МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»
Институт права
(наименование института полностью)

Кафедра Предпринимательское и трудовое право
(наименование)

40.04.01 Юриспруденция
(код и наименование направления подготовки)

Правовое обеспечение предпринимательской деятельности
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему Проблемы правового регулирования конфиденциальной информации в предпринимательской деятельности.

Студент РВ. Клопотов
(И.О. Фамилия) (личная подпись)

Научный руководитель канд. пед. наук, доцент Е.М.Чертакова
(ученая степень, звание, И.О. Фамилия)

Тольятти 2021

Оглавление

Введение

Количество информации, с которой приходится работать участником предпринимательской деятельности, неуклонно возрастает. При этом возрастает и количество способов передачи и хранения этой информации.

Одновременно с этим информация из нематериального объекта представляющего интерес или регулирующего взаимодействия внутри организации или предпринимательского сообщества превращается в объект правового регулирования со стороны государства. При этом в правовом поле складывается ситуация, когда регулируется не информация как таковая, поскольку это слишком общее понятие, а лишь ее проявления в той или иной форме. Например, телекоммуникационная информация, информация связанная с государственной и коммерческой тайной, информация о персональных данных, информация публикуемая в средствах массовой информации. Каждый из этих аспектов использования информации присутствует в предпринимательской деятельности, в том или ином виде и при работе с каждым из них нужно оценивать степень ее конфиденциальности, возможности или не возможности при ее утечки и разглашении нанести судебные риски для предпринимательской деятельности.

Подобные риски в своей перспективе способны создать ущерб. Причем этот ущерб может быть разноуровневый это и прямой материальный ущерб, потерянная выгода, репутационный ущерб, ущерб несущий правовые последствия для юридического лица или предпринимателя как субъекта права. Практика показывает законодательство часто запаздывает за проявлениями способов нарушения конфиденциальности вводя правовые новеллы как ответ на уже существующие нарушения права субъектов правовых отношений.

Особенно остро проблемы обработки персональных данных встает перед субъектами малого и среднего бизнеса, которые часто даже не

осознают, что работают с информацией конфиденциального характера требующего особого правового режима и соответствующего технического и юридического сопровождения.

Актуальность проблемы правового регулирования при работе с персональными данными клиентов состоит в проблеме возникновения ответственности субъекта предпринимательского права в случае неправомерного использования данной информации сотрудниками или третьими лицами. А также в построении специфического внутреннего документооборота связанного с получением согласия владельцев персональных дынных при совершении сделок и /или оказании услуг, так как в этом случае законодательство подразумевает работу с конфиденциальной информацией требующей специального обращения.

Уровни применения закона о персональных данных с каждым годом растут так как расширяется перечень сведений которые законодатель включает в состав информации идентифицирующей личность. Это приводит к постоянному обновлению нормативной базы на уровне как законов так и подзаконных актов. Систематизация юридических нововведений их обобщению и кодификации посвящены научные работы разного уровня, от магистерских и кандидатских работ до докторский монографий. Что является признаком актуальности темы работы и ее востребованности для юридической науки.

Объектом магистерской работы выступают общественные отношения связанные с оборотом персональных данных клиентов в процессе повседневной предпринимательской деятельности, а также нормативная правовая база принятая в Российской Федерации и Европейском Союзе.

Предметом исследования являются нормы права о защите персональных данных и обработки информации, практика их применения. Теоретические положения о применимости информационных систем для работы с персональными данными, а также нормы классифицирующие

персональные данные и регламентирующие правила их технической обработки.

Цель исследования состоит в анализе нормативно-правовой базы, регулирующей вопросы защиты персональных данных клиентов субъектов предпринимательской деятельности и разработке предложений по повышению эффективности правового механизма защиты данного вида конфиденциальной информации.

Задачами исследования является:

- изучение правовых норм связанных с защитой персональных данных клиентов предпринимателей;

- выявление нормативных правовых рисков при работе с конфиденциальной информацией, которой являются персональные данные физических лиц.

- проведение оценки судебной практик сложившейся на момент подготовке работы по спорам связанным с использованием персональных данных в предпринимательской деятельности;

- формирование рекомендации по гармонизации законодательной базы.

Методологическую основу выпускной квалификационной работы составили следующие научные методы: диалектический, синергетический, системный, исторический, метод анализа и синтеза, сравнительно-правовой, формально-логический, формально-юридический, методы аналогии и моделирования.

Теоретическая основа исследования опирается на работы сделанные в обобщении правовых отношений в информационной сфере авторами: М.А. Лапиной, И.Л. Бачило, И.Ю. Богдановской, И.М. Рассоловым, В.М. Боер, О.А. Городовым, А.К. Жаровой, Н.Н. Ковалевой, В.Н. Лопатиным, А.В. Минбалеевым, А.А. Тедеевым, В.Н. Монаховым, А.А. Стрельцовым, А.В. Морозовым, В.Б. Наумовым, Т.А. Поляковой, А.А. Фатьяновым, И.Л. Петрухиным, О.Ю. Рыбаковым, Э.В. Талапиной, С.Е. Чанновым, Г.Г. Шинкарецкой, и другими учеными.

Ученые: В.Н. Верютина, Е.К. Волчинской, М.А. Вус, Р.Б. Ситдикова, А.А. Дозорцева, А.С. Коломиец, Л.К. Терещенко, О.С. Макарова, А.В. Минбалеева, А.А. Опалевой, Ю.С. Пилипенко, Т.А. Поляковой, Р.В. Северина, И.В. Смольковой, А.А. Фатьянова, М.А. Федотова, Е.Н. Яковца в основном сконцентрировались на разрешении юридических проблем возникающих при работе с конференциальной информацией [104].

Новизна магистерского исследования заключается в комплексном исследовании теоретических и практических проблем связанных с использований персональных данных клиентов субъектами предпринимательства в сфере электронной торговли субъектов малого и среднего бизнеса.

Практическая значимость исследования обусловлена тем, что обработка персональных данных клиентов, как бизнес процесс, используется всеми предпринимателями без исключения. Закон о защите персональных данных является относительно новым и практика того как нужно обрабатывать персональные данные клиентов в соответствии с его требованиями не учитывает многими субъектами предпринимательского права.

Эмпирическая база исследования: международные акты, законы и подзаконные акты, акты судебных органов, монографические работы правового, исторического характера, материалы научных конференций.

В соответствии с поставленной целью и задачами выпускная квалификационная работа состоит из введения, трех глав, заключения, библиографического списка.

Глава 1. Общая характеристика персональных данных клиентов

1.1. Становление и развитие законодательства о персональных данных

Вопросом обеспечения особого правового режима конфиденциальной информации уделялось внимания в источниках права государственных образования еще до нашей эры. В конце IV - начале III тысячелетия до нашей эры за измену и разглашение государственной тайны в Древнем Египте устанавливалась смертная казнь [21]. В этой же время на другой стороне средиземного моря в Древнем Риме существовали правовые нормы об охране тайны торговых книг [21], а если кто то принуждал чужого раба выдать тайны своего хозяина, то наказанием за это был штраф [7].

При этом древнерусские источники указываются, что на Руси понятие «тайна» изначально отсутствовало и за счет этого правовое свойство этого термина отличалось от того, что мы видим в законах Древнего Рима [53]. С точки зрения гносеологического происхождения термина он восходит к слову «верность» и несет в себе нравственный и этический базис. Последующее развитее этого понятие сводилось к сокрытию информации прежде всего связанным с деятельностью государственных органов, таких как появившиеся в XV-XVП в.в. Приказы (тайных дел, разрядного, посольского и др.)» [17].

В европейской правовой практике законодательное понятие о персональных данных начало появляться в 30-х года XX века. Так в конституционных нормах закрепление диапозитива о защите информации личного и семейного характера произошло в 1937 году, в 1944 году это произошло в Ирландии, в Исландии подобная норма появилась в 1947 г. Это не полный перечень конституционных новел того времени. В 1936 года идя в ногу с веяниями европейского законотворчества в СССР в конституционно

правовом поле фиксируется понятие неприкосновенность жилища, охрана тайны переписки, голосования и был использован термин «тайна» [33].

Начавшее в довоенное время тенденции защиты личностного пространства граждан естественным образом прервались на период второй мировой войны и послевоенного восстановления. Хотя по хронологии принятие схожих правовых дефиниций в разных странах важность защиты личности находила отклик во все большем количестве стран [5]. Толчком к началу систематических юридическо-правых исследований в этой области является внедрение автоматизированных систем обработки данных и первых программ машинного анализу. Считается, что старт интереса приходится на 60-70-е гг., XX века. И несмотря на раннее введение конституциональных норм именно в это время начинают формироваться национальные законодательства в области защиты персональных данных.

Правовой основой для старта изменения национальных законов стало принятие Всеобщей декларации прав человека [15], провозглашенное Генеральной Ассамблеей ООН в 1948 г. В статье 12 которой было юридически закреплено, что «никто не может подвергаться произвольному вмешательству в личную и семейную жизнь лица посягательством на его честь и репутацию». Это явно является достижением или следствием процессов происходивших в период второй мировой войны.

На основе положений Всеобщей деклараций прав человека были разработаны международно-правовые документы Евросоюза. В 04.12.1950 года была принята Европейская конвенция о защите прав человека и основных свобод.[27]. Это послужила толчком к ревизии национальных законодательства Европейских стран на приведение их в соответствии с это конвенцией и введении механизма защиты персональных данных, вплоть до введения института уполномоченных по защите персональных данных [1], [2].

Пости через двадцать лет положения Венской декларации были уточнены в направлении защиты персональных данных за счет разработки в

рамках ООН Международного пакта о гражданских и политических правах от 19.12.1966 года [56], статья 17 которого гласит, что никто не может подвергнуться произвольному вмешательству в его личную жизнь [59]. Каждый человек имеет право на защиту от такого вмешательства или таких посягательств. Принятие этого закона вывело защиту личных прав и свобод над уровнем национальных конституций на уровень международных правовых актов [54].

Первый в мире специальный Закон о защите персональных данных был принят германской землей Гессен в 1970г [29].

В 1981 г. в рамках законотворческой инициативы Советом Европы была принята Конвенция о защите физических лиц при автоматизированной обработке персональных данных. А также утвержден Дополнительный протокол к данной Конвенции, посвященный созданию наблюдательных органов за соблюдением закона о защите персональных данных и их трансграничной передачи.

24.10.1995 года выходит в свет Директива 95/46/ЕС Европейского парламента и Совета Европейского союза о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных

24.12.1997 постановляется Директива 97/66/ЕС касающаяся использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций.

19.02.1999 г. выпускаются Рекомендации Комитета министров государствам - членам Совета Европы по защите неприкосновенности частной жизни в Интернете.

В 2015 году Совет Европы выпускает рекомендации [112] с изложением принципов, которым должны следовать страны союзы в своих национальных законодательствах при формировании принципов обработки персональных данных наёмных работников и кандидатов на рабочие места, - например, в отношении данных о состоянии здоровья или мониторинга использования

средств связи на рабочем месте. Рекомендации нацелены на решение проблем с обеспечением неприкосновенности частной жизни, возникающих в результате использования новых информационно-коммуникационных технологий [110-111].

23.09.1980 года принята Директива Организации по экономическому сотрудничеству и развитию (ОЭСР) «О защите неприкосновенности частной жизни и международных обменах персональными данными». Она была предназначена урегулировать вопрос неприкосновенности частной жизни в рамках международного обмена персональными данными. Страны входящие в организацию: Австрия, Канада, Дания, Франция, Германия, Норвегия, Швеция и др., разработали Основные положения директивы задача которых была унификация национальных законов о неприкосновенности частной жизни, обеспечению соблюдения соответствующих прав человека [36].

В связи с развитием интернет услуг и потребностей в деловой передачи данных идет и формирование законодательства и увеличение количества правовых актов в сфере защиты личных данных граждан и неприкосновенности частной жизни. Подвергается регуляторному контроля и формированию правил в сфере сбора обмена и обработки персональных данных граждан в рамках европейского правового поля. Можно отметить, что направление законотворчества идет в двух векторах развития, часть законодателей сосредотачивает свое внимание не регулированию компьютерных сетей и машинных методов обработки информации. Второе направление, это создание общей нормативной базы с универсальными императивами влияющий на все возможные формы работы с личной информацией гражданина.

Представленная выше хронология нормотворческой деятельности стан Евросоюза по формированию единых правил по работе с персональными данными указывает на планомерную многолетнюю работу по унификации гармонизацию законодательства в этой сфере. Стартовав в 1948 году, оно значительно опередило российскую нормотворческую практику. Это

сказалось как на полноте норма права, так и на их качестве. В СССР только в 1977 году конституционно закрепила диапозитив о конфиденциальности телефонных и телеграфных переговоров, права нормы о неприкосновенности личности, жилья, тайны переписки были ведены почти на 30 лет раньше, но их практическое применение в жизни граждан было нулевым. В целом, вопрос личной свободы граждан в Советском Союзе не находился в фокусе правоприменительной практики. Общий коллективистический посыл коммунистической идеологии приводил к массовому ограничению личных прав граждан [32].

Большое количество норм, посвящённых защите личности, в рамках Европейского права подверглась ревизии и обобщению в рамках конвенции Совета Европы о защите физических лиц при автоматизированной обработкой персональных данных [105] принятая 28.01.1981 года в Страсбурге. Диспозитивные нормы установленные в нем носят основополагающий характер в области защиты персональных данных на сегодняшний момент. Установленная данной Конвенцией цель – уважения прав и свобод каждого человека независимо от его гражданства или места жительства и в особенности его права на неприкосновенность личной сферы в связи с автоматической обработкой, касающихся его персональных данных [57].

01.10.1985 года данная Конвенция вступила в силу и сегодня ее подписало 47 государств Европы, а ратифицировало 46 (кроме Турции).

08.11.2001 г. Конвенция №108 «о защите физических лиц при автоматизированной обработкой персональных данных» была подписана от имени Российской Федерации, и 19.12.2005 произошла ее ратификация Федеральным законом № 160-ФЗ. При подписании были допущены определённые оговорки затрагивающие особенности российского законодательства, но в целом ратификация Конвенции дала серьезный импульс к обеспечению защиты персональных данных граждан РФ и к развитию национального законодательства в этой сфере [76].

До при рассмотрении формирования законодательной базы Российской федерации нужно отталкиваться от 22.11.1991 года когда верховным советом РСФСР была принята «Декларации прав и свобод человека». Она ознаменовала новый, постсоветский период развития гражданских свобод России. Обратим внимание на содержание статьи 9 которая хоть и утверждает неприкосновенность частной жизни [78], тайну переписки и телефонных переговоров, оговаривает ее ограничение путем вынесение соответствующего судебного решения. Важность принятия данной Декларации определяется, тем, что ее нормы о неприкосновенности частной жизни в 1993 году приняли конституциональный характер.

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» [80] [82]. Статья 24 Конституции определила запрет на «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия» [95-96].

В этот же период, к российской нормативной базе простоит формирование термина «персональные данные», который уже нежели используемый в Декларации прав и свобод человека [6] [97] и Конституции термин «частная жизнь» и «личная и семейная тайна». Он был введен федеральным законом от 20.02.1995 №24 «Об информации, информатизации и защите информации» в нем водилось понятие «персональные данные» как информация о гражданине, а также статьей 11 они относились к категории «конфиденциальной информации», а также определялись правовые свойства данной информации.

Однако в данном нормативном акте термин «персональные данные» задавался очень расплывчато и к ним можно было отнести «сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие

идентифицировать его личность» [36]. Это формулировка порождала слишком широкое понимание области защищаемой информации. Указ Президента РФ №188 от 06.03.1997 года сделал изъятие из формулировки исключив из нее «сведения, подлежащие распространению в средствах массовой информации в установленных федеральными законами случаях» [83] [98]. Однако, более точного формулирования, что нужно понимать под защищаемыми законом сведениями этими нормативными актами сделано не было.

27.07.2006 г. было принято два закона дополняющих один другой. Это №149-ФЗ «Об информации, информационных технологиях и о защите информации» и №152-ФЗ «О персональных данных» [38] [99]. В последнем уже системно и детально разобрано не только особенности работы с персональным данными, но и особенности работы с данными правовыми объектами. Оба закона приняты в свете подписания в 205 году Россией Конвенции №108 «о защите физических лиц при автоматизированной обработкой персональных данных» и принятых на себя обязательствах по приведению национального законодательства в соответствие с ее положениями.

Но законотворчество не стоит на месте и как в Европе принимаются новые положения регулирующие вопросы правового характера возникающие при работы в сети Интернет. Примером могут служить Директив 95/46/ЕС и 97/66/ЕС, в которых прописан регламент и производится соотнесение юридических диспозиций и технических требований к защите информации. Так и российские законодатели практически ежегодно уточняют нормативные акты, касающиеся требований к защите персональных данных.

Обращает на себя внимание изменение и даже расширение понимания об объекте защиты термина «персональные данные» если ранее это были исключительно анкетные сведения физического лица: ФИО, данные о дате и месте рождения, адрес проживания и так далее [39], [46]. То в текущей редакции Федерального Закона №152 [100], к персональным данным

относится и косвенная информация о физическом лице. Таким образом мы видим расширение понятийной общности данного правового термина. Более того этот термин применяется в форме открытой конструкции, когда законодатель не ограничивает его перечислением объектов. Основным критерием того, что какая либо информация относиться к области персональных данных является ее со относимость с субъектом – физическим лицом и возможность его по нему идентифицировать [47].

В правоприменительной практике подобные конструкции сводятся к возможности постоянного расширения списка сведений, относящихся к конфиденциальной информации, что дает возможность органам осуществляющим контроль в сфере надзора в сфере связи, информационных технологий и массовых коммуникаций предъявлять расширяющийся список требований к операторам информационных потоков, к информационным ресурсам и сервисам на предмет неправомерного использования персональных данных [50]. Не редки случае, когда одни данные сначала не относились к персональным и соответственно не требовали специального обращения, а через какой то промежуток времени становились таковыми, например из-за изменения внутренних инструкций или установок контролирующих организаций [48]. Подобная ситуация несет либо непрогнозируемые риски для предпринимателей в бизнес модели которых входит работа с данными неограниченного круга физических лиц, либо вынуждает организации перестраховывается за счет чего отказывать от возможных сервисов по работе с личными данными граждан и возможно лишать себя потенциальной прибыли.

При этом есть и обратная сторона проблемы, когда интернет сервисы или их части злоупотребляют возможностью собирать персональную информацию. Собирают ее преднамеренно без получения явного разрешения граждан, либо же получают разрешение на использование в форме отказа от ответственности или же за счет нахождения в юрисдикции не ратифицирующей Конвенцию №108 или аналогичные международные

правовые документы. Подобные злоупотребления приводят к необходимости национальных регуляторов ужесточать требования к работе с персональными данными, ужесточать правила трансграничной передачи информации или введения запрета на оный, а также введение ограничений на места хранения и о обработки информации.

Отдельной проблемой является сертификации и унификация технологических платформ по работе с персональным данными граждан, форм передачи таких данных по сетям и защита подобной информации от несанкционированного доступа или копирования. Эта проблема носит как технологический, так и юридический характер, но крайним в этих коллизиях становиться субъект предпринимательского права так как именно он отвечает со сохранность обрабатываемых персональных по нормам права.

Исторический анализ показывает постоянное развитие законодательства о персональных данных физического лица ускорившееся из-за проникновения сетевых технологий в личную и общественную жизнь. На сегодняшний день оно еще не стало отдельной отраслью права, но если рассматривать его как составную часть информационного права, то видно, что оно оказывается связующей область между информационным пространством и физическим пространством субъекта права. Это требует инкорпорации существующих правовых норм и консолидации ее в совокупности с законами о защите и обмене информацией.

1.2 Правовые основы защиты персональных данных

Правовое регулирование обработки персональных данных регулируется Федеральным законом «О персональных данных» от 27 июля 2006 года №152-ФЗ. Он действует не только на привычные в современном документообороте компьютерные способы обработки и хранения данных, главное условие, что подобные средства позволяют осуществлять поиск по массивам данных, предоставлять к ним доступ в том или ином виде [70]. При

этом закон действует и на классические или даже устаревшие способы хранения информации, такие как картотеки, учетные книги и другие физические носители.

Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных» устанавливает:

- Основные принципы понятия, связанные с тематикой обработки персональных данных;
- Обязанности оператора персональных данных;
-Условия обработки персональных данных;
- Виды ответственности за нарушения установленные Законом № 152-ФЗ;
- Права субъекта персональных данных;
- Государственные органы, осуществляющие контроль и надзор за соблюдением требований, установленных ФЗ № 152.

Не попадают под сферу регулирования закона 152-ФЗ следующие действия:

- Обработка персональных данных, содержащие сведения, относящиеся, к государственной тайне;
- Действия по организации архивов, соответствующих сфере регуляции законодательства об архивном деле в РФ;
- Обработка и хранение персональных данных физическими лицами для личных и семейных нужд при условии, что такая обработка не нарушает права владельца персональных данных;
- Персональные данные, относящиеся к деятельности судов, предоставленные в порядке судебного делопроизводства.

Персональные данные являются очень широким понятием. Под них можно отнести практически любую информацию, которая тем или иным образом затрагивает субъекта персональных данных. Таким образом закон старается максимально защитить физическое лицо, сведения о котором могут любым способом его идентифицировать, например: фамилия имя отчество,

данные о дате и месте рождения, адрес прописки и места жительства, сведения об образовании и семейном положении, а также о профессиональной деятельности и финансовом положении. Причем приведенный список не является исчерпывающи под него подает и биография, личные и деловые качества, сведения о состоянии здоровья и т.п.

Не все их них используются в предпринимательской деятельности, но в камках данного определения достаточным является соотнесения ФИО с номером телефона, электронным адресом и адресом проживания, чтобы используемые сведения попадали под определение «персональных данных».

Причем если затронут термин «обработка персональных данных», то под них попадает любая операция с ними или совокупность действий: сбор, хранение, предоставление, использование, удаления.

Формализованный подход показывает, что защита персональных данных не прописана дословно в Конституции РФ и не является прямым конституционным правом, нет статьи в который было бы прописано «право на защиту персональных данных». Но если рассматривать расширено то что сказано в статье 23 Конституции Российской Федерации, а именно «неприкосновенность частной жизни, личную и семейную тайную» в совокупности со статьей 24 в части того что «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются», то можно сделать вывод о соответствии права на защиту персональных данных физического лица Конституционным нормам.

При этом в законодательстве отсутствует четкое определение, что нужно считать личной и семейной тайной и где проходит грань между ними и понятием «персональные данные», которые в общем смысле входят в понятие «информации о частной жизни» так как определяют и идентифицируют субъекта права и соотносит сведения с его личностью и /или местом проживания. Но, с другой стороны, без их сбора использования и передачи третьим лицам невозможно существование субъекта права как социальной единицы общества.

Российская правовая доктрина рассматривает частную жизнь гражданина не в широком понимании, когда в нее входит максимально широкий спектр понятий связанных с жизнью современного человека, а более узкое понимание интимных, бытовых и семейных отношений возникающих в семейном кругу. Данный вывод 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» [77]

Юрченко И.А. полагает, что дифференциация личной и семейной тайны происходит через взаимосвязь с интересами одного человека или семьи в широком смысле [3]. Конкретизируя содержание понятия «личная тайна», Бродская И.А. включает в него вопросы индивидуальности субъекта права, его прошлого, социального обособления человека, а в семейную - семейных взаимоотношений и взаимодействий, а также тайну усыновления [11]. В семейную тайну исследователи также нередко включают конституционно закрепленное процессуальное право не свидетельствовать против себя, близких родственников и своего супруга то есть свидетельскую тайну [24].

В настоящее время проблема грамотной с точки зрения права обработки персональных данных находится в фокусе внимания абсолютно любого предпринимателя, вне зависимости от сферы деятельности. Любая организация так или иначе обрабатывает персональные данные, как сотрудников, так и клиентов. Боле того необходимо соблюдения корректного режима передачи персональных данных между субъектами предпринимательства без потери режима конфиденциальности и со соблюдением прав субъектов персональных данных.

Как только предприниматель начинает свою деятельность он становиться оператором персональных данных, так как без хранения или

использования их невозможно ни заключение трудовых соглашений с сотрудниками, ни заключение договоров на выполнение услуг или поставку товаров физическим лицам. Соответственно, у организации или индивидуального предпринимателя возникает обязанность по защите указанной информации, одновременно он становится поднадзорным государственным контролирующим органам.

Системность правовых конструкций является основой правовой науки и задачей правоведов является определить совокупность свойств объекта права, выявить его самоценность для системы определить место и провести систематизацию правого понятия синтезировав для него место в системе правовых норм.

Институт персональных данных, правовое явление, появившееся в отечественной правовой системе относительно недавно, но при этом обладающее свойством быстрого видоизменении с появлением новых информационных систем и требований. В связи с этим его место в правовой семье подлежит осознанию и научной правовой проработки. Это является требованием времени так как объем правовых коллизий разрешение которой в повседневном режиме требуется для субъектов предпринимательской деятельности ставит перед юридической наукой насущные задачи требующие разрешения. Это дает толчок к интересу со стороны юридической науки на различны ее ступенях и генерирует возникновение исследовательских работ в этой сфере направленных как на изучение свойств предмета интереса, так и на кодификацию имеющихся на сегодняшний момент правовых конструкций [44-45]

Но с точки практического использования предприниматели, в основной своей массе, не придают значение работы с персональными данными как с объектами имеющие граждаскоправовую природу. В основном тематика защиты персональных данных рассматривается как сугубо техническая задача цель которой, не допустить их утечку, несанкционированное завладение или доступ к базе данных. То есть персональные данные

рассматриваются как информационно-физические объекты, а не как объекты права. Это приводит к тому, что предприниматель сводит свой интерес к персональным данных в техническую область. При этом сама «защита персональных данных - безопасность персональных данных субъекта, который дает свои данные какому-либо государственному органу или частной организации, то есть защита именно его прав» [19].

Несмотря на общий подход и расширенные трактования того, что нужно считать персональными данными закон не дает на это исчерпывающий ответ. Персональные данные, которые еще десять лет назад считались исчерпывающими для получения информации о защищаемой личности, например, ФИО, паспортные данные, адрес проживания, место и дата рождения сегодня и так далее сегодня не являются ограниченными этим списком. Возникновения новых технических средств получения информации о личности, например, биометрические данные, фотоизображения, геолокация смартфона физического лица или цифровой след, оставляемый пользователем расширительно попадает под понятие персональных данных так как позволяет идентифицировать личность, его действия или семейный круг или круг общения. Все это является защищаемой информацией с точки зрения закона так как источником его возникновения является физическое лицо. Более того их использование позволяют идентифицировать личность субъекта и /или род его деятельности или занятий. Строго исходя из диспозитивных позиций закона о персональных данных подобные цифровые следы также должны относиться к конфиденциальной информации.

В связи с вышеизложенным можно сделать вывод в том, что состав персональных данных окончательно не сформирован. Он уточняется и расширяется по мере появления новых технически-информационных способов идентификации субъекта персональных данных. Это делает невозможным составить закон так чтобы списочно ограничить их состав, что проводит к ведению обобщенных формулировок в нормативные акты.

Глава 2 Обработка персональных данных клиентов

2.1 Проблематика работы с персональными данными в предпринимательской практике

Рассмотрим правовой базис самого понятия «конфиденциа́льность» происходит от латинского слова -confidentia, что в переводе означает доверие. Т.е. если объект взаимоотношений призывает сохранять конфиденциальность это означает, что он предполагает, что второй субъект взаимоотношений должен предотвращать возможность того, чтобы полученная им информация был разглашена или о ней узнали какие либо другие лица.

Отсюда следует расширение этого понятия на информацию и закрепление понятия конфиденциальная информация [79], т.е. информация, являющаяся конфиденциальной, то есть «доверительной, не подлежащей огласке, секретной». В общих источниках ставиться равнозначное соответствие между понятиями «тайна», «секрет» и «конфиденциальная информация». П происхождению понятие «секрет», заимствовано из французского языка secret означает — «тайна». В толковом словаре В.И.Даля приведены аналогичные по смыслу значения: «конфиденциальная» — «откровенная, по особой доверенности, неоглашаемая, задушевная»; «тайна» — «кто чего не знает, то для него тайна, все сокрытое, неизвестное, неведомое». Исходя из определений понятия конфиденциальная информация, тайна, секрет являются равнозначными [2].

В юридической литературе понятие конфиденциальность является свойство определяющий понятие коммерческой тайны. Коммерческая тайна является одним из объектов гражданских прав, предусмотренных Гражданский Кодексом РФ, с особым режимом защиты.

Законодательное определение термина конфиденциальная информация можно найти в водной части федерального закона №149-ФЗ «Об

информации, информационных технологиях и о защите информации», от 27.07.2006 г. п.7 ст. 2 - «конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя»;

Таким образом вводится принцип конфиденциальности информации как правило о неразглашении, но это принцип ограничивается не ко все информации, а некой «определенной информации», к которой лицо получило доступ.

В п.2 ст.9 уточняется что обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами. Которые в свою очередь ограничивают доступ к информациями общими признаком которых является объединение термином «тайна» и соответствующим образом зафиксированном в видео законов о «Банковской тайне», «Государственной тайне», Коммерческой тайне». Если мы выделим общие признаки объединяющие это информацию то окажется, что она должна быть специальным образом обозначена для пользователя как информация содержащая признак тайны. При этому субъекты, владеющие этой информацией и субъекты, которым предоставлено право пользования ей должны пройти определенную юридически значимую процедуру получения этой информации и ограничения допуска к этой информации других лиц. Такие как, реестры, маркировка, ограничения количества копий, и мест, где можно знакомиться с этой информацией. Таким образом, информация юридически маркируемая как «тайна» требует значительных затрат и определённый действий от пользователя для того, чтобы оставаться в рамках законно определённой конфиденциальной информацией. Из-за этого в предпринимательской деятельности конфиденциальная информация ограниченная термином «тайна» практически не используется так как требует больших затрат на поддержание признака конфиденциальности информации.

Уже в этой диспозиции содержится наложение юридических терминов так как все они подпадают под общее определений сведений доступ к котором должен быть ограничен поскольку они носят необщеизвестный характер и в случае широкого распространена могут нанести ущерб разного рода, материальный, правовой, физический, объектам / субъектам сведения о которых они несут. Именно это связано с наложением на них особого правого статуса.

Но не обязательно информация должна обладать определёнными признаком конфиденциальности как то, печать или внесение в реестр, для того чтобы относиться категории тайны. Так, большой спектр профессий и сведений, которые используются в профессиональной деятельности подпадают под категорию «профессиональной тайны». К подобной деятельности относиться адвокатская, нотариальная, страховая, врачебная и т.д. деятельность. Перечень подобных профессий хотя и ограничен, но при этом достаточно широк, для того чтобы признак конфиденциальности информации стали применим практически в любой сфере жизни.

Наверное самые широкое понимание термина конфиденциальности информации можно усмотреть в уголовном кодексе, где в ч.1 ст. 138УК предусматривается ответственность за «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан». причем под термином «иные сообщения» в статье 138УК РФ [25] следует понимать сообщения граждан, передаваемые по сетям электрической связи, например СМС- и ММС-сообщения, факсимильные сообщения, передаваемые посредством сети "Интернет" мгновенные сообщения, электронные письма, видеозвонки, а также сообщения, пересылаемые иным способом. Даже в этом разъяснении, данном в Пленум Верховного Суда Российской Федерации в постановлении №46 от 25.12.2018 г. «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 уголовного кодекса

российской федерации)» [63], не обошлось без формулировки «иным способом» расширяющий применимость закона на еще не используемые способы передачи информации.

Опять же если попытаться выявить общие признаки конфиденциальной информации связанной с профессиональной деятельностью, то вся она хоть и не требует маркировки, как это было связано для случая законодательно установленной «тайной информацией», но происходит от одного источника – гражданина и связано с его личностью напрямую. Будь то здоровье, переписка, или же доверительные отношение с адвокатом или поверенным.

Более того федеральный закон N 152-ФЗ от 27.07.2006 года «О персональных данных» постоянно актуализируется и дополняется, защищая практически все сферы частной жизни.

Для сферы предпринимательской деятельности защита персональной информации не кодифицирована и разрознена. С одной стороны есть закон о «Коммерческой тайте», но от требует специальной маркировки информации, с другой стороны есть ст.1465 ГК РФ допускающая очень широкие формулировки и типы объектов, защищаемых правом [4]. При этом во время предпринимательской деятельности юридическому лицу приходится постоянно работать с объектами права защищаемыми законодательными актами о персональных данных, а также отвечать за их сохранность. При законодательном равенстве юридического и физического лица субъект предпринимательства, в этом случае, находится в неравных условиях по отношению в физическому лицу. На особом положении, с точки зрения концентрации персональных данных, находятся и предприятия сферы образования, дошкольного воспитания и высшей школы. Они вынуждены работать с целым спектром персональных данных на детей их родителей, что накладывает на них большую ответственность как социальную, так и правовую [75].

В условиях каждодневной предпринимательской деятельности сотрудники предприятия работают с большим количеством информации

которая по своим признакам может не относиться к тайной но имеет основные признаки конфиденциальной, как то список контактов, предварительные договоренности с контрагентами, планы закупок и т.д. И то у предприятия как у юридического лица возникают проблемы защиты этой информации от посягательства других лиц, поскольку утечка внутренних сведений может негативно сказаться на финансовой деятельности организации и нанести ей ущерб при этом возместить ущерб, даже если будет доказан факт не предумышленной передачи сведений. С одной стороны, мешает отсутствие грифа коммерческой тайны, который не накладывается на весь информационный поток так как просто невозможно все засекретить [68]. С другой стороны, возникший ущерб трудно доказуемый так как нельзя, например, объявить ущербом не выигранный аукцион, который контрагенты переиграли за счет того, что узнали цену предложенного контракта и выставили меньший порог стоимости, ведь участие в аукционе не гарантирует его выигрыш. Это одна сторона проблемы использования и регулирования конфиденциальной информации.

Но есть и другая сторона работы с конфиденциальной информацией, не связанная со злым умыслом или неосторожностью участников предпринимательской деятельности. Это вопрос оформления и передачи информации подпадающие под закон «О персональных данных». Он может возникать при попытках обращения, например с клиентской базой, данных пассажиров или информации о вкладчиках. В сложившейся практике частное лицо дает свое согласие на хранение и обработку своих данных юридическому лицу с которым оно вступает в какие-либо отношения. Передача этого права осуществляется либо подписью согласия, либо методом присоединения к соглашению, последнее больше характерно для электронных сервисов. Таким образом субъект предпринимательского права получает законные основания пользоваться этими данными и даже просто хранить их. Вопросы возникают в случае необходимости передать это право другому юридическому лицу, например, в случае реорганизации, ведь

формально согласие на работы со своими персональными данными гражданин давал одному юридическому лицу, а после реорганизации пользоваться ими будет другое. Причем, например, отказ от использования существующих данных может означать потерю бизнеса новым юридическим лицом и из-за этого оно вынуждена использовать базу, не имея на это законных оснований [69]. Это в свою очередь несет в себе риски судебного преследования и возможных финансовых потерь.

Еще одна проблема возникает при передачи имеющихся сведений, защищённых признаком конфиденциальности, на аутсорсинг. Она также не связана со злым умыслом со стороны кого либо. Самый простой пример неоднозначной, с точки зрения закона ситуации, это передача сведений граждан для выполнения работ стороннему юридическому лицу. Распространенный случай — это проведение адресной рассылки клиентам. Получается, что лицо получившее согласие на работу с конфиденциальными данными не может нанять третье лицо для выполнения работ, так как ему придется передать персональные данные, а для этого нужно получить согласия от владельца персональных данных. Эта ситуация противоречит логике развития предпринимательства, когда неспецифические задачи отдается на выполнение тем, кто это делает лучше и дешевле.

Немногим проще передача прав на конфиденциальную информацию решается в сфере электронной коммерции и коммуникаций когда для передачи прав требуется только «поставить галочку». В случае же решение ситуации в «офлайн» требуется заново подписывать согласие на обработку и хранение персональных данных.

Отдельной проблемой может стоять законная трансграничная передача персональных данных, например, к сфере туризма или гостиничной сфере особенно со странами не подписавшие Конвенцию №108 «о защите физических лиц при автоматизированной обработкой персональных данных» [81]. Это определяет необходимость кодификации правовых норм связанных с оборотом персональных данных и информационной работе с ними.

2.2 Понятие и общие требования при обработке персональных данных

Обработка персональных данных является рутинной операцией в любой предпринимательской деятельности. В сложившейся практике ей не уделяется особого внимания со стороны юридического отдела предприятия, хотя именно это процесс является регламентированным на законодательном уровне. В общих чертах вопрос обработки персональных данных формулируется в статье 5 федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» [90]. Диспозитивные позиции данной нормы сложно сочетаются с реальностями и потребностями предпринимательской деятельности суть, которой в получении прибыли от совершаемой деятельности. Причем для многих предпринимателей их клиентская база является основным активом для работы и если для предприятий работающих в сегменте B2B («Business to business» — рус. «бизнес для бизнеса») нет ни каких ограничений в обработке, хранении и использовании накопленного багажа контактов, то для предприятий из области B2C (Business-to-consumer, рус. «бизнес для потребителя») закон накладывает большое количество ограничений. Рассмотрим нормы по работе с персональными данными в приложении к коммерческой деятельности предпринимателя работающего в сфере услуг для физических лиц.

Пункт 1 статьи 5 федерального закона №152-ФЗ «О персональных данных» говорит о том, что «Обработка персональных данных должна осуществляться на законной и справедливой основе». Оценка этого пункта сразу же вызывает вопросы в трактовке положений, если часть касаемая «законной основе» можно трактовать как обратку в соответствие с законном или не обратку информации для совершения противозаконных действий, то тезис о «справедливой основе» данной обработки вызывает вопросы в том, что можно считать справедливым или несправедливым при обработке персональных данных и к кому должен относится данный принцип. По

логике закона он должен быть отнесен к субъекту персональных данных, но будет ли является справедливым обработка персональных данных для формирования лучшего рекламного предложения для данного субъекта или же это будет злоупотреблением принципа законности и справедливости не понятно. При этом непонятно как относиться к обработки персональных данных внутри коммерческого предприятия основная цель которого является получение прибыли, поскольку формирования предложения на основе цифрового следа физического лица для получения коммерческого эффекта предпринимателем является действием нацеленным на получение прибыли для коммерсанта, а не для объекта предложения. Будет ли в таком случае обработка носить принцип справедливости не совсем понятно.

Пункт 2 статьи 5 федерального закона №152-ФЗ «О персональных данных» гласит о том, что «Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных». Эта норма закона, с одной стороны, носит ограничивающий характер относительно первой части данной статьи, и накладывает на субъекта собирающего персональные данные императива об установки целей сбора данных. С другой стороны ее практически невозможно соблюсти при приложении к предпринимательской деятельности. Если в случае с работой бюджетных структур императив установки целей носит логичный характер, например, медицинское учреждение собирает данные для оказания медицинских услуг и субъект персональных данных передавая их в регистратуре четко понимает цель и ограничения их предоставления, то в случае взаимодействиям с предпринимателем цель становиться либо очень конкретной либо очень размытой. Например, если пользователь предает свои данные для осуществления доставки товара, то отправка рекламной корреспонденции от предпринимателя по этому же адресу будет, строго говоря, нарушением закона так как предприниматель повторно использовал персональные данные

для других целей. Подобное логическое построение можно провести и для пары товар – услуга, товар - реклама, услуга – реклама. Для юридической защиты предпринимательской деятельности подобная неоднозначность закона требует получения особого разрешения на использования персональных данных для разного вида коммерческой деятельности.

Аналогичные вопросы с точки зрения использования базы данных клиентов возникают применительно оценки пункт 3 статьи 5 федерального закона №152-ФЗ «О персональных данных» которая утверждает «не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой». Оставляя за скобками вопрос правовой передачи базы данных клиентов физических лиц, например, между подразделениями коммерческой структуры выделенными как обособленный юридические лица, возникают вопросы, что будет считаться совместимостью целей. Опять же может привести пример самых распространенных пар коммерческой деятельности обособленных подразделений товар – услуга, товар - реклама, услуга – реклама. Будет ли цель предоставления услуги, с точки зрения п.3 ст.5 совместима с целью продажи товаров.

Мы уже несколько раз обсуждали в процессе анализа положений закона цели обработки персональных данных и пытались их анализировать в отношении субъекта предпринимательской деятельности. Законодатель в рекомендация по составлению документов определяющих политику оператора так формулирует это понятие: «Цели обработки персональных данных могут происходить, в том числе, из анализа правовых актов, регламентирующих деятельность оператора, целей фактически осуществляемой оператором деятельности, а также деятельности, которая предусмотрена учредительными документами оператора, и конкретных бизнес-процессов оператора в конкретных информационных системах персональных данных (по структурным подразделениям оператора и их

процедурам в отношении определенных категорий субъектов персональных данных)».

Данное положение сформулировано с расчетом на операторов персональных данных, к которым можно было бы ошибочно отнести только телекоммуникационные компании, в пункте 3 статьи 5 федерального закона №152-ФЗ «О персональных данных» указывается что «оператор персональных данных (оператор) это государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными». Таким образом, наши оценки того, что любой предприниматель работающий на рынке продажи товаров или услуг физическим лицам становиться оператором персональных данных в тот момент когда он их получает от субъекта персональных данных являются верными. Например, телефон, ФИО, адрес доставки, паспортные данные и так далее. Соответственно если предприниматель хочет работать с персональными данными не только в момент оказания услуги, а в дальнейшем, например при разработке маркетинговых программ, то ему необходимо формулировать цели планируемой обработки и использования персональных данных, во внутренней документации юридического лица.

Вопрос вызывает также диспозитивные установки содержащиеся в пункте 5 статьи 5 федерального закона №152-ФЗ «О персональных данных» «Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки». То есть закон запрещает сбор сведений про запас, они должны быть собраны только в том объеме который нужен для выполнения обязательства предпринимателя перед физическим лицом.

При этом персональные данные являются практически бессрочной конфиденциальной информацией так как законом не установлена длительность ее защиты, напротив из смысла соотнесения этой информации с личностью получается, что она носит закрытый характер на протяжении всей жизни гражданина. Для того чтобы исключить возможность неконтролируемого накопления персональных данных пункте 7 статьи 5 федерального закона №152-ФЗ «О персональных данных» говорит, что «обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом». То есть оператор должен их уничтожить после того ка цели обработки были достигнуты. Опять же из данной нормы права нельзя однозначно установить срок, которой можно или нужно хранить персональные данные. Законодатель опять отсылает нас к целям их использования который, например, в случае предпринимателя, занимающегося доставкой, может быть доставка товара до потребителя. Строго исходя из норм права после того, как цель достигнута и товар доставлен персональные данные должны быть уничтожены, но это не соответствует сложившейся деловой практике. Соответственно для того, чтобы можно было защититься от возможных проверок контролирующих органов в документах организации должна быть прописана цель для чего персональные данные продолжают храниться у юридического лица, а также сроки этого хранения [101-103].

В качестве примера различного подхода формулирования целей обработки персональных данных можно привести выдержку из политики в отношении конфиденциальности персональных данных ООО «Вайлдберриз» интернет магазина https://www.wildberries.ru и ООО "Интернет Решения" интернет магазин https://www.ozon.ru/.

«Оператор собирает, обрабатывает и хранит персональные данные субъекта персональных данных в целях: Исполнения договора. При этом в

соответствии с п. 5 ч. 1 ст. 6 Федерального закона «О персональных данных» обработка персональных данных, необходимая для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем, осуществляется без согласия субъекта персональных данных» [57].

«Персональные данные Обществом обрабатываются в целях, но не ограничиваясь: обеспечения соблюдения законов Российской Федерации и иных нормативных правовых актов; для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем; регистрации и обслуживании аккаунта на сайте; реализации товаров и услуг; проведение конкурсов, розыгрышей, рекламных акций и опросов, выявления победителей, доставки призов; информирования о товарах, услугах и акциях; участия в программах лояльности; формирования отзывов на товары» [56].

Хорошо видно, что в первом варианте предприниматель в формулировании целей обработки данных ограничивается дефиницией исполнения договора. Во втором случае цели обработки персональных данных прописаны более широко и позволяют использовать персональные данные клиентов практически во всех возможных сферах предпринимательской деятельности и маркетинговой активности. Последнее предпочтительнее так как при возникновении запросов о правомерности использования персональных данных для тех или иных сервисов интернет магазин, всегда можно сослаться на соответствие данных действий сформулированным в положениях, целям в то время как в первом случае

возникает необходимость юридической оценке тезис «исполнение договора». В этом случае сразу возникает масса вопросов о соответствия действий оператора договорным отношениям. Так например, если интернет магазин руководствуясь первым вариантом целей начнет использовать персональные данные для рекламной или маркетинговой компании то это проблематично рассматривать как исполнение договора поставки, что делает правомерность подобного использования персональных данных спорным.

В практике формулирования целей сбора персональных данных можно встреть подобную формулировку «Целью обработки персональных данных является выполнения обязательств Оператора перед Пользователями в отношении использования Сайта и его сервисов» [58]. Пытаясь максимально широко представить цели обработки персональных данных и надеясь такой размытой формулировкой охватить наибольшее пространство возможных вариантов действий предприниматель создает юридические неопределённости которые в случае возникновения спорных ситуаций могут трактоваться не в пользу оператора персональных данных [8]. Даже при поверхностной правой оценке сформулированных целей возникает вопрос что можно считать сервисами сайта, а что нет.

Таким образом оценка норм действующего законодательства и примеры практической реализации формулирования целей обработки персональных данных физических лиц открывает перед нами неоднородность в использования норм права и показывает значимость четкого определение целей юридических документах предпринимателей [9]. Видно, что более широкие и неоднозначные формулировки положение об обработке персональных данных вызывают боле вопросов правового характера и могут отрицательно сказать на решении суда в случае возникновения правовых споров. Рекомендуется при составлении положения по обработке конфиденциальной информации субъекта предпринимательского права формулировать цели обработки персональных

данных таким образом, чтобы охватить все возможные сферы их использования.

2.3. Особенности сбора и накопления персональных данных клиентов

Из содержания предыдущего параграфа следует, что предприниматель начиная работать в сфере оказания услуг физическим лицам автоматически становится оператором персональных данных и обязан соблюдать требования предъявляемые в федерального закона №152-ФЗ «О персональных данных» и первое о чем предприниматель должен позаботиться это в получении согласия субъекта персональных данных на обработку персональных данных, как того требует пункт 1 части 1 статьи 6 федерального закона №152-ФЗ «О персональных данных»: «обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных». Способ получения этого согласия может быть сделан в прямой письменной форме или же получен путем присоединение субъекта персональных данных к действующим правилам в которых прописывается право юридического лица на обработку персональных данных. Из сказанного выше следует, что в этих же правилах должна быть в явном виде определена цель обработки персональных данных.

Для предпринимательской деятельности основным является случай отраженный в пункт 1 части 1 статьи 6 федерального закона №152-ФЗ «О персональных данных»: «обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем». Исходя из него заключение договорных отношений с субъектом права дает право на обработку его

персональных данных, но не снимает необходимости получения разрешение на подобную обработку от физического лица.

В случае если предприниматель выступает в качестве посредника или же привлекает контрагента для выполнение заключенного с физическим лицом договора оно вынуждено передать третьему лицу персональные данные для обработки причем третье лицо находится в более мягком правовом режиме так как в соответствии части 4 статьи 6 федерального закона №152-ФЗ «О персональных данных» «лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных». То есть оно для работы с персональными данными будет использовать получение изначально согласие, но при этом ответственность за обрабатываемые данные все равно будет нести юридическое лицо, изначально получившее согласие от субъекта персональных данных. Так, указывается в части 5 статьи 6 федерального закона №152-ФЗ «О персональных данных», «в случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор». Поэтому риск судебных издержек по претензиям субъекта персональных данных будет нести оператор, получивший согласие. Но в случае возникновения ответственности из-за неправомерного использования информации компанией он получает право возместить возможной ущерб у подрядчика за счет седлающей дефиниции части 5 статьи 6 федерального закона №152-ФЗ «О персональных данных» «Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором». Несмотря на то данная норма права следует из общих принципов гражданской правовой системы, законодатель отдельно оговорил эту возможность.

Самой главной правовой дефиницией и особенностей персональных данных является их конфиденциальность, то есть лицо, получившее их от

субъекта персональных данных не вправе передавать их третьих лицам «Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных», статья 7 федерального закона №152-ФЗ «О персональных данных». Исходя из этого возникает определенные правила работы с персональными данными одним из основополагающих направления является обеспечение их безопасности при обработке и хранении, поэтому оборудование, на котором производится обработка персональных данных и методы ее обработки требуют соблюдения определённого регламента.

При этом законодательство не требует именно автоматизированной обработки, возможно обрабатывать и без использования средств автоматизации, но трудно представить себе современную предпринимательскую деятельность без использования компьютеров. При этом нужно рассматривать вопрос неавтоматической обработки как часть общего процесса работы с персональными данными который все равно присутствует в любой организации. Причем требуется специальное информирование работников, о том, что они работы с персональными данными являющимися конфиденциальными, а также о методах и ограничениях подобной обработки. В методических рекомендациях требуется также знакомство персонала с нормативно-правовой базой по данной тематике, а также с локальными нормативными актами организации [50].

Однако на сегодняшний день внимание сосредоточено все-таки на компьютерных системах обработки данных. При этом «Оператор сам обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных

настоящим Федеральным законом» часть 1 статья 18.1 федерального закона №152-ФЗ «О персональных данных». То есть именно оператор может выбирать самостоятельно выбирать средства защиты информации, но при этом он обязан выполнять требования установленные Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [65]. Данный нормативный акт «устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных» при этом определение, что нужно считать информационными системами персональных данных дано с части 10 статьи 3 федерального закона №152-ФЗ «О персональных данных» и определяется как «совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств». Получается, что любая совокупность персональных данных, например, ФИО, телефон и адрес, находящейся в компьютере, который по определению позволяет их обрабатывать либо при помощи офисных приложений, либо при помощи систем бухгалтерского и складского учета, например, 1С уже подпадает под определение информационной системы и следовательно, попадает под действия выше упомянутого приказа. При этом в статье 5 Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 вводится перечень информационных систем которые подразделяются на:

- Информационная система специальных категорий персональных данных
- Информационная система биометрических персональных данных
- Информационная система общедоступных персональных данных
- Информационная система иных категорий персональных данных
- Информационная система персональных данных сотрудников оператора

Информационные системы клиентов субъектов предпринимательского права в основном можно отнести к категории системы иных категорий персональных данных и следовательно оператор такой системы обязан руководствоваться классификацией угроз установленных в приказе и учитывать их при построении программно-аппаратных комплексов обработки данных и при подготовке сотрудников. Также предприниматели вынуждены обрабатывать и информационные системы персональных данных сотрудников оператора, так как у него находятся персональные данные физических лиц с которыми заключены трудовые договора.

Меры которые оператор базы данных должен выполнять для работы с персональными данными изложены в Приказе N 21 от 18 февраля 2013 г. Федеральная Службы по Техническому и Экспортному Контролю «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [71]. Многие предприниматели думают, что требования этого приказа не относятся к ним так как они обрабатывают небольшое количество персональных данных, но на самом деле это не так. Закон не устанавливает минимальное количество персональных данных для которых применимы данные нормативы. Исходя из изложенных в них дефиниций для любого количества персональных данных оператор должен принять меря по обеспечению их безопасности. Согласно абзацу 2 статьи 1 Приказа N 21 от 18 февраля 2013 г. Федеральной Службы по Техническому и Экспортному Контролю «Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных».

Более того статья 2 этого же приказа возлагает на оператора ответственность за обработку персональных данных. Причем формулировка

звучит так «оператор или лицо, осуществляющее обработку персональных данных», то есть норма закона не дает возможность участнику предпринимательской деятельности завить, что оно не является оператором в силу каких либо обстоятельств. Фактическая обработка персональных данных уже само по себе накладывает на него обязательства в силу закона.

Обращает внимание, второй абзац статьи 2 Приказа N 21 от 18 февраля 2013 г. Федеральной Службы по Техническому и Экспортному Контролю «Для выполнения работ по обеспечению безопасности персональных данных при их обработке в информационной системе в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации». В которой появляется требование получения «лицензии на деятельность по технической защите конфиденциальной информации». Из данной нормы права следует требование по лицензированию деятельности по защите информации, но если в данной формулировке требование по лицензированию накладывается на третьих лиц, то в статье 6 этого приказа возникает требование об оценки безопасности обработки персональных данных, причем она может производиться как самим оператором, так и лицензированным контрагентом. В этой части закона возникает логическое противоречие поскольку ставится равенство между оценкой безопасности проведённой самим оператором и лицензированным контрагентом. Это подразумевает, что уровень знаний и компетенций оператора должны быть равнозначны лицензированному контрагенту. Что при отсутствии специальной подготовки проблематично из-за большого количества оцениваемых рисков, что будет показано ниже.

Получается следующая правовая конструкция. Законодатель требует соблюдение режима конфиденциальности при работе с любым количеством персональных данных. Таким образом, любой предприниматель, работающий с физическими лицами автоматически становиться оператором

персональных данных. Для соблюдения режима конфиденциальности должна быть проведена оценка возможных рисков безопасности работы с персональными данными. Эта оценка может быть проведена как самим оператором, так и лицензированным контрагентом. Наличие лицензии для оценки рисков подразумевает наличие специализированных компетенций подтверждающихся во время лицензирования. Таким образом мы видим, что несмотря на отсутствие в законе требования к лицензированию оператора персональных данных, подразумевается, что он должен обладать специализированными знаниями в области соблюдения режима конфиденциальности.

2.4 Меры по обеспечению безопасности персональных данных клиентов

Как уже было разобрано выше законодатель возлагает на оператора персональных полную ответственность по защите безопасности базы персональных данных, с которые он использует в своей работе (обрабатывает). Поэтому ему необходимо выполнять меры по обеспечению безопасности конфиденциальной информации которые систематизированы в статье 8 Приказа N 21 от 18 февраля 2013 г. Федеральной Службы по Техническому и Экспортному Контролю «В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

-идентификация и аутентификация субъектов доступа и объектов доступа;

-управление доступом субъектов доступа к объектам доступа;

-ограничение программной среды;

-защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

-регистрация событий безопасности;

-антивирусная защита;

-обнаружение (предотвращение) вторжений;

-контроль (анализ) защищенности персональных данных;

-обеспечение целостности информационной системы и персональных данных;

-обеспечение доступности персональных данных;

- защита среды виртуализации;

- защита технических средств;

- защита информационной системы, ее средств, систем связи и передачи данных;

- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

-управление конфигурацией информационной системы и системы защиты персональных данных».

Выбор мер защиты конфиденциальной информации должен соответствовать требованиям, изложенным в Постановлении Правительства РФ от 1 ноября 2012 г. N 1119, где уровни защищённости разбиты на 4 ступени в зависимости от угроз и от типа вида персональных данных с которыми проводится работа оператором. В случае обработки персональных данных в предпринимательской деятельности нужно ориентироваться на 4-ый минимальный уровень защищенности. Под него попадают данные попадающие под критерии изложенные в статье 12 данного приказа и под нее попадают информационные системы для которых актуальны угрозы 3-го типа. При этом в системе предприятий могут обрабатываться как

общедоступные персональные данные, так и «иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора». В данной формулировке обращает внимание отсутствие нижнего порога по количеству субъектов персональных данных обрабатываемых в системе. Установлен только верхний порог в 100 тысяч субъектов, при его превышении уровень защищенности необходим для работы с этими информационными системами должен быть повышен.

В статье 13 Постановления Правительства РФ от 1 ноября 2012 г. N 1119 устанавливаются требования необходимые для обеспечения четвертого уровня защищенности персональных данных в которые входит:

- «организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечение сохранности носителей персональных данных;

- утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз».

Оценка данного перечня действий с точки зрения бизнес процессов ведения предпринимательской деятельности показывает, что первые два пункта по организации режима безопасности помещения и обеспечения сохранности носителей информации в целом реализуется при повседневных бизнес процессах малого и среднего бизнеса. Про необходимости соблюдения пункта б статьи 13 Постановления многие руководители

забывают или не знают, но эти действия должны быть отнесены в зону компетенции юридического департамента по подготовке внутренних юридических актов организации.

Пункт г статьи 13 Постановления Правительства РФ от 1 ноября 2012 г. N 1119 имеет неоднозначную конструкцию. С одно стороны он требует «использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации», что подразумевает использование специальных программных продуктов лицензированных под работу с персональными данными, с другой стороны вводится дефиниция что их использование нужно только «в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз». При этом остается открытым вопрос кто должен сформулировать актуальные угрозы для конкретной информационной системы. Это вопрос был затронут в параграфе 2.1 магистерской работы и установлена неоднозначность требований регулятора, который с одно стороны дает возможность оператору персональных данных самому осуществить оценку угроз для информационной системы, а с другой стороны, в случае привлечений для этого контрагентов требует наличия соответствующей лицензии и компетенций. В случае применения данных норм к предпринимательской деятельности подобная неопределенность дает возможность для неоднозначного толкования закона контролирующими организациями.

В статье 8 Приказа N 21 от 18 февраля 2013 г. Федеральной Службы по Техническому и Экспортному Контролю систематизированы меры по обеспечению безопасности персональных данных в которые входят:

- Меры по идентификации и аутентификации субъектов и объектов доступа

- Меры по управлению доступом субъектов доступа к объектам доступа

-Меры по ограничению программной среды

- Меры по защите машинных носителей персональных данных
- Меры по регистрации событий безопасности
- Меры по антивирусной защите
- Меры по обнаружению (предотвращению) вторжений
- Меры по контролю (анализу) защищенности персональных данных
- Меры по обеспечению целостности информационной системы
- Меры по обеспечению доступности персональных данных
- Меры по защите среды виртуализации
- Меры по защите технических средств
- Меры по защите информационной системы, ее средств, систем связи и передачи данных
- Меры по выявлению инцидентов и реагированию на них
- Меры по управлению конфигурацией информационной системы

Приказом предусматривает пятнадцать различных типов мер по обеспечению безопасности максимальный набор которых требуется для обеспечения первого уровня защищённости персональных данных. Так как в предпринимательской деятельности достаточно четвертого уровня защищённости то мер по обеспечению безопасности требуется ограниченный перечень.

От оператора персональных данных требуется:

- Идентификация и аутентификация пользователей, являющихся работниками оператора.

- Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов.

- Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.

- Защита обратной связи при вводе аутентификационной информации.

- Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей).

- Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей.

- Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа.

- Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами.

- Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.

- Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.

- Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе).

- Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.

- Регламентация и контроль использования в информационной системе технологий беспроводного доступа.

- Регламентация и контроль использования в информационной системе мобильных технических средств.

- Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).

- Определение событий безопасности, подлежащих регистрации, и сроков их хранения.

- Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.

- Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения.

- Защита информации о событиях безопасности.

- Реализация антивирусной защиты.

- Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

- Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

-Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации.

- Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин.

- Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены.

-Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

- Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.

Проведенный анализ требования законодательства показывает необходимость соблюдения почти тридцати пунктов соответствия только по процедурных вопросам работы с персональными данными. Подобный перечень требований требует либо использования специализированных

программных продуктов для работы с персональным данными, либо работы отдельного высококвалифицированного специалиста задачей которого был бы контроль процедур работы с персональными данными в соответствии с требования законодательства. Подобное невозможно в рамках предпринимательской деятельности субъектов малого и затруднительно для среднего бизнеса. В связи, с чем можно утверждать, что процедурные требования по работе с персональными данными физических лиц в российском законодательном поле являются избыточными. По нашему мнению, законодателем должны быть введены ограничительные и достаточные меры по применимости данных нормативных актов для разных категорий бизнеса либо для разного объема обрабатываемых персональных данных.

2.5 Особенности передачи персональных данных клиентов

Интенсификация предпринимательской деятельности невозможна без информационного обмена между субъектами бизнеса. Одним из типов информации, которую приходится передавать при взаимодействии предпринимателей это персональные данные клиентов, например, при передаче транспортной компании списка клиентов на доставку. Подобная передача персональных данных находится под регулированием федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» в силу статья 3 которого определяет, что обработкой персональных данных является «любое действие (операция)» с персональными данными, в том числе и передача. При этом, как было отмечено в предыдущей части работы, ответственность за сохранность персональных данных полностью лежит на том, кто эти данные получил от физического лица. И если при работе внутри Российской Федерации все субъекты предпринимательской деятельности действуют в одном правом поле и при работе с персональными данными должны руководствоваться федеральным законом от 27.07.2006 г. №152-ФЗ «О

персональных данных», то в случае трансграничной передачи равномерность правового поля нарушается. Но и в этом случае действия оператора персональных данных регулируются федеральным законом №152-ФЗ в силу пункта 11 статьи 3 и отдельно оговариваются в статье 12 данного нормативного акта [13]. Разбору ее особенностей и посвященная данная часть магистерской работы.

Начнем с того, что закон разрешает передачу персональных данных не во все страны и даже оговаривает, что она может запрещении или ограничена. При этом все страны делятся на три категории [12].

К первой категории относятся страны являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ N 108) [33]. Именно для гармонизации внутренних законов Российской Федерации с положениями данной конвенции и разрабатывался федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных» [14]. Страны участники Конвенции работают на одних правовых принципах и стандартах защиты персональных данных физических лиц и часть 1 статьи 12 разрешает передачу персональных данных в эти страны. Всего стран ратифицировавших Конвенцию №108 – сорок семь [106-107].

Ко второй категории стан относятся страны «обеспечивающие адекватную защиту прав субъектов персональных данных». В данном случае под адекватностью нужно понимать равносильность или схожесть внутренних нормативных актов страны с принципами защиты персональных данных принятых в Российском законодательстве. Перечень таких стран утверждается Приказом №274 от 15 марта 2013 г. Федеральной службы ко надзору в сфере связи, информационных технологий и массовых коммуникаций [72] и содержится в его приложении. Список стран постоянно пересматривается как в сторону расширения [16], так и сторону сокращения стран по мнению нашего регулирующего органа обеспечивающих адекватную защиту прав субъектов персональных данных [10] [108]. На

сегодняшний момент в нее входит 22 страны. В публикациях в сети Интернет можно встреть ошибочное мнение, что стран подписавших Конвенцию №108 Совета Европы 63 [55] или 67, но это ошибочное мнение основанное, скорей всего на суммировании списка стран на самом деле подписавших или ратифицировавших данный нормативный акт и стран входящих в Приложение 1 Приказом №274 от 15 марта 2013 г. Роскомнадзора.

Третья группа стран, это все остальные страны и они по нормам части 4 статьи 12 федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных» относятся к странам «не обеспечивающих адекватной защиты прав субъектов персональных данных» поэтому передача персональных данных в эти страны возможна только с «наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных», пункта 1 части 4 статьи 12 [18] [109]. Это очень важная императивная оговорка, которую нужно учитывать в предпринимательской деятельности.

В качестве примера приведем одни из распространённых мелких бизнесов по посреднической деятельности по приобретению товаров в магазинах или на аукционах в Соединённых Штатах Америки, которые не входят в список стран, в которые разрешена передача персональных данных. Так вот заказ товаров с доставкой непосредственно заказчику почтовыми службами из США, в данном случае, будет нарушение закона «О защите персональных данных» так как для осуществления такой доставки пришлось бы предать персональные данные заказчика в страну, в которую это делать запрещено. А для того, чтобы это сделать по закону пришлось бы получать с каждого заказчика письменное разрешение на подобную передачу данных [20].

В этом ключе обращает на себя внимание опыт работы китайских компаний на российском рынке. Китайская Народная Республика не присоединялась к Конвенцию №108 Совета Европы и не входит в список стран, утвержденных Приказом №274 от 15 марта 2013 г. Роскомнадзора.

При этом китайский интернет магазин AliExpress https://aliexpress.ru является крупнейшим по объему заказов в российской сетевой торговле. Ответ на этот вопрос находится в Политике Конфиденциальности AliExpress [56] из которой мы видим, что обмен данными ведется с оператором, которым является AliExpress Russia Holding Private Limited зарегистрированная в Сингапуре, который входит в число стран обеспечивающих адекватную защиту прав субъектов персональных данных и входящую в список Приложения 1 Приказа №274 от 15 марта 2013 г. Роскомнадзора [22]. Более того для соответствия требованиям российского законодательства в политике конфиденциальности внесен пункт L где отражены требования федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных». В ключе рассматриваемого в параграфе вопроса интерес представляет оговорка о трансграничной передачи данных изложенная в следующем виде:

«Поскольку Aliexpress является международным сервисом мы можем осуществлять трансграничную передачу персональных данных покупателей и продавцов на территории государств, обеспечивающих адекватную защиту прав субъектов персональных данных (Сингапур, Германия), и государств, не обеспечивающих адекватную защиту прав субъектов персональных данных (Китай, США). Передача персональных данных на территории государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, возможна в случаях исполнения договора [23], стороной которого является покупатель или продавец (см. выше)».

Таким образом, предприниматель в виде интернет магазина Aliexpress пытается обеспечить себе защиту от претензий по нарушению пункта 1 части 4 статьи 12 федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных» требующего письменного согласия субъекта персональных данных на подобную трансграничную передачу за счет отсылки к вынужденному соблюдению договора поставки, по тексту: «Договора оказания транзакционных услуг и иных соглашений, заключаемых между нами и пользователями AliExpress (Покупателями и Продавцами)». В базе судебных

дел, рассматриваемых в судах российской юрисдикции по отношению к AliExpress Russia Holding Private Limited, нет претензий по нарушению закона о персональных данных [84].

Из оценки нормативных актов и их применимости к субъектам предпринимательской деятельности мы видим, что проблема трансграничной передачи персональных данных актуальна для глобальных мировых вендоров. Для локальных игроков, даже занимающих лидирующие позиции на рынке, это не актуально, хотя они оговаривают возможность привлечения третьих лиц для работы с персональными данными клиентов и возможности трансграничной передачи персональных данных [85]. При этом остается открытым вопрос о правом оформлении облачных решений по работе с персональными данными, которые сегодня развиваются стремительными темпами. Также закон накладывает ограничения на юрисдикцию физического размещением серверов подобных хранилищ, а при этом открытым остается вопрос о их сертификации для работы с конфиденциальной информацией. В действующей редакции закона «О защите персональных данных» подобные решения напрямую не регулируются.

На наш взгляд стоит произвести законодательную оценку такому новому явлению как облачные сервисы и облачные хранилища на предмет их соответствия закону «О персональных данных», а также законодательно определить требования к подобным сервисам по защите персональных данных физических лиц.

Глава 3 Гарантии защиты персональных данных клиентов

3.1 Правовой механизм защиты прав клиентов при обработке их персональных данных

Основой правового механизма защиты персональных данных клиентов предпринимателе является федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных» статья 2 которого ставит именно это основной целью данного нормативного акта: «Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну». Все его дефиниции ставят основной целью обеспечения законных требований гражданина на защиту информации о себе которая в наш информационное время составляет информационный образ гражданина. В части нормативных положений можно проследить соотношение с нормами материального права выраженного в нематериальной форме, если речь идет об автоматической, компьютерной обработке данных. Закон многими положениями проводит неразрывную связь между гражданином – субъектом права и его персональными данными являющейся его нематериально собственностью.

Но тут есть и различия с материальными, вещными объектами права, поскольку персональные данные, как это не странно, возникают как юридический объект только в момент отчуждения их от субъекта персональных данных, то есть в тот момент когда он их передает, сам или через третьих лиц другому юридическому субъекту, который уже в свою очередь пользуется им как информационным и юридическим объектом. Поэтому права субъекта персональных данных закреплённые в Главе 3 федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» сильно отличаются от вещных прав, поскольку объект права, после возникновения, не находится у обладателя права, а находится у третьего лица

которое называется законом оператором права. Таким оператором становиться предприниматель, получивший от клиента персональные данные, например, для исполнения договора.

Таким образом и права субъекта персональных данных на сами персональные данные очень специфические он может ознакомиться с ними, узнать цели использования, изменить их или потребовать их удаления, то есть получить подтверждения, что его персональные данные обрабатываются и распорядиться ими. «Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными» часть 1 статьи 14 федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных».

Еще одной специфической особенностью прав субъекта персональных данных является его право на получение информации о целях обработки персональных данных. Таким образом он получает информацию не только о факте обработки данных, но и о том зачем и для чего они обрабатываются. Так например, при заключении договора поставки законной целью обработки персональных данных будут действия целью которых будет исполнение текущего заключенного договора. При этом обработка персональных данных для проведения маркетинговых или рекламных акций будет уже требовать получения дополнительного разрешения от субъекта персональных данных [41].

Подробно разберем права субъекта персональных данных, установленные частью 7 статьи 14 федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных»:

«Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;

- цели и применяемые оператором способы обработки персональных данных;

- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

- сроки обработки персональных данных, в том числе сроки их хранения;

- порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

- информацию об осуществленной или о предполагаемой трансграничной передаче данных;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

- иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами».

Первым и основным правом которое установил законодатель является право на «подтверждение факта обработки персональных данных», поскольку подтверждение или не подтверждения этого факта имеет юридически значимые последствия [42-43]. В данном случае наблюдается явно слабая позиция субъекта персональных данных по отношению к оператору так как он требует доступа к тому, что физически не находится в его распоряжении. Оператор же, как лицо, владеющее доступом к информации в незаконных целях или в недобросовестных устремлениях имеет возможность не сообщить владельцу персональных данных об их

обработке. Получается, что субъект персональных данных будет вынужден доказывать, что его данные обрабатываются, например фактом их передачи или другим способом, или же обратиться за защитой своих интересов в уполномоченный орган или прибегнуть к судебной защите, часть 1 статьи 17 федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных». Уполномоченным органом для защиты прав субъектов персональных данных будет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), статья 1 Постановления Правительства РФ от 16.03.2009 N 228 (ред. от 28.12.2020) «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» [64].

Следующим фактом, который требует юридического подтверждения, это правовые основания для проведения обработки персональных данных. Получены ли сведения законным способом, в порядке установленном федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных», или же нет. Получил ли оператор согласие субъекта персональных данных или может быть информация получена из открытых источников. Причем в последнем случае, даже если персональные данные получены из открытых источников, субъект персональных данных все равно не теряет права распоряжаться ими.

Еще одним важным юридически значимым фактом является «цель обработки персональных данных», без установки цели для которых собирались и обрабатывались персональные данные субъект не имеет возможности осознанно и разумно определить свое отношение обработке своих данных и распорядиться своим правом на то удалить или оставить их данном оператору.

В третьем пункте закона еще раз уделяется внимание праву на ознакомления с целями обработки персональных данных, но его нужно рассматривать в связке со способами обработки персональным данным. В

данном случае акцентируется внимание именно на способе обработки и целям для которых эта обработка осуществляется.

Для обеспечение полноценной юридической защиты субъект персональных данных несомненно имеет право знать то к кому он должен предъявлять претензии и с кого требовать соблюдения своих прав. Это зафиксировано в пункте 4 части 7 статьи 14 федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных», который устанавливает требование к оператору представлять не только «наименование и место нахождения оператора» персональных данных, но и лицо, которое производит обработку. В данном случае имеется ввиду не физическое лицо, которое непосредственно занимается обработкой данных поэтому поводу есть даже оговорка «за исключением работников оператора», а лицо в понимании юридического или физического лица которому передается, поручается обработка данных если она осуществляется не самим оператором. Закон разрешает перепоручать обработку данных третьим лицам, но ответственность за их сохранность и конфиденциальность все равно оставляет на операторе, части 5 статьи 6 №152-ФЗ. Это же требование дублируется и раскрывается в пункте 10 части 7 статьи 14 федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных», где методом перечисления расписывается какие данные о лице которому поручена обработка персональных данных субъекта должна быть раскрыта. Тут мы видим единый подход к раскрытию информации если данные об наименовании и адресе оператора персональных данных должных быть доступны субъекту, то и сведения о третьем лице, которому поручена подобная обработка оператором тоже должная быть предоставлена.

И только в пятом пункте статьи законодатель доходит самих персональных данных и фиксирует право субъекта на получение информации о том какие конкретно данные о нем обрабатываются данным оператором. Тут нужно напомнить, что персональные данные не ограничиваются фамилией именем отчеством, адресом и паспортными

данными. Ими может явятся все что позволяет идентифицировать субъекта персональных и если мы говорим о мире сети Интернет, то это может быть IP адрес, MAC адрес, цифровой след, файлы Куки (cookie), данные геопозиционирования и другие. Обращает на себя внимание требование о раскрытие источника получения персональных данных, который непосредственно связан с пунктом два данной статью. Персональные данные, которые обрабатывает оператор должны иметь законный источник происхождения.

Персональные данные относятся к бессрочным конфиденциальным данным, поскольку они в любой момент времени могут идентифицировать субъекта персональных данных, поэтому часть 7 статьи 5 федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» устанавливает ограничение в сроке обработки персональных данных достижением установленных целей, после чего персональные данные должны быть либо уничтожены, либо обезличены. Субъект персональных данные имеет право знать сроки в течении которого производится обработка его персональных данных. Если посмотреть практику по декларированию политики в отношении обработки персональных данных российских предпринимателей то мы увидим, что срочность обработки персональных в декларациях ООО «Вайлдберриз» [57] https://www.wildberries.ru и ООО «Интернет Решения» [56] https://www.ozon.ru/ не огранивается. Скорей всего составители политики решили, что это само собой вытекает из заявленных целей обработки персональных данных, что не противоречит федеральному закону от 27.07.2006 г. №152-ФЗ «О персональных данных». Однако, не совсем понятно как при реализации права субъекта персональных данных закреплённое пунктом 6 часть 7 статьи 14 федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» они будут описывать сроки обработки персональных данных, так как следуя данной норме права они должны быть установлены в явном виде.

В Политике конфиденциальности международного интернет магазина AliExpress [56] предусмотрен отдельный пункт D посвящённый хранению персональных данных и там срок хранения персональных данных сформулирован следующим образом «Мы храним Вашу персональную информацию на протяжении времени, когда у нас есть обоснованная коммерческая необходимость хранить такие данные в целях оказания Вам услуг или предоставления продуктов, насколько это требуется или допустимо в соответствии с применимым законодательством». То есть в конструкции данного положения подразумевается, что срок обработки персональных данных ограничен договорными отношениями с клиентов, но может быть ограничен в зависимости от требований локального законодательства. Подобные оговорки «локального» характера мы неоднократно встречаем в правилах китайского предпринимателя и даже разбирали в Главе 2 работы в отношении трансграничной передачи персональных данных.

Пример прямого нарушения императива федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» о срочности обработки персональных мы находим в Положениях о политике конфиденциальности ООО «М-Инвест» [49], интернет магазин https://www.xcom-shop.ru. В абзаце 2 части 4 данного положения сказано: «Обработка персональных данных Пользователя осуществляется без ограничения срока». Это прямое нарушение принципа ограничения сроков обработки персональных данных, установленного законодателем.

Извещение пользователя о порядке осуществления его прав закреплённый в пункте 7 части 7 статьи 14 федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных» по смыслу своих дефиниций относиться не к моменту запроса пользователем персональных данных, а к предоставлению ему возможности знать о своих правах до составления запроса и на момент возникновения требования на составления данного запроса. Именно для соответствия этому требованию закона и

производится публикация правил работы с персональными данными на страницах сайтов компаний работающих с физическими лицами. Там же должна указываться и информация о трансграничной передаче данных, а если пользователь запросил информацию о персональных данных, то оператор должен указать о возможной трансграничной передачи данных в явном виде.

Если мы проанализируем положения о работе с персональными данными, принятыми у российских предпринимателей, то мы увидим, что в них не оговаривается трансграничная передача сведений, в то время как в положениях китайского интернет магазина AliExpress [56] они явно прописаны и оговорены для пользователей из Российской Федерации в части L правил.

В части 8 статьи 14 федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных» оговариваются ограничения прав субъекта персональных данных на получение данных и доступ к ним, но это связано с работой правоохранительных органов и не относится к сфере предпринимательской деятельности. Но именно к этой сфере относятся положения статьи 15 федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных» «Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации» которое требует получение предварительного согласия субъекта персональных данных на получение рекламной и маркетинговой информации. Причем факт доказывания наличия предварительного согласия лежит на операторе персональных данных. В случае если он не доказал факт получения согласия, то обработка персональных данных будет считаться незаконной.

Построение защиты прав на персональные данные физического лица строиться на том, что он является слабой стороной в споре с оператором персональных данных и поэтому ему даны существенные права, а на оператора возлагаются обязательства по их соблюдению. Для исключения

злоупотреблением правом со стороны субъектов персонального права законом установлены временные интервалы для случаев повторных запросов со стороны субъектов персональных данных.

Из проведенного анализа нормативных актов и их практической реализации в предпринимательской деятельности в положениях об обработке персональной информации мы видим, что предприниматели часто игнорируют требования закона о явном объявлении целей обработки персональных данных ограничиваясь дефиницией о выполнении договорных обязательств. Ни у кого из рассмотренных юридических лиц в явном виде не приписаны сроки обработки персональных данных, а также можно назвать расплывчатыми формулировки о трансграничной передаче персональных данных даже в тех случаях когда это оговаривает.

3.2 Ответственность в сфере обработки персональных данных клиентов

Нормы закона «О персональных данных» устанавливают ответственность оператора персональных данных за несоблюдения требования закона. Ответственность перед субъектом персональных данных возникает в момент, когда оператору передаются персональные данные. Причем поскольку нормы права подразумевают законность получения персональных данных то на оператора возлагается обязанность соблюдения принципов законности при их получении и проверка принципа законности получения персональных данных если он получает их от третьих лиц. Это может быть как представитель субъекта персональных данных в виде физического лица, например опекун несовершеннолетнего ребенка, или же другое юридическое лицо от которого поступают персональные данные. Требование подтверждения законности передачи персональных данных от третьих лиц напрямую следует из части 1 статьи 9 федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» «Согласие на обработку

персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме». А это обстоятельство нужно обратить внимание так как в предпринимательской деятельности практикуется использование, так называемых, баз данных клиентов, когда самого предпринимателя не очень заботит законность ее происхождения. Уже одни факт обработки подобных персональных данных, даже нахождение их и хранение на компьютерных носителях юридического лица является нарушением федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» и влечет за собой ответственность.

Законодательством предусмотрены все типы ответственности за несоблюдения законодательства в области персональных данных [87]. Работника допустившего нарушения могут привлечь к дисциплинарной и материальной ответственность в порядке закреплённом в «Трудовом кодексе». Кроме этого предусмотрена гражданско-правовая, административная и уголовная ответственность за нарушение правил обработки и хранения персональных данных сотрудников и клиентов. Уголовная ответственность наступает в случаях связанных с публичной публикацией персональных данных и не входит в сферу рассматриваемых правовых отношений, поэтому в работе мы затронем только административную ответственность [27] [86].

Статья 13.11 Кодекса «Об административных правонарушениях» от 30.12.2001 N 195-ФЗ [49] полностью посвящена нарушениям законодательства в области персональных данных, за исключением уголовно наказуемых деяний [26].

Часть 1 статьи 13.11 Кодекса «Об административных правонарушениях» от 30.12.2001 N 195-ФЗ устанавливает ответственность за нарушение статьи 6 и статьи 10 нарушением федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» в том случае когда идет обработка персональных данных несовместимая с целями сбора

персональных данных или же обработка тех данных которые не предусмотрены законодательством РФ. Как раз к этому случаю относятся рекламные рассылки по базе персональных данных клиентов, которая собиралась, например, для доставки товара. А также к этому случаю будет относиться сбор избыточных данных исполнения договора данных о субъекте персонального права [28]. Нарушение этой статьи влечет «предупреждение или наложение административного штрафа на граждан в размере от одной тысячи до трех тысяч рублей; на должностных лиц - от пяти тысяч до десяти тысяч рублей; на юридических лиц - от тридцати тысяч до пятидесяти тысяч рублей».

В случае если обработка персональных данных ведется без согласия субъекта персональных данных, например, как в случае который приведен в начале параграфа статьи 13.11 Кодекса «Об административных правонарушениях» от 30.12.2001 N 195-ФЗ подразумевает более строгую ответственность по части 2. Также под эту часть попадёт и нарушение состава сведений при обработке персональных данных, например включение в них информации о национальности или политических пристрастиях [30]. Привлечение к ответственности по этой части влечет наложение административного штрафа на граждан в размере от трех тысяч до пяти тысяч рублей; на должностных лиц - от десяти тысяч до двадцати тысяч рублей; на юридических лиц - от пятнадцати тысяч до семидесяти пяти тысяч рублей.

Часть 3 статьи 13.11 Кодекса «Об административных правонарушениях» от 30.12.2001 N 195-ФЗ подразумевает ответственность ща нарушение части 2 статьи 18.1 федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» обязывающей оператора публиковать в неограниченном доступе информацию о политике оператора в отношении обработке персональных данных, а также сведений о реализуемых требованиях к защите персональных данных [31].

В предыдущих главах мы анализировали положения об обработке персональных данных нескольких крупных интернет магазинов и определили различные подходы в исполнении норма федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных». Анализ положений данных публичных документов в области раскрытия информации о реализуемых требованиях к защите персональных данных также показывает большую разницу [34] в исполнении и трактовке положений части 2 статьи 18.1 федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» [60].

Так в положениях интернет магазина ООО «Вайлдберриз» [57] https://www.wildberries.ru описанию средств защиты посвящена глава 6 где подробно расписываются принимаемые меры для обеспечения конфиденциальности персональных данных. В положениях ООО «Интернет Решения» [56] магазин https://www.ozon.ru/, подошли боле формально и просто задекларировали о том, что они занимаются защитой в соответствие с требованием закона, но без раскрытия принимаемых для этого мер. Подобный подход мы видим и в случае оценки положений китайского вендера AliExpress [56]. Но самым слабым, с юридической точке зрения являются положения о защите персональных данных ООО «М-Инвест» [58], интернет магазин https://www.xcom-shop.ru, где просто декларируется соответствие закону о персональных данных без раскрытия какой либо информации [88-89].

Ответственность по часть 3 статьи 13.11 Кодекса «Об административных правонарушениях» от 30.12.2001 N 195-ФЗ не самая строгая, нарушитель даже может ограничится предупреждением [67].

Самый крупный штраф по данной статье предусмотрен в части 8 и накладывается он за то, что операторы персональных данных не обрабатывают из на территории Российской Федерации. Размер штрафа по этой части может достигать шести миллионов рублей. Более того при повторном нарушении максимальный размер штрафа возрастает до

восемнадцати миллионов рублей. При этом правоприменительной практике по данной части статьи 13.11 КоАП РФ еще нет.

3.3 Проблемы правоприменительной практики по спорам об обработке персональных данных

Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных» за время своего существования подвергается постоянной модернизации и актуализации поскольку находится на защите интересов граждан на самой быстротечной и быстроменяющейся сетевой - информационной сфере жизни современного общества. Буквально перед защитой магистерской работы 11.06.2021 года Президент Российской Федерации В.В.Путин подписал закон №216-ФЗ «О внесении изменений в статьи 183 и 320 Уголовного кодекса Российской Федерации» [91-92] [74], которым изменяется мера ответственности в сторону ужесточения в случае нарушения федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», в случае если произошло «Разглашение сведений о мерах безопасности, в отношении должностного лица правоохранительного или иного контролирующего органа». Это пример, последовательных действий государства в сторону усиления контроля за информацией распространяющихся посредством информационных сетей [35] [93]. Несмотря на то, что это напрямую не относится к теме магистерской работы, связанной с предпринимательской деятельностью, но это демонстрирует тенденции повышения контроля государства над информацией и требует от субъектов предпринимательского права внимательно относиться с соблюдению конфиденциальности персональной информации и к учету ограничений и обязательств накладываемых на них нормативными актами.

Сфера защиты персональных является новой и база правоприменительной практике в этой сфере пока еще недостаточно

разработана. В данном обзоре приводится сведения, собранные в правовых базах данных на май 2021 года [37] [73] [94].

Так, на указанный период, судебных актов затрагивающих в своих фабулах вопросы о привлечении по статьи 13.11 Кодекса «Об административных правонарушениях» от 30.12.2001 N 195-ФЗ всего 356 наибольшее количество рассмотренных дел приводится на суды Москвы и Московской области. Из поверхностного обзора сразу видна системная ошибка в определении подсудности по рассмотрению судебных претензий в рамках статьи 13.11 КоАП РФ. Физические лица обращаются за защитой своих интересов в арбитражные суды РФ полагая, что раз они выставляют претензии к юридическому лицу то рассмотрение их заявлений подсудно арбитражному суду. Так в постановлении Первого арбитражного апелляционного суда от 20 июня 2018 г. по делу N А11-5722/2018 [62] подробно разъясняется, что «дела об административных правонарушениях, предусмотренных статьей 13.11 Кодекса Российской Федерации об административных правонарушениях исключены из компетенции арбитражных судов». Поэтому граждан при разрешении дел связанных с привлечением к ответственности юридических лиц по делам связанным с нарушением федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» необходимо обращаться суды общей юрисдикции. Это подтвердил Верховный Суд РФ определением от 28 ноября 2018 г. №301-АД18-19101 [51]. «рассмотрение дел об административных правонарушениях, предусмотренных статьями 13.11 и 13.12 КоАП РФ к компетенции органов Роскомнадзора, куда обратилась заявительница, не относится. Согласно статье 23.1 арбитражного процессуального кодекса РФ рассмотрение этих дел отнесено к компетенции судов общей юрисдикции».

В имеющейся практике часть обращений связано с рассмотрением споров, где фабулой дела является обращение гражданина за предоставлением персональных данных от оператора персональных данных, которым является работодатель. То есть отношения между субъектом

персональных данных и оператором регулируются трудовым законодательством, что облегчает установку факта наличия обработки персональных данных.

Часть дел связана с нарушениями в роботе средств массовой информации, когда персональные данные публикуются изданием без согласия на то субъекта персональных данных, например, Постановление Верховного Суда от 28 июня 2018 г. N 74-АД18-11 [62] где обжаловалось привлечение к административной ответственности главного редактора газеты за публикацию персональных данных. Также есть судебные споры о незаконной публикации персональных данных в сети Интернет [40].

Наряду с этим постепенно формируется практика затрагивающие вопросы предпринимательского права. В предыдущих параграфах, в качестве спорной с точки зрения права ситуации, был рассмотрен пример, когда предприниматель для маркетингового продвижения товара или для рекламы услуги использует персональные данные полученные с нарушением норм федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», например, используя базу данных клиентов другого юридического лица или даже получая их из открытых источников. Последний случай стал спорной ситуацией между ООО "ИНВЕСТ ЛАЙФ" и физическим лицом, Постановление Московского городского суда от 3 августа 2017 г. N 4а-2675/2017 [61]. Юридическое лицо использовало персональные данные физического лица для предложения ему услуги: «Согласно материалам дела, 14 июня 2016 года генеральный директор ООО "ИНВЕСТ ЛАЙФ" (юридический адрес: <...>) Ф. допустил использование информации о гражданине Р*** И.Э. (его персональных данных), а именно Ф.И.О. и номера его мобильного телефона (***), осуществив звонок на указанный номер в целях продвижения инвестиционных продуктов Общества». Это действие было признано судом составом административного правонарушения по статье 13.11 КоАП РФ. Обратим внимание на выводы суда кассационной инстанции сделанные в постановлении: «Системный анализ приведенных

норм позволяет сделать вывод о том, что использование оператором персональных данных физического лица, независимо от источников их получения, в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с ним посредством связи допускается только после получения согласия субъекта персональных данных (физического лица)».

«В ходе рассмотрения настоящего дела установлено, что ООО "ИНВЕСТ ЛАЙФ", генеральным директором которого является Ф., использовало персональные данные Р*** И.Э. (его Ф.И.О. и телефонный номер), то есть информацию, прямо относящуюся к нему, в целях реализации инвестиционных продуктов без его предварительного согласия».

Таким образом вне зависимости от способа получения персональных данных клиента использовать их в предпринимательской деятельности можно только с после получения предварительного согласия субъекта персональных данных.

Достаточно часто фокус споров находится в области передачи персональных данных от кредитной организации к коллекторским агентам оказывающим банкам услуги по взысканию задолженности с должников. Истцами в подобных делах выступают физические лица предъявляющие претензии о нарушении федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» в отношении банковских организации. В пример можно привести апелляционное определение Саратовского областного суда от 25 июня 2019 года по делу №33-4572 [52] ответчиком, в котором выступает ПАО «Сбербанк России» в которой истец М. оспаривал право ответчика передавать персональные данные третьим лица. Согласно мотивационной части решения суда было установлено, что истец М. заключил с ответчиком ПАО «Сбербанк России» кредитный договор, который содержал следующий существенный для рассмотрения дела пункт которым «истец предоставил право банку при неисполнении или ненадлежащем исполнении заемщиком обязательств и наличии

просроченной задолженности по договору без уведомления заемщика поручать третьим лицам на основании агентских или иных договоров, заключенных кредитором с третьими лицами, осуществлять действия, направленные на погашение заемщиком просроченной задолженности по договору; предоставлять третьим лицам в соответствии с условиями агентских или иных договоров информацию и документы, подтверждающие права кредитора по договору, в том числе о предоставленном заемщику кредите, размере задолженности заемщика по договору, условиях договора, а также информацию о заемщике, в том числе содержащую его персональные данные».

Основываясь на правом анализе этого пункта договора суд счел, что «при заключении договора истец сообщил ответчику свои персональные данные (фамилию, имя, отчество, год, месяц, дату и место рождения, адрес, семейное, социальное и имущественное положение, образование, профессию, доходы, контактные телефоны, другую информацию), предъявил паспорт гражданина Российской Федерации, а также действуя своей волей и в своем интересе, дал согласие на их обработку (в том числе на сбор, систематизацию, накопление, хранение, уточнение, обновление, изменение, распространение, передачу (включая трансграничную передачу), обезличивание, блокирование и уничтожение)». На основании чего посчитал передачу персональных данных истца третьему лицу, которым выступило коллекторское агентство законным.

«Принимая во внимание, что истец при заключении кредитного договора выразил свое согласие на обработку и передачу ПАО "Сбербанк России" персональных данных третьим лицам, в том числе для взыскания задолженности по кредитному договору. пришел к правильному выводу о том, что действия банка по передаче персональных данных истца не нарушают прав истца как субъекта персональных данных и не противоречат положениям Федерального закона от 27 июля 2006 года N 152-ФЗ "О

персональных данных" и, как следствие, отказал в удовлетворении исковых требований».

При этом иной подход в трактовании федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» мы видим в постановлении Девятого Арбитражного Апелляционного суда от 02 марта 2018 года №09АП-4283/2018 по делу N А40-173100/17 [66]. Суть претензии состояла в обжаловании ООО "СК "Ренессанс Жизнь" постановления о привлечении к административной ответственности предусмотренной частями 1, 2 статьи 14.8 Кодекса Российской Федерации об административных правонарушениях вынесенное Управлением Роспотребнадзора по Республике Татарстан. Разобрав дело апелляционный суд установил ошибочность привлечения ООО "СК "Ренессанс Жизнь" в административной ответственности по частям 1, 2 статьи 14.8 КоАП РФ, но установил наличие состава правонарушения подлежащего административному наказанию предусмотренному статьей 13.11 Кодекса Российской Федерации об административных правонарушениях. Так судом дана правовая оценка следующих пунктов страхового договора: «в п. 8.4 раздела 8 договора страхования указано "Подписывая настоящий договор, страхователь в соответствии с ФЗ РФ "О персональных данных" N 152-ФЗ от 27.07.2006 выражает страховщику согласие на обработку, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, указанных в настоящем договоре страхования; в том числе передачу Агенту КБ "Ренессанс Кредит" (ООО), перестраховочным организациям (в том числе находящимся за рубежом) своих персональных данных...».

Эту формулировку суд посчитал нарушающей ч. 1 ст. 9 Федерального закона "О персональных данных". Поскольку «из текста заключенного между потребителем договора страхования невозможно установить наименование или ФИО и адрес компаний, осуществляющих рассылку, агента по

агентскому договору, перестраховочных организаций, перечень персональных данных, на обработку которых дается согласие субъекта персональных данных».

«Не поименованные лица, фактически становятся операторами либо лицами, получившими доступ к персональным данным потребителя, не становятся обязанными сохранять конфиденциальность таких данных».

«Подписав данное условие договора страхования, потребитель фактически соглашается с возможностью обработки его персональных данных третьими лицами, при этом страховой компанией не были учтены установленные законом специальные требования к письменному согласию субъекта персональных данных».

Подобная трактовка нормы договора арбитражным судом апелляционной инстанции показывает, что закон требует от предпринимателя письменного согласия на передачу своих персональных данных конкретному юридическому лицу.

Анализ данных судебных актов показывает разный правовой подход к трактовке законности пунктов договора заключенного между клиентом и предпринимателем со стороны судов общей юрисдикции и арбитражного суда. Такая неоднозначность правоприменительной практики отрицательно сказывается на предпринимательской деятельности поскольку не дает однозначной оценки в каком виде должно получаться согласие на передачу персональных данных третьим лицам от субъекта персональных данных. Плюс разность судебных актов будет фактором неопределённости в случае судебного разрешения спорных ситуаций.

Из оценки судебных актов видно, что правоприменительная практика по вопросам обработки персональных данных только формируется и трактовка одних и тех норм может отличаться в зависимости от юрисдикции судов. Для защиты, как интересов предпринимателей, так и субъектов персонального права требуется унификации применения права, что требует разъяснений в этом вопросе от высших судов Российской Федерации.

Заключение

Конфиденциальная информация сопровождает человечество с момента зарождения общественных отношений. С развитием предпринимательского дела в постоянный оборот вошли такие понятия как банковская и коммерческая тайна. Относительно недавно к списку конфиденциальной информации добавились еще и персональные данные. В магистерской работе рассмотрены особенности становления юридического понятия «персональные данные» в контексте одного из видов конфиденциальной информации. Рассмотрены правовые основы законодательства о защите персональных данных, а также требования предъявляемые законодательством Российской Федерации к сбору, обработке и хранению персональных данных. Рассмотрены права субъекта персональных данных и правовые формы их защиты.

Из оценок норм права можно сделать вывод о том, что состав персональных данных окончательно не сформирован. Он уточняется и расширяется по мере появления новых технически-информационных способов идентификации субъекта персональных данных. Это делает невозможным составить закон так чтобы списочно ограничить их состав, что проводит к ведению обобщенных формулировок в нормативные акты.

Оценка практической реализации формулирования целей обработки персональных данных физических лиц открывает перед нами неоднородность в использования норм права и показывает значимость четкого определение целей юридических документах предпринимателей. Из проведенного анализа мы видим, что предприниматели часто игнорируют требования закона о явном объявлении целей и сроков обработки персональных данных ограничиваясь дефиницией о выполнении договорных обязательств.

Рекомендуется при составлении положения по обработке конфиденциальной информации субъекта предпринимательского права

формулировать цели обработки персональных данных таким образом, чтобы охватить все возможные сферы их использования в предпринимательской деятельности.

Ни у кого из рассмотренных юридических лиц в явном виде не приписаны сроки обработки персональных данных, а также можно назвать расплывчатыми формулировки о трансграничной передаче персональных данных даже в тех случаях года это оговаривает.

Рекомендуется более четко формулировать эти положения в заявляемой политике по работе с персональными данными.

Проведенный анализ законодательства показывает необходимость соблюдения почти тридцати пунктов соответствия только по процедурных вопросам работы с персональными данными. Подобный перечень требований требует либо использования специализированных программных продуктов для работы с персональным данными, либо работы отдельного высококвалифицированного специалиста задачей которого был бы контроль процедур работы с персональными данными в соответствии с требования законодательства. Подобное невозможно в рамках предпринимательской деятельности субъектов малого и затруднительно для среднего бизнеса. В связи, с чем можно утверждать, что процедурные требования по работе с персональными данными физических лиц в российском законодательном поле являются избыточными.

Предлагается ввести ограничительные и достаточные меры по применимости данных нормативных актов для разных категорий бизнеса либо для разного объема обрабатываемых персональных данных.

Проблема трансграничной передачи персональных данных актуальна для глобальных мировых вендоров. Для локальных игроков, даже занимающих лидирующие позиции на рынке, это не актуально, хотя они оговаривают возможность привлечения третьих лиц для работы с персональными данными клиентов и возможности трансграничной передачи персональных данных.

На наш взгляд, стоит произвести законодательную оценку такому новому явлению как облачные сервисы и облачные хранилища на предмет их соответствия закону «О персональных данных», а также законодательно определить требования к подобным сервисам по защите персональных данных физических лиц.

Из оценки судебных актов видно, что правоприменительная практика по вопросам обработки персональных данных только формируется и трактовка одних и тех норм может отличаться в зависимости от юрисдикции судов. Для защиты, как интересов предпринимателей, так и субъектов персонального права требуется унификации применения норм права, что требует разъяснений в этом вопросе от Высших Судов Российской Федерации.

Список используемой литературы и используемых источников

1. Авдеев В.В. Государственная регистрация индивидуальных предпринимателей // Бухгалтер и закон. 2013. № 2. С. 12-21.
2. Авдеев М.Ю. Законодательство РФ о неприкосновенности частной жизни: к вопросу о заимствовании зарубежного опыта // Новый юридический журнал. 2014. N 1. С. 35-53.
3. Авдеева М.В., Пиджаков А.Ю. «Тайна» как правовое понятие // Ленинградский юридический журнал. 2012. № 4 (30). С. 142
4. Алексеев С. С. Структура советского права, М., «Юрид. лит.», 1975, 264 с.
5. Андреев В.К. Обязательство, связанное с осуществлением предпринимательской деятельности (предпринимательский договор) // Юрист. 2015. № 16. С. 4-8.
6. Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 N 95-ФЗ // Собрание законодательства РФ. 2002. N 30. Ст. 3012
7. Бабина Е.Е. История развития законодательства в области защиты государственной тайны в России // Вестник УрФО. Безопасность в информационной сфере. 2013. № 2 (8). С. 7.
8. Бадамшин С.К. Каримова Э.С. Процедура государственной регистрации индивидуального предпринимателя: теория и практика // Актуальные проблемы права на современном этапе развития России и Республики Башкортостан. Сибай: Изд-во ГУП РБ «СГТ», 2013. С. 40-45.
9. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год URL:https://fstec.ru/component/attachments/download/289 (дата обращения: 13.06.2021).
10. Бахрах Д.Н., Российснский Б.В., Старилов Ю.Н. Административное право // ООО «Издательство НОРМА», 2007.

11. Бродская И.А. Конфиденциальные сведения: способы использования. Правовой смысл понятия «разглашение» // Адвокат. 2000. № 3. С. 10.

12. Бунин О.Ю. Аспекты справедливой уголовной ответственности подставных физических лиц в юридическом лице // Адвокат. 2016. N 3. С. 73 - 77.

13. Вайпан В.А. Источники предпринимательского права: теория и практика // Право и экономика. 2015. N 10. С. 4 - 17.

14. Виленский А.В., Лылова О.В. Specificity of the territory of small business and its state support in Russia // Экономика: вчера, сегодня, завтра. 2016. № 3. С. 186-197.

15. Всеобщая Декларация прав человека: принята Генеральной Ассамблеей Организации Объединенных Наций в 1948 году // Рос. газета. 1995. 5 апр. 26)

16. Гвоздева О.М. Конституционное право на предпринимательскую деятельность в современной России: теоретический аспект // Конкурентное право. 2014. № 4. С. 5-8.

17. Гиляров Е.М., Балабанов С.П. Государственно-правовое обеспечение информационной функции в истории России // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. Тамбов: Грамота, 2013. № 3 (29): в 2 ч. Ч. I. С. 48-52.

18. Горбачева Е.М. Достоверность сведений, вносимых в Единый государственный реестр юридических лиц: проблемы судебно-арбитражной практики // Арбитражные споры. 2015. N 1. С. 112 - 122.

19. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 N 51-ФЗ // Собрание законодательства РФ. – 1994. - № 32. Ст. 3301. 4)

20. Гришаев С.П. Эволюция законодательства о юридических лицах // СПС КонсультантПлюс. 2015.

21. Губин Е.П. Правовое обеспечение свободы экономической деятельности // Предпринимательское право. 2015. № 4. С. 3-9.

22. Закон РСФСР от 22.03.1991 г. № 948-1 «О конкуренции и ограничении монополистической деятельности на товарных рынках» // Ведомости СНД и ВС РСФСР. 1991. - N 16. Ст. 499.

23. Ионов В.И. Бизнес-право. М., 1998. С. 59.

24. Кибальник А., Соломоненко И. Понятие и виды тайны в уголовном праве // Российская юстиция. 2001. № 2. С. 55. 43)

25. Князькин С.И., Юрлов И.А. Гражданский, арбитражный и административный процесс в схемах с комментариями: учебник. М.: Инфотропик Медиа, 2015. 434 с.

26. Кодекс Российской Федерации «Об административных правонарушениях» от 30.12.2001 N 195-ФЗ // Собрание законодательства РФ. 2002. - N1 (ч. 1). Ст. 1.

27. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ URL:http://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 13.06.2021). 57)

28. Кодификация российского частного права 2015 / В.В. Витрянский, С.Ю. Головина, Б.М. Гонгало и другие; под ред. П.В. Крашенинникова. - М.: Статут, 2015. - 447 с.

29. Конвенции Совета Европы о защите физических лиц в отношении автоматизированной обработки персональных данных (ETS N 108) (заключена в г. Страсбурге, 28 января 1981 г.). // «Бюллетень трудового и социального законодательства РФ», №4, 2014.

30. Конституционная экономика: Учебник для юридических и экономических вузов. Отв. ред. Гаджиев Г.А. М.: 2010. – 256 с.

31. Конституционное право Российской Федерации: учебник для студентов, обучающихся по направлению подготовки «Юриспруденция» (квалификация «бакалавр» / И.А. Алжеев, И.Б. Власенко, Е.Ю. Догадайло и

другие; отв. ред. С.И. Носов. М.: Статут, 2014. 391 с.

32. Конституционно-правовые основы защиты персональных данных Касимов В. В. Тольяттинский государственный университет, Институт права, Кафедра Конституционное и административное право. Магистерская диссертация. Тольяти, 2017, 100 с

33. Конституция (Основной закон) Союза Советских Социалистических Республик. Утверждена Постановлением Чрезвычайного VIII съезда Советов Союза ССР от 5 декабря 1936 г. // Известия ЦИК СССР и ВЦИК. № 283. 06 декабря 1936.

34. Конституция РФ, принятая всенародным голосованием 12.12.1993 (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ) // Собрание законодательства РФ. 2014. №31. Ст. 4398.

35. Корпоративное право: учебник / Е.Г. Афанасьева, В.Ю. Бакшинскас, Е.П. Губин и другие; отв. ред. И.С. Шиткина. 2-е изд., перераб. и доп. М: КНОРУС, 2015. 1080 с.

36. Крутикова Д.И. Правовой режим информации ограниченного доступа в банковской деятельности: дис. канд. юрид. наук. / М., 2015. С. 10 2)

37. Кузнецов И.В. Правовые основы банкротства индивидуальных предпринимателей в российском праве // Современное общество и право. 2014. № 3 (16). С. 14.

38. Лаптев В.А. Правовое регулирование предпринимательства в России (исторический аспект) // Lex russica. 2015. № 4. С. 33-45.

39. Мартыненко, А.Е. Международный опыт осуществления контроля в сфере обработки персональных данных / А.Е. Мартыненко // SCIENCE TIME. 2014. № 12(12). - С. 312. 29)

40. Месропова С. Какими видами деятельности может заниматься ИП? // Административное право. 2014. N 2. С. 51 - 58.

41. Методические рекомендации «По разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных

системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» / Центр м 8 ФСБ России 31 марта 2015 года № 149/7/2/6-432 URL:http://www.fsb.ru/files/PDF/Metodicheskie_recomendacii.pdf (дата обращения: 13.06.2021).

42. Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли от 21 апреля 2010 года № 2 / Министерство связи и массовых коммуникаций Российской Федерации URL: https://digital.gov.ru/common/upload/publication/1410065MC.pdf (дата обращения: 13.06.2021).

43. Мохов А.А. Комментарий к Федеральному закону от 7 мая 2013 г. N 78-ФЗ «Об уполномоченных по защите прав предпринимателей в Российской Федерации»: научно-практический (постатейный). М.: КОНТРАКТ, 2014. 56 с.

44. Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 г. № 146-ФЗ // Собрание законодательства РФ. - 1998. - N 31. Ст. 3824.

45. Нефедова О.Ю. Применение арбитражными судами положений статьи 31 Арбитражного процессуального кодекса Российской Федерации // Арбитражные споры. 2015. N 3. С. 87 - 95.

46. Николаева Т.А. Правовое регулирование экономической деятельности в Российской Федерации // Конституционное и муниципальное право. 2015. № 12. С. 24-26.

47. Новиков В. А. Неприкосновенность частной жизни как конституционное право и объект уголовно-правовой охраны // Юридический мир. 2014. N 7. С. 18 - 21.

48. О гражданских и политических правах: Международный Пакт от 16.12.1966 // Бюллетень Верховного Суда РФ. 1994. N 12.

49. О защите прав человека и основных свобод: Конвенция Совета Европы (Заключена в г. Риме 04.11.1950) (с изм. от 13.05.2004) // Бюллетень международных договоров. 2001. № 3.

50. Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации: Постановление Правительства РФ от 15.09.2008 N 687 // Собрание законодательства РФ. 22.09.2008. № 38. Ст. 4320.

51. Определение Верховного Суда Российской Федерации от 28 ноября 2018 г. №301-АД18-19101 // Текст документа не был опубликован - СПС «Консультант Плюс».

52. Определение Саратовского областного суда от 25 июня 2019 года по делу №33-4572 // Текст документа не был опубликован - СПС «Консультант Плюс».

53. Памятники русского права. Вып. 1: Памятники права Киевского государства X-XII вв. / под ред. С.В. Юшкова; сост. А.А. Зимин. М.: Госюриздат, 1952.

54. Петрухин И.Л. Личные тайны (человек и власть). М., 1998. С. 8; Пермяков М.В. Исторические предпосылки возникновения категории «тайна» // Ленинградский юридический журнал. 2012. № 4 (30). С. 23 21)

55. Политика Конфиденциальности AliExpress URL:https://sell.aliexpress.com /ru/__pc/Zj6CxW2d6V.htm?spm=5261.ams_95368.0.0.2a4f2089VpRRIe (дата обращения: 13.06.2021).

56. Политика ООО "Интернет Решения" в отношении обработки персональных данных URL:https://docs.ozon.ru/common/attachments/personal_data_ooo_internet_resheniya.pdf (дата обращения: 13.06.2021).

57. Политика ООО «Вайлдберриз» в отношении конфиденциальности персональных данных URL:https://images.wbstatic.net/oferta/politika-konfidentsialnosti-wildberries.pdf (дата обращения: 13.06.2021).

58. Положение о политике конфиденциальности ООО «М-Инвест» URL:https://www.xcom-shop.ru/pages/privacy_policy/ (дата обращения: 13.06.2021).

59. Попондопуло В. Ф. Коммерческое (предпринимательское) право. М., 2003. С. 217.

60. Постановление Верховного Суда Российской Федерации от 28 июня 2018 г. N 74-АД18-11 // Текст документа не был опубликован - СПС «Консультант Плюс».

61. Постановление Московского городского суда от 3 августа 2017 г. N 4а-2675/2017 // Текст документа не был опубликован - СПС «Консультант Плюс».

62. Постановление Первого арбитражного апелляционного суда от 20 июня 2018 г. по делу N А11-5722/2018 // Текст документа не был опубликован - СПС «Консультант Плюс».

63. Постановление Пленума Верховного Суда РФ от 25.12.2018 N 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» от 25.12.2018 №46 URL:http://www.consultant.ru/document/cons_doc_LAW_314616/#dst100014 (дата обращения: 13.06.2021).

64. Постановление Правительства РФ от 16.03.2009 N 228 (ред. от 28.12.2020) "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций" http://www.consultant.ru/document/cons_doc_LAW_85889/ (дата обращения: 13.06.2021).

65. Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 // Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257

66. Постановлении Девятого Арбитражного Апелляционного суда от 02 марта 2018 года №09АП-4283/2018 по делу N А40-173100/17 // Текст документа не был опубликован - СПС «Консультант Плюс».

67. Постановлении Пленума Верховного Суда РФ и Пленума Высшего Арбитражного Суда РФ от 1 июля 1996 г. № 6/8 «О некоторых вопросах, связанных с применением части первой Гражданского кодекса Российской Федерации» // Текст документа не был опубликован - СПС «Консультант Плюс».

68. Правовое обеспечение конфиденциальности информации в условиях развития информационного общества. Камалова Г.Г. автореферат диссертации на соискание ученой степени кандидата юридических наук / Институт государства и права РАН. Москва, 2020

69. Правовые проблемы совершенствования защиты интеллектуальной собственности в РФ Чертакова Е.М. // Карельский научный журнал. 2014. № 4 (9). С. 24-26.

70. Предпринимательское право: учебник для студентов вузов, обучающихся по направлениям "Юриспруденция" и "Экономика"; по научной специальности 12.00.03 "Гражданское право; предпринимательское право; семейное право; международное частное право" / [Н. Д. Эриашвили, Н. М. Коршунов, А. В. Тумаков и другие] ; под ред.: Н. Д. Эриашвили [и другие]. - 7-е изд., перераб. и доп. - Москва : ЮНИТИ : Закон и право, 2020. - 495 с.

71. Приказ N 21 от 18 февраля 2013 г. Федеральной Службы по Техническому и Экспортному Контролю «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» URL:http://www.consultant.ru/document/cons_doc_LAW_146520/ (дата обращения: 13.06.2021).

72. Приказ №274 от 15 марта 2013 г. Федеральной службы ко

надзору в сфере связи, информационных технологий и массовых коммуникаций
URL:http://www.consultant.ru/document/cons_doc_LAW_145512/2ff7a8c72de3994f30496a0ccbb1ddafdaddf518/ (дата обращения: 13.06.2021).

73. Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 378 г. Москва "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности" URL: https://rg.ru/2014/09/17/zashita-dok.html (дата обращения: 13.06.2021).

74. Проблемы гармонизации экономических отношений и права в цифровой экономике : Harmonization of economic relations and law in the digital economy : монография / [Андреев Владимир Константинович, Белых Владимир Сергеевич, Беляева Ольга Александровна и другие] ; ответственные редакторы В. А. Вайпан, М. А. Егорова ; Московский государственный университет им. М. В. Ломоносова, Международный союз юристов и экономистов (Франция) [и другие]. - Москва : Юстицинформ, 2020. - 279 с.

75. Программа "Успех": мониторинг результатов освоения образовательной программы. Бурлакова И.А., Клопотова Е.Е., Ягловская Е.К. // Психологическая наука и образование www.psyedu.ru. 2011. № 1. С. 190-200. 5)

76. Салиева Р.Н. Конституционно-правовые гарантии защиты прав субъектов предпринимательской деятельности при осуществлении государственного контроля (надзора) // Государственная власть и местное самоуправление. 2013. № 9. С. 29-31.

77. Семейный кодекс Российской Федерации от 29.12.1995 №223-ФЗ

(ред. от 30.12.2015). // «Российская газета», №17, 27.01.1996.)

78. Скворцова Т.А., Смоленский М.Б. Предпринимательское право: учебное пособие / под ред. Т.А. Скворцовой. М.: Юстицинформ, 2014. 402 с.

79. Словарь иностранных слов: актуальная лексика, толкования, этимология // под ред. Н. С. Арапова, Р. С. Кимягарова и др. М., 1999. С. 160; / Ожегов С. И. Указ. соч. С. 447. 1)

80. Собрание законодательства Российской Федерации, 2006, N 31, ст. 3451; 2009, N 48, ст. 5716; N 52, ст. 6439; 2010, N 27, ст. 3407; N 31, ст. 4173, ст. 4196; N 49, ст. 6409; 2011, N 23, ст. 3263; N 31, ст. 4701

81. Стригунова Д.П. О правовом статусе индивидуального предпринимателя // Юрист. 2015. № 9. С. 22-27.

82. Сюбарева И.Ф. Совершенствование правового регулирования деятельности, связанной с получением дохода, и ответственности учреждений // Юрист. 2015. № 13. С. 41 46.

83. Терещенко Л. К. Отдельные вопросы применения законодательства о персональных данных // Комментарий судебной практики / под ред. К. Б. Ярошенко. М.: КОНТРАКТ, 2014. Вып. 19. С. 3 - 13. 36), 32 37

84. Тихомирова Л.В., Тихомиров М.Ю. Индивидуальный предприниматель: Комментарии, судебная практика, официальные разъяснения / под общ. ред. Тихомирова М.Ю. М.: Издательство Тихомирова М.Ю., 2014. 125 с.

85. Толмачева О.В. Индивидуальный предприниматель или общество с ограниченной ответственностью // Теоретические и практические аспекты развития современной цивилистической науки. Сборник научных трудов. Под ред. К.В. Бельгисовой, И.В. Петрова. Краснодар, 2014. С. 106-111.

86. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ // Собрание законодательства РФ. 1996. N 25. Ст. 2954

87. Указ Президента РФ от 10.09.2012 N 1276 «Об оценке эффективности деятельности руководителей федеральных органов

исполнительной власти и высших должностных лиц (руководителей высших исполнительных органов государственной власти) субъектов Российской Федерации по созданию благоприятных условий ведения предпринимательской деятельности» // Собрание законодательства РФ. 2012. N 38. Ст. 5068.

88. Указание ЦБ РФ от 10.12.2015 N 3889-У "Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных" URL: https://minjust.consultant.ru/documents/18554 (дата обращения: 13.06.2021).

89. Урванцева Е.В. Проблемы законодательного регулирования административного контроля и надзора за деятельностью индивидуального предпринимателя // Закон и право. 2014. № 2. С. 125-127.

90. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ от 27 июля 2006 года N 152-ФЗ URL: http://www.consultant.ru/ document/cons_doc_LAW_61801/ (дата обращения: 13.06.2021).

91. Федеральный закон №216-ФЗ «О внесении изменений в статьи 183 и 320 Уголовного кодекса Российской Федерации» URL:http://www.consultant.ru/document/cons_doc_LAW_386904/ (дата обращения: 13.06.2021).

92. Федеральный закон от 05.04.2010 г. N 40-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросу поддержки социально ориентированных некоммерческих организаций» // Собрание законодательства РФ. 2010. N 15. Ст. 1736.

93. Федеральный закон от 05.04.2013 N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» // Собрание законодательства РФ. 2013. N 14. Ст. 1652.

94. Федеральный закон от 08.08.2001 г. № 134-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при проведении

государственного контроля (надзора)» // Собрание законодательства РФ. 2001. N 33 (часть I). Ст. 3436.

95. Федеральный закон от 20.02.1995 №24-ФЗ «Об информации, информатизации и защите информации» (от 06.07.2016 N 374-ФЗ). // «Российская газета», №39, 22.02.1995. 35)

96. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 13.06.2021).

97. Федеральный закон от 24.07.2007 N 209-ФЗ «О развитии малого и среднего предпринимательства в Российской Федерации» // Собрание законодательства РФ. 2007. N 31. Ст. 4006.

98. Федеральный закон от 26.07.2006 N 135-ФЗ «О защите конкуренции» // Собрание законодательства РФ. 2006. N 31 (1 ч.). Ст. 3434.

99. Федеральный закон от 28.12.2009 г. № 381-ФЗ «Об основах государственного регулирования торговой деятельности в Российской Федерации» // Собрание законодательства Российской Федерации. 2010. № 1. Ст. 2.

100. Федеральный конституционный закон от 21.07.1994 № 1-ФКЗ (ред. от 14.12.2015) «О Конституционном Суде Российской Федерации» // Собрание законодательства РФ. 1994. N 13. Ст. 1447

101. Фроловский Н.Г. Управление предпринимательскими корпорациями в Российской Федерации (правовой аспект): Дис. ... канд. юрид. наук. Белгород, 2004. С. 47.

102. Чорновол Е.П. Головизнин А.В. Нормативно-правовые, доктринальные и правоприменительные признаки предпринимательской деятельности // Право и экономика. 2016. № 1 (335). С. 16-22.

103. Шишмарева Т.П. Соотношение процедур ликвидации и прекращения правоспособности юридического лица // Законы России: опыт, анализ, практика. 2015. N 6. С. 51 - 55.

104. Яковлев В.Ф. Россия: экономика, гражданское право (вопросы теории и практики). М.: РИЦ ИСПИ РАН, 2000. С. 165.

105. Якушев В.С. О понятии правового института // Правоведение. 1970. №6. С. 62-63.

106. Chart of signatures and ratifications of Treaty 213 Protocol No. 15 amending the Convention for the Protection of Human Rights and Fundamental Freedoms Status as of 13/06/2021 URL:https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/213/signatures?p_auth=oEd8WFmG (дата обращения: 13.06.2021).

107. Danton de Rouffignac, Peter. Doing business with Eastern Europe : A handb. for the 1990s / Peter Danton de Rouffignac. - London : Pitman, 1991. - XVII, 237 c.

108. Global and transnational business : Strategy a. management / George Stonehouse, Jim Hamill, David Campbell, Tony Purdie. - Chichester [etc.] : Wiley, Cop. 2000. - XVI, 463 c.

109. Hardy, Len. Successful business operations : How to develop a. exploit competitive advantage / Len Hardy. - Oxford; Cambridge (Mass.) : Blackwell, 1990. - XVI, 321 c.

110. Harrison, Andrew L. International business : Global competition from a Europ. perspective / Andrew L. Harrison, Ertuğrul Dalkiran, Ena Elsey. - Oxford : Oxford univ. press, 2000. - XXVII, 491 c.

111. Lazonick, William. Business organization and the myth of the market economy / William Lazonick. - Cambridge etc. : Cambridge univ. press, 1991. - XIV, 372 c.

112. Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment (1 April 2015). [Электронный ресурс] - Электр. дан. - Заглавие с экрана. URL: https://wcd.coe.int/ViewDoc.jsp?id=2306625 (дата обращения 13.06.2021).