например, в начале марта в «Яндекс.Еде» сообщили об утечке в Сеть номеров телефонов и информации о заказах клиентов. В компании сослались на недобросовестные действия одного из сотрудников [54]. Позднее в интернете появилась ссылка на ресурс, на котором персональные данные пользователей «Яндекс.Еды» были опубликованы в виде карты. Сайт позволял узнать адреса доставок, телефон, электронную почту, сумму заказов за шесть месяцев. Роскомнадзор заблокировал сайт с данными пользователей и составил на «Яндекс.Еду» протокол. Сервис был оштрафован на 60 тыс. руб. [49].

Еще один случай, Роскомнадзор составил в отношении «Ростелекома» административный протокол по ч. 1 ст. 13.11 КоАП, выявив во время проверки нарушения законодательства в сфере оборота персональных данных клиентов, сообщают «Ведомости» со ссылкой на представителя ведомства. Протокол передали в суд. Максимальная ответственность по однократному нарушению по этой статье предусматривает штраф в размере 100 тыс. руб., по повторному — до 300 тыс., напомнили опрошенные газетой юристы [55].

Роскомнадзор начал проверку по факту утечки данных в июне. Это произошло, после того как Telegram-канал «Утечки информации» сообщил, что неизвестные выложили в Сеть документы внутренних аккаунтов «Ростелекома». Они содержат более 109 тыс. строк с именами и фамилиями, электронными адресами и телефонами. «Ростелеком» начал расследование и сообщил, что проверяет на причастность к произошедшему уволенного сотрудника, который в декабре 2021 года скопировал часть внутреннего телефонного справочника.

Вскоре после этого «Утечки информации» сообщили, что в открытый доступ попали данные клиентов сервиса «Умный дом» — почти 713 тыс. строк, которые включают ФИО, адрес электронной почты, телефон, пароль и IP-адрес. В «Ростелекоме» заявили, что приняты срочные меры, чтобы инцидент не сказался на оказании услуг клиентам и их интересы не пострадали [49].

Такой же случай произошёл и с компанией «Гемотест». Мировой судебный участок московского района Вешняки оштрафовал компанию «Гемотест» за утечку 300 гигабайт персональных данных клиентов, следует из решения, опубликованного в судебной картотеке [56].

Решение вынесено 8 июля, к ответственности привлечена ООО «Лаборатория Гемотест», отмечается в картотеке.

В постановлении суда говорится, что компания признана виновной по ч. 1 ст. 13.11 КоАП (нарушения при обработке персональных данных) и ей назначен штраф в размере 60 тыс. руб.

На судебном заседании представители управления Роскомнадзора по Центральному федеральному округу сообщили, что в интернете были незаконно размещены персональные данные клиентов компании, после чего ведомство получило требование от Генпрокуратуры провести проверку.

Она состоялась во второй половине мая, был подтвержден факт утечки и нарушения закона «О персональных данных», говорится в постановлении. Там также указано, что доступ к учетной записи с данными клиентов злоумышленнику, который позже выложил их в Сеть, предоставил сотрудник компании. «Скачано было более 300 Гб информации с персональными данными клиентов, ответственность за сотрудников несет юридическое лицо», — говорится в постановлении.

В «Гемотесте» РБК сообщили, что оспорят решение суда и хотят получить от Роскомнадзора конкретные указания по устранению нарушений [49].

Если взять статистические данные за 2021 - 2022 год, то мы отчетливо можем увидеть разницу виновников утечки персональных данных в процентном соотношении например в 2021 году – руководители были виновниками в 9,1 %; хакеры всего лишь 2%; бывшие сотрудники 1,4%; а вот непривилегированные сотрудники набрали большее соотношении в 61,2%. Как мы видим в 2021 году превышающее значение по утечки информации все-таки служило у непривилегированных сотрудников. А вот в 2022 году все кардинально поменялось, утечка по вине руководителей составила 0,7%; по вине бывших сотрудников тоже составило 0,7%; у непривилегированных сотрудников процент утечки можно сказать максимально упал до 8,8%; а вот хакеры вырвались в перед и практически заняли весь процентный состав набрав 89,8%. Мы видим, как поменялся потенциал виновников, если ранее в этом списке лидировали сотрудники, то сейчас этим правом преобладают

хакеры. Эти данные были взяты мной из аналитического отчета «infowatch» [50]

В I полугодии 2022 года в Роскомнадзор и его территориальные органы поступило 144 835 обращений граждан, что на 25,5% больше, чем за аналогичный период прошлого года. Из них в письменном виде – 19 067, устно – 101, в электронном формате – 125 667. Если взять количество входящих обращений в первой половине 2022года в процентном соотношении, то будет выглядеть следующая картина, писем в электронном виде поступило 86,77%; письменно 13,16%; устно 0,7%.

Основные темы обращений граждан были по противоправной информации в интернете - это было массово 98,5%; жалоб по защите персональных данных поступило гораздо меньше всего 1,5% и это понятно, что многие даже не питают надежду на восстановления справедливости в данной области; в деятельности в сфере связи показатель 12,8%; а вот в сфере нарушения СМИ набрало немного больше показатель в сумме 15%.

Массовая доля жалоб, пришлась на март месяц. Граждане жаловались на размещения противоправной информации в том числе и фейковой информации касающейся военной операции на Украине. В 2022 году поступило в Роскомнадзор 63592 жалобы на фейки, что говорит нам о росте практически в два раза, так, например в 2021 году процент поступивших жалоб на противоправную информацию и фейки составляло 34629.

Мы отчетливо видим, как растут кибератаки в социальных сетях и электронных базах. В 2022 году все значительно усложнилось касаемо утечек персональной или конфиденциальной информации. Ситуация нам наглядно показала в статистике на сколько мы не готовы устоять перед хакерами и мошенниками, но зато отчетливо видим свои пробелы в индустрии информационных технологий.

Нужно принимать много усилий для защиты наших данных. Есть компании программирования, которые предлагают свои услуги в области защиты утечек. Такие компании предлагают свои услуги в виде контроля

всей почты, таких как Gmail, Mail.ru, Яндекс. Почта. Их системы автоматически анализируют текст сообщений, отправляемые файлы и изображения на наличие в них конфиденциальной информации. Их системы проверяют на соответствие политикам безопасности сообщения, переданные при помощи почтовых серверов Microsoft Exchange Server, Lotus Notes и др. Они могут ограничить доступ и видеть все входы и выходы по сети Интернета.

Такие компании внедряют свои кибер -системы и контролируют:

- Поток доступа персонала к определенным данным с возможным ограничение доступа;
- Мониторят весь рабочий процесс в течении рабочего времени, их системы видят какие сайты посещал сотрудник и сколько провел там времени;
- Возможна блокировка доступа сотрудников к определенным сайтам через рабочий компьютер;
- Контролируют доступ к интернет-ресурсам;
- Устанавливают программу отслеживания и записи входящих и исходящих звонков;
- Контролируют полностью отправку всех файлов, электронную почту, контролируют информацию, отправленную в облачные носители;
- Контролируют внешние устройства таких как USB – карт, различных дисков, принтеров и сканеров [58].

Эти компании защищают нас от различных угроз и атак по защите наших персональных данных и конфиденциальной информации, они могут увидеть и разоблачить мошеннические схемы и предотвратить недопустимы действия. Это, кстати, очень стимулирует сотрудника и саму трудовую дисциплину, ведь понимая, что сотрудника отслеживают на рабочем месте, он вряд ли пойдет на риск.

Таким компаниям мы должны доверять на сто процентов, но, к сожалению, часто они тоже не справляются с хакерскими атаками и их ИТ-безопасность страдает.

3.2 Рекомендации по совершенствованию в практике и законодательстве защиты персональных данных

Важнейшим решением стоит в усовершенствовании правового регулирования в защите персональных данных. Нужно дополнять ответственность за нарушения, чтобы не побуждало к противоправным действиям для распространения информации. Нужны жесткие меры в правовой системе. Если бы мы достигли тех вершин, что базы данных были усовершенствованы в использовании, отвечающие по полной безопасности, наши данные были надежно защищены, то можно было бы выйти на мировой информационный уровень. Всегда задаюсь вопросом почему хакеры так проворнее, хитрее, изощреннее, они всегда знают выход из ситуации, как можно обойти ту или иную программу, создают все возможные программные вирусы и все это в кратчайшие сроки. Почему наши айтишники, разработчики мыслят по-другому, почему их реакция не так быстра. Возможно, по той причине, что они не мотивированы поставленной задачей. Если мошенники делают свою работу, то они отчетливо понимаю, что как поработал, столько и заработал. Они понимают всю выгоду своему уму и скорости своих действий. Значит нам нужно рассматривать такой подход как было бы выгодно хакерам и мошенникам. Мотивация — это стимул и главная цель проделанной работы. Чем выше мотивация, тем выше результативность.

Что в данной ситуации можно рассмотреть, первое это оплата труда разработчикам, у них не должно быть фиксированного денежного содержания, либо должно быть минимальным, но с учетом премиальных. А вот от премиальных как раз и будет зависеть их работа. Разработчик должен четко понимать, что от его скорости и умения быстро реагировать, зависит

высота оплаты. Тут должны быть четко проставлены цели и цена. Если разработчик будет идейным это вообще большой плюс. Это то, что касается разработчика.

Ситуация с Банками тоже неоднозначна, как со стороны сотрудников банка, так и со стороны клиентов этого банка. Например, банк, когда запрашивает у клиента подписание справки для передачи третьим лицам, не должен настаивать. Если клиент не подписывает, то банк не вправе отказать в услуге. Достаточно справки подтверждения с переченью документов, что клиент предоставил. Для проверки документов, должна существовать единая база данных с ограниченным доступом для таких организаций, в которые необходимо их предоставлять. Банк как минимум может запросить все его интересующие документы в определенных организациях и органах. Например, справка по форме 2НДФЛ, ее можно запросить официально с налоговой инспекции, паспорт в паспортном столе и т.д. Это если стоит остро вопрос о подтверждении данных этих справок. Так и в других организациях.

Со стороны операторов, обрабатывающих персональные данные, то им наоборот нужно все ужесточить и усложнить. Они должны вести четкий отчет по приему, внесению и обработке информации, ежедневно отчитываясь о проделанной работе. Четко следить за сохранностью данной информации, исключая все возможные внешние и внутренние, постороннее воздействие. И если обнаружена угроза, то незамедлительно должен оповестить. На данный момент с 1 сентября этого года, институт «персональных данных» предпринял новые методы и решения в ряду нормативных актах по защите персональных данных Госдума приняла закон «О персональных данных», в них говорится об условиях, которые обязаны выполнять все компании при утечке информации. Они должны сообщить в Роскомнадзор в течение 24 часов, а сами результаты расследования этих утечек они должны предоставить в течение 72 часов. По мнению некоторых крупных компаний эти законы и поправки по защите персональных данных очень усложнят

работу компаний. Так как всех операторов обяжут приобрести совсем не дешевое оборудование, для выполнения функций по установки безопасности, чтобы предотвратить утечку и слив информации третьим лицам.

Например, институт «персональных данных» рассматривает предложения от крупных компаний, которые предлагают альтернативу для системы наказаний, которая подразумевает уголовную ответственность за массовые утечки базы персональных данных. В этом предложение предлагается удерживать с предприятий нарушителей процент с годового оборота. За факт утечки – 1%, но если предприятие не предупредило в течение 3х дней Роскомнадзор, то выплачивать придется -3%. В цифрах это примерно 500000-700000 рублей в государственную казну если при этом утечка данных будет свыше 1000 человек.

Система безопасности Банка и других организаций как государственных, так и муниципальных по защите персональных данных должны анализировать содержимое, иметь антивирусные средства, должны проводить полный мониторинг и контроль персональных данных, должны предотвращать от любых несанкционированных вторжений.

В социальных сетях я думаю, что основную часть ответственности за предоставление какой-либо информации, должен нести сам пользователь. Он должен понимать, что социальные сети имеют масштабный характер, и предоставляя какие-либо данные должен понимать, что это может возникнуть на всеобщее обозрение. Дополнительно, конечно, нужно составить документ в электронном виде, где пользователь таких сайтов как ВКонтакте, Одноклассники, Инстаграм и другие должен сам выбирать для себя приоритетную информацию. Он должен иметь право выбора какая информация для него имеет значение конфиденциальности, а какую можно выставить на всеобщую аудиторию. Так же операторы таких сайтов должны в рекламном виде предупреждать о возможных утечках и угрозах по использованию персональных данных пользователя. Его нужно также часто оповещать о таких противоправных действиях и махинациях со стороны

мошенников, как передача личных данных банковских карт. Если такая информация будет выходить автоматически при входе на страничку пользователя, думаю в разы уменьшится процент по передаче денежных средств мошенникам.

Малый и средний бизнес тоже находится в зоне риска, у каждой организации есть свой сервер, на котором хранятся все документы, счета, акции, да и вообще вся финансовая составляющая. Таким компаниям тоже есть, что терять. На них также устраивают хакерские атаки. Которым противостоять очень непросто. Зачастую культура защиты данных в компании очень низкая. Только представьте, что, если посторонние получают доступ к вашим счетам, сетевым программам (таким как 1С), как может использовать эти данные. Бывают даже криминальные случаи, когда мошенники выбирают сотрудника и подкупом либо шантажом начинают воздействовать на него. Такой сотрудник тоже запросто может слить всю информацию на сторону. Атаки с помощью инсайдера – самый опасный и трудно фиксируемый вид угрозы, и самый главный враг малого и среднего бизнеса.

Например в организации МИФНС №11 по Ленинградской области установлены программы АИС3, Налог 3, ДКС и 1С. И в этих базах хранится множество информации о принадлежащем имуществе, автомобилях их номера, данные на налогоплательщиков, счета, адреса прописки и т.д. За этими программами следит информационный отдел. Они каждый день проверяют ход истории всех движений в этих сайтах. От входящих требований, писем до проведения проверок камеральными проверяющими отделами. Устанавливают антивирусные программы и каждую неделю их обновляют, делают, так сказать, чистку программы. Если они обнаруживают подозрительные действия, начинаю проводить служебную проверку. Однажды у нас был такой случай инспектор налоговой службы приводил документы по выплате 3НДФЛ, без сопроводительных и подтверждающих обоснованность такой выплаты документов. Один сотрудник обнаружил

расхождение в документах и сообщил в службу безопасности. Служба безопасности в свою очередь завела служебное расследование и подключили информационный отдел для прослеживания действий по конкретному каналу. Естественно проследив, кто работал с этими документами было не сложно и сразу нашли виновника. Это не касается к утечке персональных данных, но это наглядно показывает, как сотрудник легко может бравировать на рабочем месте.

Но в этой истории так же видно, что нужен подход и к таким внутренним воздействиям. Нужна более жесткая проверка и защита, что сотрудник даже не мог подумать об умышленных необдуманных и неправомерных действий. В этом я вижу недоработку разработчиков, данной программы. Так, как если бы в данной программе был запрет проведения выплаты без дополнительных сведений и четкой проверке этих сведений на наличие таковых, то у сотрудника не получилось провести данные документ в действие. Поэтому разработчики данных программ тоже играют огромную роль в защите персональных и вообще любой конфиденциальной информацией. Еще на стаде проектирования, разработчик должен предусмотреть все возможные проблемы, связанные с утечкой данных, особенно внутренней.

Еще в качестве улучшения воздействия на сотрудников компаний, которые несут ответственность за внесение и хранение баз данных, за умышленные неправомерные воздействия, нужно не только делать выговор и увольнять, нужно установить штраф от 50000 рублей. Такая сумма очень существенна для любого среднего звена гражданина.

Если с сотрудником организации все понятно, что и как с ним действовать и как на него можно воздействовать и предотвратить утечки, то с внешними конкурентами не так все просто. В таких компаниях сидят профессионалы и они действуют наверняка, они понимают четкую цель своих действий. В таких компаниях работают лучшие информационные разработчики. Они создают программы уловки, для копирования данных

конкурирующей компании. Даже, казалось бы, простая флэш карта, может оказаться не такой безобидной.

Бывают разные виды утечек например:

- случайные утечки – происходят из-за потери физических носителей (сим-карты, флешки, планшеты, смартфоны), раскрытия паролей в следствие ошибочных действий человека,
- умышленные утечки из-за предоставления избыточных прав доступа – разглашение допускают сотрудники, имеющие доступ к закрытым IT-данным,
- умышленные инсайдерские утечки – сотрудник может специально раскрыть данные за пределами компании, иногда даже не имея легального доступа к информации [58],
- кража информации – осуществляется извне при помощи IT-инструментов (вирусы, вредоносные программы, хакерские атаки) или технических устройств (фото-, видеонаблюдение, подслушивающая аппаратура),
- кража носителей информации – физическое хищение устройств, непосредственно использующихся для хранения: банка данных, паролей, персональной информации,
- взлом ПО – проникновение в систему предприятия с помощью неучтенных уязвимостей или вредоносных программ.

Борьба должна быть с такими видами утечек по каждой индивидуальна. В первую очередь нужно установить сложные паролевые системы возможен биометрический доступ к особо важным данным. Использовать криптографические методы шифрования для защиты конфиденциальной информации и персональных данных, потому что это самая надежная защита самой непосредственно информации, а не доступа к этой информации.

Нужна зачистка не нужной информации, которая находится на хранении в базах. Нужно удалять те документы, которые уже не понадобятся и у этих документов не установлен срок хранения. Если документы

находятся в бумажном носителе, то в обязательном порядке нужно приобретение Шредер для уничтожения бумажных документов, так как выбросив их вы тоже попадаете под статью об утечке информации. Ведь неизвестно куда такие документы и в какие руки могут попасть. Возможно использование IRM — это контейнеризация каждого документа, содержащего ценные сведения[59]. Работает это так: к каждому документу привязывается информация о ключах шифрования и доступе. Даже если его украдут (например, на флешке), не смогут прочитать на своем устройстве. Внедрение такого решения обойдется дорого, но оно того стоит, если у вас на руках очень важная информация.

Если данные все-таки были похищены хакерами, то нужно установить, где, как и когда это произошло. Собрать если такое возможно доказательства виновников и определить виновника, и подать на него в суд. В данном случае, конечно, много не вернуть и не исправить, но можно наказать виновника как на привлечение к ответственности за не правомерные действия, так и рублём и получить материальную компенсацию.

У нас в принципе в данной области по защите персональных данных, в области правоприменительной практике, есть множество организационных, технических, кадровых и правовых трудностей. Нужно многое менять в правоохранительной системе, нужно дополнять защитные, контролирующие действия для охраны, проверки и защиты персональных данных. Нужно больше уполномочивать органы по защите персональных данных. Ужесточение в наказательной базе при нарушении и несанкционированного вмешательства в персональные данные и конфиденциальную информацию. Штрафные санкции должны быть такими же высокими, как и в зарубежных странах. Высокий штраф может оказать ключевую роль в решении пойти на неправомерные поступки, так как в мелких мошеннических деяниях это неоправданные риски.

Ужесточение наказания за неправомерные действия оператором по защите персональных данных и, в частности, обычных граждан, посягающих

на персональные данные и любую конфиденциальную, думаю сильно повлияют на большинство нарушителей.

Вот, например, если мы возьмем КоАП РФ, то там статьи, предусмотренные для защиты персональных данных, при нарушении этих статей, нет уголовной защищенности. Например такой статьи как ст.19.4 КоАП РФ «Неповиновение законному распоряжению должностного лица органа, осуществляющего государственный надзор (контроль), должностного лица организации, уполномоченной в соответствии с федеральными законами на осуществление государственного надзора, должностного лица органа, осуществляющего муниципальный контроль»[8], то мы увидим, в этих статьях, что нарушая закон, а тем более неповиновение этому закону влечет наказание в виде штрафа. Я с этим категорически не согласна, считаю, что это довольно суровое предписание для выполнения своих прямых обязанностей и если таковые не исполняются, то это уже можно отнести как предательство законов. Предательство законов — это халатное и наплевательское отношение, которое должно быть наказуемо более сурово. Если по такой статье ввести уголовную ответственность, думаю оператор будет более дисциплинирован.

Взять, например п2. Ст. 13.11 КоАП РФ, за обработку персональных данных без письменного согласия субъекта, нужно применять уголовную ответственность, а не обходится штрафом. Так как обрабатывая и работая с персональными данными субъекта, я рассматриваю как вторжение в его личную жизнь, что должно быть сурово наказано.

Согласна, что не вовсе статьи можно, да и нужно ли дополнять уголовной ответственностью, но нужно четко понимать разграничения этих деяний. И если это деяние по халатности, либо такие деяния, которые не несут особого вреда не субъекту ни его репутации, то тут можно наказать рублем, но таким, чтобы долго вспоминалось. А вот если это умышленное, то это нужно переводить в часть уголовной ответственности.

Возьмем п.6 ст. 13.11. КоАП РФ, использование базы с персональными данными без средств автоматизации, можно отнести к уклонению от своих обязательств, и если такие деяния были обнаружены, но не нанесли вреда субъекту, то можно ограничится штрафом и желательно максимальный до 1000000 рублей, но при повторном нарушении применять уголовную ответственность.

Не соглашусь с наказательным положением и по ст. 137 Уголовного Кодекса РФ «Нарушение неприкосновенности частной жизни»[30], в этой статье за распространение частной информации на бубличное выставление и огласка в сми карается законом, всего лишь от 2х до 5ти лет. Тут, конечно, тоже должно быть дополнение к каждому пункту, ведь распространяемая информация бывает тоже разной, и тут нужно рассматривать степь нанесения морального ущерба. Так распространив информацию в СМИ, можно опозорить субъекта, и он будет жить с этим всю жизнь, будет испытывать моральные муки. Когда в свою очередь виновник максимум отсидел 5 лет, а то и выйдет по УДО, выходит с чистой совестью и не вспоминает о своих деяниях. В таких случаях виновник тоже должен долго осознавать свою вину. Если он отсидел свой положенный срок, нужно обязать выплачивать материальный пожизненный ущерб либо сроком до 25 лет, в виде моральной компенсации за причинённые страдания, сумма может быть от 5000 до 50000 рублей в месяц.

В статье 272 Уголовного кодекса РФ «Неправомерный доступ к компьютерной информации» [30], я бы тоже ужесточила наказание в каждом пункте отдельно. Например, в п.1 данной статьи наказание предусмотрено в виде штрафа до 200000 рублей и лишения свободы до 4х лет. Я бы заменила наказание в виде штрафа до 500000 рублей и лишением свободы до 7 лет; в п. 2 также заменила штраф с 300000 рублей до 500000 и лишением свободы с 4х лет до 10 лет; в п.3 наказание предусмотренное я бы заменила в виде штрафа с 500000 рублей на 1000000 рублей, а срок лишения свободы с 5 лет до 15; ну

и в п.4 при возникновении тяжких последствий лишением свободы до 25 лет, с компенсационной выплатой пострадавшему.

Как и выше указанной статье я бы применила такие же карательные меры и к ст.183 Уголовного кодекса РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» [30].

Вывод

Что можно подчеркнуть в третьей главе, это то, что статистика нам четко показывает, как сильно меняется все не в нашу пользу, как мошенники и хакеры усовершенствуют свои навыки. Что за последний только год в связи с ухудшением обстановки на фоне спецоперации на Украине, было зафиксировано множество кибер атак. Как в Российской Федерации произошли утечки таких известных компаний как «Яндекс Еда», «Гемотест», «Ростелеком» и др. Все они конечно были наказаны в виде наложения штрафа. Были переведены статистические данные за 2021 и 2022 года по обращению и вида обращения гражданами по защите персональных данных, на которых мы видим разницу и спрос.

В исправлении ошибок и недочетов в области защиты персональных данных я привела ряд предложений по изменению и улучшению работы по безопасности защиты персональных данных. Были предложены методы усовершенствования в разных сферах как, касаемо определенного субъекта(сотрудника), так и оператора, также предложения по разработки определенных программ и как избавиться от минусов при начальной разработке таких программ. Базовые предложения для социальных сетей. Как можно заранее предупредить пользователя социальной сети о грядущей опасности.

Можно увидеть послабление в действующих нормативно -правовых актах. Изучив их, я увидела, что иногда можно нарушить, не думая о последствиях, так наказание не стоит «выеденного яйца». Я дополнила

некоторые статьи так как вижу их я в будущем. Считаю, что ужесточение законов влечет за собой правопорядок всех, кто относится к обработке, защите и хранению персональных данных и любой конфиденциальной информации. Когда ответственный за любые действия с персональными данными и конфиденциальной информацией, будет четко понимать последствия и очень жесткое меры наказанию, то я думаю процент обращений граждан по защите персональных данных максимально сократится.

Заключение

Анализируя выше написанное по поводу защиты и охраны персональных данных можно утверждать, что существует множество мнений и многих авторов есть своя точка зрения по определению и классификации терминологии, информации и нормативно правовых актов. Есть два доступа к информации открытый и закрытый. К закрытому доступу относится Указ Президента «Об утверждении перечня сведений конфиденциального характера», что подразумевает под собой конфиденциальность персональных данных.

Есть определения понятия «персональных данных» и что к ним относится в ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ (ред. от 14.07.2022) "О персональных данных", в ней четко указано кто и как должны хранить и обрабатывать персональные данные. Что такое персональные данные – это имя, фамилия, дата и место рождения, паспортные данные, прописка, должность, профессия и многое другое, что относится непосредственно к физическому лицу. Кто несет ответственность, кто является оператором обработки персональных данных, что относится к уничтожению, хранению, предоставлению, блокировке и автоматизации данных.

На основании всех нормативно правовых актов понятно, что персональные данные — это конфиденциальная информация и за несоблюдение законных действий по отношению передачи, обработке и других действий, наступает юридическая ответственность.

Многие утверждают, что безопасность конфиденциальной информации носит безопасный характер на высоком уровне, с чем я крайне несогласна. Я считаю персональные данные находятся в состоянии правовой незащищенности от несанкционированного доступа. И мною были приведены примеры, в каких областях это не доработано. Если брать рабочую специфику, при устройстве на работу, то тут практически все понятно и с безопасностью и обработкой и хранением. В трудовом

законодательстве гл. 14 ФЗ-197 «Трудовой кодекс РФ», пописаны четкие условия обработки, хранения и юридическая ответственность за несоблюдение. В данной сфере легче найти нарушения и пресечь противодействия, нежели в информационной, либо в частном порядке, когда такими деяниями помышляют мошенники и наживаются на безграмотности и социально не защищенных физических лиц.

Общие нормативно правовые акты обеспечивают безопасность в защите ограниченного доступа к информации, но все равно далеки от совершенства. Вычислить утечку информации и довести до судебного определения вины с юридической ответственностью и наложением штрафа за содеянные правонарушения, крайне редкое явление.

Необходимо создать такой механизм защиты в правовых отношениях по защите персональных данных, чтобы можно было с первой подачи собственных данных по цепочке отследить несанкционированную утечку и предотвратить последствия. К этому процессу необходимо подключить информационных специалистов по разработке специальных программ блокировок по утечке несанкционированной информации. Так же усилить контроль нормативно правовыми актами и законами ужесточающее наказание и увеличение штрафов за ответственность утечки и незаконного использования персональных данных.

Замечу, что органы государственной власти не бездействуют и 6 июня 2022 года Госдума приняла поправки к закону «О персональных данных», в них говорится об условиях, которые обязаны выполнять все компании при утечке информации. К этому подключен Роскомнадзор которому операторы должны сообщить об утечке в течение 24 часов, а результаты расследования утечек они должны предоставить в течение 72 часов. Увеличились и штрафы, хотя я считаю, что сумма штрафов занижена. За факт утечки – 1%, но если предприятие не предупредило в течение 3х дней Роскомнадзор, то выплачивать придется -3%. В цифрах это примерно 500000-700000 рублей в

государственную казну если при этом утечка данных будет свыше 1000 человек.

Юридическая ответственность за нарушение норм о персональных данных, играет большую роль в исполнении соответствующих требований по выполнению юридическим и физическим лицом своих обязательств. Это дает надежду на то, что уполномоченный оператор по обработке персональных данных будет исправно и честно, не нарушая законодательство выполнять свои прямые обязанности.

Законодательство определенно не совершенно в проблемах по защите персональных данных, они безусловно есть. Много пробелов и недостатков в сфере защиты персональных данных, но также есть законы, защищающие нас и наши данные в контроле уполномоченных органов, таких как Роскомнадзор, ФСТЭК, ФСБ.

Контрольные органы проводят плановые и внеплановые проверки для соблюдения все законодательных норм. Это обеспечивает порядок и ответственность в обеспечении правильности оформления, обработки и хранения персональных данных юридическими лицами. При нарушении своих прямых обязанностей при обработке персональных данных, таки юридические лица могут быть минимум оштрафованы, а максимум лишение лицензии на исполнения своей деятельности.

Можно подчеркнуть, что статистика нам четко показывает, как сильно меняется все не в нашу пользу, как мошенники и хакеры усовершенствуют свои навыки. Что за последний только год в связи с ухудшением обстановки на фоне спецоперации на Украине, было зафиксировано множество кибер атак. Как в Российской Федерации произошли утечки таких известных компаний как «Яндекс Еда», «Гемотест», «Ростелеком» и др. Все они конечно были наказаны в виде наложения штрафа. Были переведены статистические данные за 2021 и 2022 года по обращению и вида обращения гражданами по защите персональных данных, на которых мы видим разницу и спрос.

В исправлении ошибок и недочетов в области защиты персональных данных я привела ряд предложений по изменению и улучшению работы по безопасности защиты персональных данных. Были предложены методы усовершенствования в разных сферах как, касаемо определенного субъекта(сотрудника), так и оператора, также предложения по разработки определенных программ и как избавиться от минусов при начальной разработке таких программ. Базовые предложения для социальных сетей. Как можно заранее предупредить пользователя социальной сети о грядущей опасности.

Можно увидеть послабление в действующих нормативно -правовых актах. Изучив их, я увидела, что иногда можно нарушить, не думая о последствиях, так наказание не стоит «выеденного яйца». Я дополнила некоторые статьи так как вижу их я в будущем. Считаю, что ужесточение законов влечет за собой правопорядок всех, кто относится к обработке, защите и хранению персональных данных и любой конфиденциальной информации. Когда ответственный за любые действия с персональными данными и конфиденциальной информацией, будет четко понимать последствия и очень жесткое меры наказанию, то я думаю процент обращений граждан по защите персональных данных максимально сократится.

Список используемой литературы и источников

1. Алистархов В. Выбор вида наказания работнику за разглашение сведений с ограниченным доступом // Трудовое право. 2014. №9. С. 37 – 48.
2. Бадьина А. Обработка, порядок хранения и передвижения персональных данных // Кадровик. Кадровое делопроизводство. 2012. №1. С. 162 – 171.
3. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: учебник. СПб., 2001. С.224-225
4. Ветров Д.М. Защита персональных данных и защита информации на предприятии. Некоторые спорные вопросы применения // Проблема права. Челябинск, 2010, №1. С. 119
5. Грибанов А.А. Общий регламент о защите персональных данных (General Data Protection Regulation): идеи для совершенствования российского законодательства / А.А. Грибанов // Закон. 2018. N 3. С. 149 – 162.
6. Давыдова Е. В. Что работодателю необходимо знать о персональных данных работников? // Отдел кадров коммерческой организации. 2015. №3. С. 33 – 42.
7. Климович Е.В. О сущности понятия «персональные данные» как конфиденциальной информации особой категории // Международные юридические чтения: материалы ежегодной международной научно-практической конференции (14 апреля 2005г). ОМСК, 2005 Ч.2. С. 27.
8. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 16.04.2022) (с изм. и доп., вступ. в силу с 27.04.2022)
9. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 №6-ФКЗ, от 30.12.2008 №7-ФКЗ, от 21.07.2014 N 11-ФКЗ). // «Собрание законодательства РФ», 04.08.2014, №31, ст. 4398.
10. Назаров, Д. М. «Основы обеспечения безопасности персональных данных в организации» [Текст]: учеб. пособие / Д. М. Назаров, К. М. Саматов; М-во

науки и высш. образования Рос. Федерации, Урал. гос. экон. ун-т. — Екатеринбург: Изд-во Урал. гос. экон. ун-та, 2019. — 118 с.
11. Отрасли права. аналитический портал: http://отрасли-права.рф/
12. Постановление Правительства Российской Федерации от 28.11.2011 г. № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»//СЗ РФ. - 05.12.2011. - №49. – ст. 7284
13. Постановление Правительства Российской Федерации от 15.06.2022 № 1066 "О размещении физическими лицами своих биометрических персональных данных в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица"
14. Постановление Правительства Российской Федерации от 16.06.2022 № 1089 "Об утверждении Положения о единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица"
15. Постановление Правительства Российской Федерации от 15.06.2022 № 1067 "О случаях и сроках использования биометрических персональных данных, размещенных физическими лицами в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица"

16. Разъяснения Роскомнадзора «Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве»// http://rkn.gov.ru/
17. Разъяснения Роскомнадзора О вопросах отнесения фото и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки // http://25.rsoc.ru
18. Разъяснения Роскомнадзора О вопросах отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки // http://25.rsoc.ru
19. Развитие регулирования: новые вызовы в условиях радикальных технологических изменений: доклад к XX Апрельской международной научной конференции по проблемам развития экономики и общества, Москва, 9 - 12 апреля 2019 г. / М.Я. Блинкин, А.С. Дупан, А.Ю. Иванов [и др.]; руководитель авторского коллектива Ю.В. Симачев. Москва: Изд. дом Высшей школы экономики, 2019. 88 с.
20. Савельев А. И. Законодательство о локализации данных и его влияние на рынок электронной коммерции в России // Закон. 2014. №9. С. 51 – 68.
21. Серков П. П. Административная ответственность в российском праве: современное осмысление и новые подходы: монография. М.: Норма, Инфра-М, 2012. 480 с.
22. Свирин Ю. А. Дивергенция в системе права: монография. М.: Астра Полиграфия, 2012. 392 с.
23. Ситникова Е. Г., Сенаторова Н. В. Трудовой договор: некоторые основания прекращения. М.: Библиотечка «Российской газеты», 2014. Вып. №2. 192 с.
24. Ситникова Е. Г., Сенаторова Н. В. Трудовой кодекс Российской Федерации. Раздел III. Трудовой договор: постатейный научно-практический комментарий М.: Библиотечка «Российской газеты», 2013. Вып. VII–VIII. 720 с.

25. Соколова О.С. Проблемы реализации Федерального закона "О персональных данных" / О.С. Соколова // Современное право. 2006. N 9. С. 37 - 41.
26. "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ (ред. от 25.02.2022) (с изм. и доп., вступ. в силу с 01.03.2022), ТК РФ Статья 86. Общие требования при обработке персональных данных работника и гарантии их защиты.
27. Терещенко Л. К. Доступ к информации: правовые гарантии // Журнал российского права. 2010. №10. С. 46 – 53.
28. Терещенко Л. К., Тиунов О. И. Правовой режим персональных данных // Журнал российского права. 2014. №12. С. 42 – 49.
29. Трудового кодекса РФ). М.: Библиотечка «Российской газеты», 2013. Вып. 1. 192 с.
30. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 25.03.2022) УК РФ Статья 137. – «Нарушение неприкосновенности частной жизни»
31. Указ Президента РФ от 17.03.2008 № 351 (ред. от 25.07.2014) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
32. Федосин А. С. Защита конституционного права человека и гражданина на неприкосновенность частной жизни прав форматизированной обработке персональных данных в РФ: автореф. дис. канд. юрид. наук. Саранск, 2014. 27 с.
33. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (ред. от 21.07.2014). // «Собрание законодательства РФ», 31.07.2006, №31 (1 ч.), ст. 3451.
34. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» (от 06.07.2016 N 374-ФЗ). // «Собрание законодательства РФ», 31.07.2006, №31 (1 ч.), ст. 3448.

35. Федеральный закон "О персональных данных": научно-практический комментарий. Под редакцией А.А. Приезжевой, 2015 г. – 177 стр. От коллектива Роскомнадзора.
36. Федеральный правовой портал «Юридическая Россия»: http://law.edu.ru/
37. Федеральный закон от 07 июля 2003 г. №126-ФЗ «О связи» // СЗ РФ. – 2003. - №28. – ст. 2895
38. Федеральный закон от 21 июля 1997 г. № 118-ФЗ «О судебных приставах» // СЗ РФ. – 28.07.1997. – № 30. – ст. 3590
39. Федеральный закон от 07.05.2013 № 99-ФЗ (ред. от 28.12.2013) «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» и Федерального закона «О персональных данных»
40. Федеральный закон "О внесении изменений в статьи 14 и 14.1 Федерального закона "Об информации, информационных технологиях и о защите информации" и статью 5 Федерального закона "О внесении изменений в отдельные законодательные акты Российской Федерации" от 14.07.2022 N 325-ФЗ (последняя редакция)
41. Федеральный закон "О внесении изменений в Федеральный закон "О персональных данных", отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона "О банках и банковской деятельности" от 14.07.2022 N 266-ФЗ (последняя редакция)
42. Цыдакова Э.А. Гарантии охраны и защиты персональных данных человека и гражданина // Конституционное муниципальное право .2007. №14
43. Шередин Р.В. Защита персональных данных: новые требования: интернет-интервью 10.01.2012 [Электронный ресурс] / Р.В. Шередин. – Режим доступа: URL: http://oblteleset.ru/2012/10-01-2012-zashhitapersonalnyxdannyx-novye-trebovaniya/ (дата обращения: 02.09.2022)
44. Электронный ресурс: https://rkn.gov.ru (дата обращения 10.12.2022)

45. Электронный ресурс: https://www.consultant.ru/ (дата обращения 10.12.2022)
46. Электронный ресурс: https://base.garant.ru/ (дата обращения 10.12.2022)
47. Электронный ресурс: https://demo.consultant.ru/cgi/online.cgi?req=doc&ts=rl1XeIT08lLD0MfB&cacheid=5511A7B81FF1C630499D611DCB9AB7A8&mode=splus&rnd=D72hEA&base=CJI&n=128542#qx7XeITiv0X5m1WK (дата обращения 15.11.2022)
48. Электронный ресурс: http://47.rospotrebnadzor.ru/ (дата обращения 05.09.2022)
49. Электронный ресурс: https://www.rbc.ru/society/12/07/2022/62cd46ce9a794714baa4a984 (дата обращения 26.10.2022)
50. Электронный ресурс: https://www.infowatch.ru/ (дата обращения 10.10.2022)
51. Электронный ресурс: http://lawlibrary.ru/ (дата обращения 18.08.2022(
52. Якушев В.С. О понятии правового института // Правоведение. 1970. №6. С. 62–63.
53. Янковский Р.М. Legal design: новые вызовы и новые возможности / Р.М. Янковский // Закон. 2019. N 5. С. 76 - 86.
54. Act on the Protection of Personal Information Act No. 57 of (2003) [Электронный ресурс]. – Режим доступа: URL:http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf (дата обращения: 25.12.2022)
55. Arkhipov V., Naumov V. The Legal Definition of Personal Data in the Regulatory Environment of the Russian Federation: Between Formal Certainty and Technological Development / V. Arkhipov, V. Naumov // Computer Law & Security Review. – 2016. – No. 32. – P. 872, 877, 883, 886
56. Brazilian Data Protection Law (LGPD) (As amended by Law No. 13,853/2019) [Электронный ресурс]. – Режим доступа: URL:https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_La w.pdf (дата обращения: 03.01.2023)

57. California Consumer Privacy Act of 2018 [Электронный ресурс]. – Режим доступа: URL: https://oag.ca.gov/privacy/ccpa (дата обращения: 14.11.2022)
58. The personal data protection bill, 2018 [Электронный ресурс]. – Режим доступа: URL:https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill, 2018.pdf (дата обращения: 17.02.2023)
59. The Personal Information Protection and Electronic Documents Act (PIPEDA) 13.04.2000 [Электронный ресурс]. – Режим доступа: URL: http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf (дата обращения: 14.01.2023)