МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
федерации федеральное государственное автономное образовательное
учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ГОСУДАРСТВА И ПРАВА
Кафедра трудового права и предпринимательства

Заведующий кафедрой,
доктор юрид.наук, доцент
Л.В. Зайцева

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
магистра

«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА: НА МАТЕРИАЛАХ ПРАКТИКИ»

40.04.01 «Юриспруденция»
магистерская программа «Корпоративный юрист»

Выполнил работу
студент 3 курса
заочной формы обучения
Сафронов Кирилл Сергеевич

Научный руководитель
канд. юрид. наук, доцент
Чикирева Ирина Павловна

Рецензент
канд. юрид. наук,
Начальник управления финансов и организационно-правовой работы
Департамента по общественным связям, коммуникациям и молодежной политике Тюменской области
Пермяков Антон Викторович

Тюмень
2020 год

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

	Нормативные правовые акты
Конвенция, Конвенция 1981 года	Конвенция о защите физических лиц при автоматизированной обработке персональных данных, заключенная в г. Страсбурге 28 января 1981 г.
Общий Регламент о защите персональных данных, Регламент	Регламент Европейского парламента и совета Европейского союза "О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)" N 2016/679, принятый в г. Брюсселе 27 апреля 2016 г.
ГК РФ	Гражданский кодекс Российской Федерации
ГПК РФ	Гражданский процессуальный кодекс Российской Федерации
КоАП РФ	Кодекс Российской Федерации об административных правонарушениях
НК РФ	Налоговый кодекс Российской Федерации
ТК РФ	Трудовой кодекс Российской Федерации
УК РФ	Уголовный кодекс Российской Федерации
Закон о коммерческой тайне	Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне"
Закон о персональных	Федеральный закон от 27.07.2006 N 152-ФЗ "О

данных, 152-ФЗ	персональных данных"
Методические рекомендации	Методические рекомендации по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения, утвержденные Приказом Роскомнадзора от 30.05.2017 N 94
Разъяснения Роскомнадзора об обработке персональных данных работников	разъяснения Роскомнадзора от 14.12.2012 "Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве"
Положение	Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённые Постановлением Правительства РФ от 17.11.2007 № 781.

Органы и организации

ООН	Организация объединенных наций
ЕС, Евросоюз	Европейский союз
Минкомсвязь России	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Минэкономразвития России	Министерство экономического развития Российской Федерации
Роскомнадзор	Федеральная служба по надзору в сфере связи,

	информационных технологий и массовых коммуникаций
ФНС России	Федеральная налоговая служба
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСС России	Фонд социального страхования Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю

Прочие сокращения

ПД	Персональные данные
ИНН	идентификационный номер налогоплательщика
СКУД	система контроля управления доступа
СНИЛС	страховой номер индивидуального лицевого счета

ВВЕДЕНИЕ

В последнее время в нашем обществе технологии совершенствуются каждый день, молниеносного изменяясь, а потоки ценной информации, в особенности персональных данных работников, которые представляют собой огромную ценность для тех, кто сможет ими воспользоваться остаются без надлежащей правовой защиты.

Однако, мы не можем не следовать за прогрессом и должны своевременно и эффективно отвечать на те вызовы, которые представляют нововведения, которые коснулись всех сфер человеческой жизни, в особенности трудовых, и иных связанных с ними отношений.

В наш век, когда технологии окружают все и всех на каждом шагу в распоряжении работодателя, имеется огромный инструментарий для отслеживания эффективной деятельности его работников, к таким инструментам можно отнести и видеонаблюдение рабочего процесса, и контроль звонков офиса, переписка и иная деятельность работников, которая осуществляется с корпоративных устройств, тщательное отслеживание всего что касается посещения интернет-страниц в рабочее время. Многие работодатели предпринимают попытки оптимизировать и автоматизировать все процессы, связанные с персоналом. Все это привело к созданию огромного количества баз данных, которые содержат в себе личные дела каждого из работников, которые в свою содержат различную информацию и персональные данные сотрудников.

Конечно, такие масштабные изменения привели к возникновению большому количества законодательных актов, регулирующих отношения, связанные с обработкой и защитой информации в целом и персональных данных в частности.

Повсеместное использование информационных технологий и преимуществ, которые предоставляет возможность практически беспрепятственного доступа к любой информации обеспечивают обществу реализацию права на свободу информации, однако при этом серьезно повышают риск несанкционированного

доступа к личной информации.

Предоставление личной информации должно быть правом каждого человека и зависит исключительно от его воли. Однако, зачастую возникают ситуации, когда представление такой информации необходимо, например при трудоустройстве, поскольку каждый соискатель обязан донести до работодателя персональную информацию исходя из положений, закрепленных Трудовым кодексом Российской Федерации.

В процессе трудоустройства гражданин представляет документы и заполняет анкеты, содержащие разделы, связанные не только с профессиональной деятельностью, но и с аспектами личной жизни человека.

Каждый работодатель имеет непосредственное желание получить различную информацию о потенциальном работнике, которая может повлиять на его решение и не разграничивает информацию о личной жизни человека и информацию, которая непосредственно характеризует человека как работника, оценивая его профессиональные качества, уровень его компетенции или качества его образования.

Трудности с определением допустимой степени вмешательства и пределов посягательств на частную жизнь работника затрудняют применение правил, регулирующих правила обработки и распространения информации в сфере труда, и нередко приводят к совершению правонарушений или уголовно наказуемых преступлений.

Персональные данные, которые обрабатываются работодателями, прежде всего, призваны идентифицировать человека в качестве работника, и служат работодателем для определения требуемых ему компетенций, кроме того такие данные, необходимы работодателем для исполнения иных функций, например уплата обязательных платежей возмещение льгот и гарантий со стороны государства, таким образом любой из работников предполагает в некоторой степени вмешательство в его частую жизнь отношении той информации, которая находится в распоряжении работодателя как оператора персональных данных работника.

При этом современное правовое регулирование требует от работодателя, как оператора персональных данных, неукоснительно соблюдать требования, установленные действующим законодательством РФ с целью безопасной обработки и сохранности личных данных работника.

Важность правового регулирования обработки персональных данных работников определяется тем, что, данном этапе развития трудовых отношений, работодателю необходимо предоставить не только гарантию неразглашения от других сотрудников своей организации в адрес третьих лиц информации, связанной с трудовой деятельностью, а также обеспечить качественную программную техническую и физическую защиту прав работников на сохранность личной информации сотрудников при ее хранении.

Многие из ученых (Бачило, Л. А. Волкова О.П.., В. Л. Глотова, М. В. Лушникова, и другие) занимались решением проблем, возникающих в процессе регулирования обработки персональных данных работников, однако этот вопрос остается недостаточно изученным в силу того, что развитие информационной отрасли постоянно и динамично.

Объектом настоящей магистерской диссертации являются отношения, связанные обработкой персональных данных в трудовых и иных связанных с ними отношениях.

Предметом исследования являются положения трудового законодательства, практики его применения и перспективы развития такого применения, для исследования был также проанализирован ряд теоретических положений, касающихся нормативного регулирования отношений по защите персональных данных и личной информации работников, которые определяют виды персональных данных, подходы к понимаю, что является персональными данным, при каких условиях и с учетом каких принципов должна производится их обработки, что понимается под обработкой персональных данных, каким правилам должны следовать работодателя выполняя функции оператора персональных данных, а также каким образом должна быть определена ответственность за неисполнение требований, по обработке персональных

данных.

Целью исследования был определён подробный аналитический разбор правовых норм и судебной практики РФ и зарубежных стран, регулирующей защиту персональных данных работников, для разработки универсальных методических рекомендаций для работодателей по повышению эффективности правового механизма защиты ПД и предохранения работодателей от нарушения законодательства.

Для достижения этой цели был поставлен и разрешен ряд задач:

- проведено исследование исторического аспекта формирования и развития института персональных данных в зарубежных странах и РФ;

- раскрыто понятие «персональные данные» и «персональные данные сотрудника, работника» и их восприятие и различие в подходе различных исследователей;

- детально изучены требования действующего законодательства, которые необходимо соблюдать при обработке персональных данных в трудовых отношениях, подготовлен анализ характеристик сбора, накопления, хранения, использования и передачи персональных данных работников;

- Исследована различная практика судов РФ, международных правовых актов, а также практика уполномоченных органов РФ по привлечению работодателей к ответственности за нарушение требований к обеспечению сохранности персональных данных;

- подготовлен ряд универсальных практических рекомендаций для работодателей для обеспечения правильной и безопасной обработки персональных данных.

В качестве методологической основы были использованы различные научные методы, в их числе – исторический, метод аналогии, синергетический, системный, метод анализа и синтеза диалектический, сравнительно-правовой, формально-правовой.

Эмпирическую основу составили, законы и постановления, судебные акты судов РФ, научные работы правового и исторического характера различных

авторов, материалы семинаров и научных статей.

Научная новизна диссертации, по нашему мнению, заключается в том, что были выявлены и проанализированы с практической стороны существующие проблемы, касающиеся правового регулирования персональных данных в трудовых и иных связанных с ними отношениях.

Работа может быть также использована в практическом значении, в частности, результаты исследования можно использовать для утверждения универсальных методических рекомендаций для работодателей-операторов персональных данных и органов, осуществляющих государственный контроль и надзор за обработкой персональных данных с целью организации на предприятиях системы обеспечения правильной и безопасной обработки персональных данных.

Апробация результатов исследования проводилась путем публикации научной статьи по теме «Организация системы защиты и ответственность за нарушение законодательства о персональных данных работников в условиях развития цифровых технологий. Сравнительный анализ российского и зарубежного опыта» в научном журнале Молодой ученый № 47 (337) за ноябрь 2020 г.

Содержание работы составляют: введение, три главы, заключение и библиографический список.

ГЛАВА 1. ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

1.1. История развития правового регулирования института персональных данных. Основные понятия и принципы в области защиты персональных данных работника

История развития законодательства о персональных данных насчитывает несколько десятилетий. Многие авторы, исследующие тему необходимости защиты персональных данных, начинают со знаменитой статьи «Право на Конфиденциальность» Сэмюэля Уоррена и Луиса Брандейса опубликованную 15 декабря 1890 года в гарвардском законодательном обозревателе «Harvard Law Review». Хотя эффект на развитие дискуссии о защите конфиденциальности данных этой статьи нельзя недооценивать, это не означает, что до 1890 года не было никаких дискуссий о вторжениях в частную жизнь. Как показывает Уэстин в своих публикациях, в XV веке слово "приватность" уже использовалось в Англии, и исторические исследования показывают, что колонисты в Новой Англии уважали приватность по отношению к дом человека, его семья и даже право на конфиденциальность его переписки. Кроме того, известно, что уже в 1790 году существовала оппозиция против первой переписи населения США, хотя правительство требовало немногим больше, чем перечисление лиц, как рабов, так и свободных. [Дмитрик, с. 45].

Это возражение привело к тому, что в 1840 году переписчикам были даны инструкции о том, что индивидуальные данные должны рассматриваться как конфиденциальные. Было высказано опасение, что гражданин не был должным образом защищен от опасности того, что частные дела или семейные тайны будут раскрыты перед судом.

Однако с 1890 года связь с использованием технических средств становится очевидной. Как упоминалось в статье Уоррена и Брандейса, использование мгновенных фотографий делает возможной публикацию в

различных целях без согласия отдельного лица. Классическим видом вторжения в частную жизнь является использование без согласия человека фотографии для продвижения продукта. Важным считается дело «Roberson v. Rochester Folding Box Co» которая поразила Юридический мир Нью-Йорка. В этом деле местная компания-производитель муки решила использовать фотографию Эбигейл Рочестер, очаровательной и привлекательной девушки, чтобы продвигать свой продукт. По этой причине блестящий лозунг «Мука вашей семьи» был использован вместе с фотографией и помещен в многочисленных магазинах, складах и салунах. Абигейл заявила о своем "праве на частную жизнь" и подала иск на сумму 15 000 долларов. Нью-Йоркский суд отклонил иск, заявив, что ее иск не имеет права на основании того, что праву еще неизвестно, что было нарушено. Это решение вызвало большое удивление и оказало сильное влияние на последующие судебные дела, в частности, особенно спустя три года Pavesich v. New England Life Insurance Co. В этом судебном деле фотография Паоло Павесича была использована, также без его согласия, компанией по страхованию жизни для рекламы.

На фотографии был изображен здоровый мужчина, который якобы купил полис страхования жизни, в отличие от больного человека, который не сделал и предположительно не мог сделать такую «бесценную» покупку для своей будущей безопасности. Под портретом Певесича была надпись: “в мой здоровый и продуктивный период жизни я купил страховку в компании New England Life Insurance Co. из Бостона Массачусетс, и сегодня моя семейная жизнь защищена.” Павесич, по сути, никогда не покупал такую страховку жизни и не делал никаких подобных заявлений. Он счел рекламу отвратительной и подал иск о возмещении ущерба в размере 25 000 долларов. В этом случае право на неприкосновенность частной жизни было единогласно признано. Суд признал необходимость страховой компании возместить убытки за вторжение в частную жизнь Павесича Это был сильный прецедент именно для одного аспекта личной неприкосновенности: несанкционированного использования фотографии человека.

С начала 30-х годов XX века в ряде европейских Конституций уже установлены правила защиты личной и семейной информации, в пример можно привести Конституции Исландии в 1944 и Ирландии в 1937. [Российский ежегодник трудового права, с. 156-183]

Затем в 1948 году была Принята Всеобщая декларация прав человека, включающая 12-е основное право, то есть право на неприкосновенность частной жизни.

Исследовательские проекты в области защиты информации от незаконного доступа и неправомерного использования появились в 60-70-х годах двадцатого века и, прежде всего возникли вследствие первых компьютерных технологий и началом их использования в процессе обработки данных.

Тогда же зарождается одно из первых национальных правовых регулирований персональных данных. В его основу были положены идем Всеобщей декларации прав человека принятой Генеральной Ассамблеей Организации Объединённых Наций в 1948 года в которой было закреплено, что никто не может быть подвергнут произвольному вмешательству в личную и семейную жизнь человека, и что такое вмешательство наносит ущерб его чести и репутации, а статья 23 декларации провозглашает право на труд, свободный выбор работы, справедливые и благоприятные условия труда и защиту от безработицы.

В совокупности это означало, что в трудовых отношениях, в отношении вопросов личной и семейной жизни, защиты чести и достоинства личности люди находятся под защитой государства.

Кроме того, в вопросе нормативных актом между народного права, защищающих права и свободы человека, его личную жизнь, подготовленных в рамках Организации Объединённых Наций, стоит также остановится на Международном пакте о гражданских и политических правах от 19 декабря 1966 года, согласно положениям которого никто не может подвергаться

произвольному вмешательству в его личную жизнь. Каждый человек имеет право на защиту от такого вмешательства или агрессии. [Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С. с. 22]

В 1967 году в США вступает в силу Закон о свободе информации (FOIA) и дает каждому право запрашивать доступ к документам у государственных органов. Другие страны следуют этому примеру.

Стоит также обратить внимание, что первый в мире специальный закон «О защите персональных данных» был принят в 1970 году в немецкой Федеральной земле Гессен.

Далее в 1980 Организация экономического сотрудничества и развития издает принципы по защите данных, отражающие все более широкое использование компьютеров для обработки деловых операций.

В 1981 Совет Европы принимает конвенцию о защите данных, в соответствии с которой право на неприкосновенность частной жизни является юридическим императивом, появляются правило автоматизированной обработки персональных данных, а также был разработан протокол к Конвенции, затрагивающий вопросы организации работы наблюдательных органов и вопросов трансграничной передачи персональных данных. [Кухаренко Т.А., Захарова Н.А. с. 45]

После этого, в 1983 Федеральный Конституционный суд Германии выносит основополагающее решение в отношении решения о переписи населения. Вердикт считается важной вехой в защите данных.

В 1993ем было рассмотрено дело в котором некий мистер П.К Браун был обвинен в нарушении закона Великобритании о защите данных 1984 года за использование персональных данных или целей, отличных от описанных в реестре защиты данных, однако в дальнейшем решение было отменено.

24го октября 1995 года была принята директива 95/46/EC о защите прав частных лиц в отношении обработки персональных данных , позднее была принята и закреплена Директива 97/66/EC от 15 декабря 1997 года, касающаяся

использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций. [Пищита А.Н., Гончаров Н.Г., с. 33]

И в 2015 году ООН опубликовала рекомендации, в которых описаны принципы, которым должны следовать в своем национальном законодательстве в отношении обработки персональных данных сотрудников и кандидатов на рабочем месте, например, в отношении данных здоровья или мониторинга использования связи на рабочем месте. Эти рекомендации направлены на решение проблем конфиденциальности, связанных с новыми информационно-коммуникационными технологиями.

В целом, это время можно определить как период интенсивных исследований и законодательства о защите конфиденциальности в области сбора и использования личных данных. Некоторые страны приняли законы, которые касаются только компьютеризированных методов защиты персональных данных. Другие государства подошли с более широких позиций, не ограничиваясь конкретными типами технологий обработки данных.

Нормативное регулирование персональных данных в западных странах значительно превзошло российскую нормативную практику.

Исторически, правовую систему в отношении персональных данных можно было характеризовать как испытывающую особые трудности с закреплением и декларированием прав на неприкосновенность частной жизни и ограничениями на распространение информации об этом, поскольку ходом исторического развития Национального общества и государства с 1917 года было постоянное господство государства над человеком. Вопросы и проблемы защиты личной информации и персональных данных в тот период освещены не были.

Главной задачей постсоциалистического российского права было создание института защиты прав и свобод человека и гражданина, устанавливающего границы допустимого вмешательства в личную жизнь человека в осуществление его личной свободы.

Исследования личной свободы, частной жизни начали свое развитие в 80-х годах XX века и проводились в рамках науки о гражданском праве, теории права, конституционного права, международного права и других отраслей права. Научное направление, охватывающее все вопросы регулирования отношений в отношении персональных данных, является отдельным институтом защиты персональных данных в рамках информационного права.

Главные идея в этих исследованиях заключается в том, что эта правовая конструкция проистекает из прав человека, содержащихся в источниках международного права. Поэтому О. Волкова, исследуя доступ к персональным данным работника в сфере трудовых отношений, начинается с изучения основных правил и базовых о персональных данных и прав субъектов персональных данных, которые появились впервые в современной истории в Всеобщей декларации прав человека (1948), Европейской Конвенции о защите прав человека и основных свобод (1950), Международный пакт о гражданских и политических правах (1966 год) и другие международные документы. [Волкова, с. 2]

Последующие вехи в эволюции науки, связанной с информационным правом, было обусловлено факторами исторического развития РФ как государства, к которым можно отнести: более позднее распространение компьютерных технологий и относительно недавним освобождением от государственной цензуры.

В нашей стране основные права и свободы человека и гражданина, в том числе и те, что касались сферы информационной излагались в Конституции РФ, принятой всенародным голосованием в 1993 году, согласно части 1 статьи 23 Конституции РФ, каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, а в статье 24 указано, что сбор, хранение и распространение информации о личной жизни лица без его согласия не допускается.

В течение длительного периода времени до 2006 года Федеральный закон Российской Федерации от 20.02.1995 года "Об информации, компьютеризации и

защите информации" был основным источником, консолидирующим правовые основы информационного оборота в России, персональные данные отнесены к конфиденциальной информации.

В будущем, быстрое развитие отношений по поводу распространения информации привело к новым юридическим проблемам в информационной сфере, которые трудно было предсказать в 1995 году. Например, закон не в полной мере учитывал возможности "компьютерной революции" и защиты персональных данных в условиях автоматизированной обработки.

Изначально в российской правовой системе вопросы защиты персональных данных регулировались отраслевым законодательством, которое не отличалось согласованностью.

Первый шаг в создании правового регулирования института персональных данных лица был сделан в 2001 году, когда Российская Федерация ратифицировала Конвенцию о защите физических лиц.

Ратификация послужила отправной точкой для разработки Закона о персональных данных.

На нынешнем этапе происходит европейская модернизация законодательство о защите персональных данных, направленное на укрепление региональной интеграции. В частности, разрабатывается проект модернизации основного документа Совета Европы - "Конвенции о защите физических лиц при автоматизированной обработке персональных данных".

В данный момент Европейский союз рассматривает проект нового закона о прямых действиях по защите персональных данных (в обмен на директивы, которые были реализованы путем адаптации и включения его положений в национальное законодательство). Он включает требование о том, чтобы организации уведомляли об утечках персональных данных в течение 24 часов. Компаниям, нарушающим закон, грозит штраф в размере до 4% от их мирового оборота. Закон установит единый набор правил для европейских компаний и компаний за пределами Европы, если они предлагают свои услуги в Европейском Союзе.

Как было отмечено ранее, Федеральный закон о персональных данных № 152-ФЗ определяет персональные данные как любую информацию, относящейся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

При этом вышеизложенное определение не позволяет в полном мере дать точный ответ что является персональными данными, а что нет, что кроме всего прочего подтверждается позицией Роскомнадзора, который в своем комментарии, указывает что, «при буквальном толковании к понятию «персональные данные» можно отнести широкий круг информации. В частности, в нем нет указания на связь между прямой или косвенной определенностью или «определимостью» физического лица. Соответственно, отсутствует однозначное понимание того, в каких случаях собираемые и обрабатываемые данные будут относиться к персональным, а в каких – нет». [Буркова, с. 2]

Для представления, что такое персональные данные в трудовых отношениях, следует обратиться к статье 65 Трудового кодекса РФ, согласно которой определен перечень документов, необходимых для заключения трудового договора.

Таким образом, кроме паспорта, удостоверяющего личность работника, его трудовой книжки, свидетельства об обязательном пенсионном страховании, документов военного учета и образования законодатель предусматривает возможность подачи дополнительных документов на основании Трудового кодекса и других правовых актов.

Например, иностранец, который поступает на работу, вместе с документами, указанными в статье 65 Трудового кодекса Российской Федерации, у работодателя имеется разрешение на работу или патент, разрешение на временное проживание или вид на жительство (статья 327.3 трудового кодекса Российской Федерации).

Объем информации, получаемой работодателем работника во время найма, увеличивается на протяжении всей его трудовой деятельности.

В соответствии с положениями, закрепленными ч. 4 ст. 86 Трудового кодекса, работодатель не имеет права получать и обрабатывать информацию о работнике, относящуюся к особым категориям персональных данных, за исключением случаев, предусмотренных Трудовым кодексом РФ и другими федеральными законами.

Например, в соответствии со статьей 179 Трудового кодекса Российской Федерации при сокращении численности или численности работников с одинаковой производительностью и квалификацией предпочтение отдается оставлению на работе семьям, в которых имеются иждивенцы (два и более), в рассматриваемом случае предоставление работодателю сведений о семейном положении играет в пользу работника.

При обработке информации о состоянии здоровья будущего работника работодатель должен учитывать, что он не может превышать информацию, связанную с вопросом о возможности выполнения трудовой функции. Кроме того, информация о состоянии здоровья представляет собой медицинскую тайну, разглашение которой не допускается.

Перейдем к рассмотрению биометрических персональных данных, так статья 11 закона 152-ФЗ определяет биометрические персональные данные как сведения, характеризующие физиологические и биологические характеристики человека, на основании которых можно определить его личность и которые используются оператором для установления личности субъекта ПД.

Биометрические данные характеризуются особой чувствительностью, поскольку они неразрывно связаны с личностью работника, поэтому законодатель устанавливает особое требование для их защиты. [Кривоногов, с. 4]

На практике часто возникает вопрос, какую информацию можно отнести к биометрии. К примеру, согласно разъяснениям Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) биометрические данные включают физиологические данные (данные отпечатков пальцев, радужной оболочки глаза, анализ ДНК, рост, вес и

другие), а также другие физиологические или биологические характеристики человека, включая изображение человека (фотография и видеозапись), которые позволяют их идентифицировать и используются оператором для определения личности субъекта" . [Разъяснения Роскомнадзора от 02.09.2013]

Однако в научно-практическом комментарии, опубликованном в 2015 под редакцией зам. руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций году, высказывается иная позиция позицию в отношении присвоения фото - и видеоизображений биометрической информации в связи с тем, что при визуальной оценке фотография или видеоизображение лица, являющегося Близнецом или внешнее сходство которого с идентифицированным лицом очевидно, а также в случае пластических операций не позволит достоверно идентифицировать субъекта. [Приезживая, с. 29]

Таким образом, можно сделать вывод, что по-настоящему биометрическая обработка персональных данных предназначена только для тех работодателей, которые ввиду секретности своей деятельности организуют сложную систему прохода на территорию организации, включающую, например, сканирование сетчатки или считыватель отпечатков пальцев.

По нашему мнению, отсутствие единообразной интерпретации термина «биометрические данные» и, следовательно, понимание того, какие человеческие данные можно считать биометрическими, является неотложной проблемой, которую необходимо решить на законодательном уровне.

В ходе трудовых отношений работодатель обрабатывает персональные данные работников как компьютерными средствами, например путем ведения учета кадровых заказов в электронной базе 1С, так и без нее путем организации хранения личных файлов работников на бумаге. В обоих случаях обработка должна осуществляться в соответствии с принципами, установленными Федеральным законом 152-ФЗ.

Основные принципы обработки персональных данных перечислены в статье 5 Федерального закона № 152. Помимо общих принципов законности и

справедливости, на федеральном уровне устанавливается необходимость конкретного подхода к обработке персональных данных и недопустимость обработки, несовместимой с целью сбора персональных данных. Законодатель также отмечает, что содержание и объем обработанных персональных данных должны соответствовать заявленным целям обработки, а обработанные персональные данные не могут быть избыточными.

Следовательно, обработка персональных данных, выходящих за рамки назначенных целей, не допускается.

Согласно пункту 3 статьи 5 152-ФЗ запрещается объединение нескольких баз данных, в которых содержатся персональные данные, обрабатываемые в целях, несовместимых друг с другом. Анализируя этот принцип, можно сделать вывод о том, что работодатель обязан сортировать персональные данные работников и организовывать их хранение таким образом, чтобы при обработке конкретной категории получались персональные данные, соответствующие этой цели.

Важными представляются в этом ключе принципы точности, достаточности и актуальности персональных данных для целей их обработки. При этом в качестве достаточной определяется такая информация объем которой позволяет достигать целей обработки. Актуальность персональных данных означает, что во время обработки персональных данных последние являются своевременными, надежными и значимыми для достижения цели обработки.

Кроме того, пункт 6 статьи 5 Федерального закона № 152 прямо устанавливает обязательство оператора принимать необходимые меры для своевременной актуализации данных.

Представляется логичным, что данные о работнике могут измениться, например, работник может изменить фамилию или получить дополнительное образование. В соответствии с постановлением Министерства труда Российской Федерации от 10.10/2003 № 69 «об утверждении Инструкции по заполнению книг труда», изменения в записи книги о фамилии, имени, отчества производятся на основании паспорта, свидетельств о браке, расторжении брака, изменении

фамилии, имени, отчества и других документов и со ссылкой на их номер и дату. Поэтому работодатель должен своевременно знать об изменениях в документах, полученных от работника.

Однако действующее законодательство не дает работодателю права требовать от работника информации об изменениях в его персональных данных. В связи с этим некоторые ученые предлагают закрепить в статье 22 Трудового кодекса РФ право работодателя получать от работника информацию, связанную с выполнением его трудовой функции. По нашему мнению, предоставление такого права работодателю является нарушением конституционного принципа неприкосновенности частной жизни. Кроме того, работодатель имеет право, установить обязанность работника предоставлять информацию об изменениях в персональных данных с целью их уточнения и обновления.

1.2. Соотношение прав и обязанностей субъектов персональных данных и оператора в трудовых отношениях

Прежде всего в разборе соотношения субъекта работника и работодателя оператора, необходимо подчеркнуть, что работодатель в качестве оператора персональных данных должен обеспечить хранение документов, содержащих персональные данные надлежащим образом.

Целесообразно использовать доступные современные технические средства охраны, а для персональных данных, хранящихся в электронном виде, – программные средства защиты информации. Требования законодательства по обеспечению безопасности персональных данных при их обработке и хранении установлены Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённые Постановлением Правительства РФ от 17.11.2007 № 781.

Согласно ч. 2 п. 2 положения безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

Определены права самих работников. Так, они имеют право:

– на полную информацию об их персональных данных и обработке этих данных;

– на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника;

– на определение своих представителей для защиты своих персональных данных;

– на доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

– на требование об исключении или исправлении неверных или неполных персональных данных. При отказе работодателя исключить или исправить персональные данные работника последний имеет право заявить в письменной форме работодателю о своём несогласии, обосновав таковое.

Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

– на требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведённых в них исключениях, исправлениях или дополнениях;

Любой работающий не должен отказываться от своих прав на сохранение и защиту своей личной, семейной тайны (п. 9 ст. 86 ТК РФ). Работодатель обязан ознакомить под подпись работников и их представителей с документами, устанавливающими порядок обработки персональных данных работников, а также с их правами и обязанностями в этой области.

Руководитель организации (работодатель) как сторона трудового правоотношения обязан не только рационально использовать труд работников, справедливо оплачивать их труд в соответствии с вкладом, создавать безопасные условия труда, создавать условия, обеспечивающие участие работников в управлении организацией, но и обеспечивать безопасность персональных данных при их обработке и хранении. Виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном ТК РФ и иными федеральными законами, а также к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами, однако подробнее вопросы связанные

с ответственностью законодательства о персональных данных будут рассмотрены нами позднее.

Кроме того, в ст. 86 «Общие требования при обработке персональных данных работника и гарантии их защиты» ТК РФ установлено, что в целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

- обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

- при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, настоящим Кодексом и иными федеральными законами;

- все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

- работодатель не имеет права получать и обрабатывать сведения о работнике, относящиеся в соответствии с законодательством Российской Федерации в области персональных данных к специальным категориям персональных данных, за исключением случаев, предусмотренных настоящим Кодексом и другими федеральными законами;

- работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его

профсоюзной деятельности, за исключением случаев, предусмотренных настоящим Кодексом или иными федеральными законами;

- при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

- защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном настоящим Кодексом и иными федеральными законами;

- работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

- работники не должны отказываться от своих прав на сохранение и защиту тайны;

- работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников".

В ст. 88 «Передача персональных данных работника» ТК РФ закреплено, что при передаче персональных данных работника работодатель должен соблюдать следующие требования:

-не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных настоящим Кодексом или иными федеральными законами;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они

сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном настоящим Кодексом и иными федеральными законами;

- осуществлять передачу персональных данных работника в пределах одной организации, у одного индивидуального предпринимателя в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать персональные данные работника представителям работников в порядке, установленном настоящим Кодексом и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций".

В соответствии со ст. 89 ТК РФ в целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют следующие права.

Во-первых, право на полную информацию о своих персональных данных и обработке этих данных.

Согласно п. 8 ст. 86 ТК РФ работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

Порядок хранения и использования персональных данных работников устанавливается работодателем с соблюдением требований ТК РФ и иных федеральных законов (ст. 87 ТК РФ).

Работодателю необходим локальный акт для правового регулирования вопросов обработки персональных данных, в качестве которого может выступать положение о персональных данных. Отсутствие положения о персональных данных, равно как и неознакомление работников с таким положением, признается нарушением трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права, и влечет привлечение к административной ответственности по ч. 1 ст. 5.27 КоАП РФ.

Рекомендациями Роскомнадзора от 27.07.2017 года определены основные подходы к структуре и форме документа, определяющего политику оператора в отношении обработки ПД.

Прежде всего рекомендациями определены ключевые структурные компоненты, такие как:

- «Общие положения», данный раздел включает в себя основные понятия, основные права и обязанности оператора;

- «Цели сбора персональных данных», цели должны быть определены оператором в соответствии со своей деятельностью, определенной учредительными документами операторами, используемыми информационными системами и т.д.

- «Правовые основания обработки персональных данных», в качестве правовых основания обработки ПД выступают нормативные правовые акта, постановления правительства, приказы Роскомнадзора, уставные документы оператора, и т.д.

- «Объем и категории обрабатываемых ПД, субъекты персональных данных», здесь прежде всего отмечается, недопустимость сбора оператором избыточного количества персональных данных, которые не служат для достижения целей обработки. В качестве субъектов ПД определяются соискатели, работники, бывшие работники, клиенты и т.д.

- «Порядок и условия обработки персональных данных».

Данный раздел устанавливает порядок действий оператора по обработке персональных данных с конкретными субъектами, четкие сроки обработки, использование технических средств в обработке и другие, в том числе правила блокирования, удаления и порядок выполнение иных действий. [Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, с. 4]

На основании изложенного, в отношении документа определяющего политику по обработке ПД что прямых законодательных требований относительно его содержания на настоящий момент не установлено, приводимые рекомендации лишь определяют примерную его структуру и содержание и оператор-работодатель должен сам определять содержание документа, ориентируясь на категории ПД и субъектов, количество обрабатываемых данных и применяемые информационные системы и технические средства, а также на требования постановления правительства в отношении таких систем.

Во-вторых, право на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника.

В соответствии со ст. 62 ТК РФ такие документы работодатель обязан выдать работнику по его письменному заявлению не позднее трех рабочих дней со дня подачи этого заявления. При этом копии документов, связанных с работой, должны быть заверены надлежащим образом и предоставляться работнику безвозмездно.

В-третьих, право на определение своих представителей для защиты своих персональных данных.

В-четвертых, право на доступ к медицинской документации, отражающей состояние своего здоровья, с помощью медицинского работника по своему выбору.

Работник имеет право знакомиться с медицинской документацией, содержащей сведения о своем здоровье, а также может привлечь для исследования таких документов медицинского работника, выбранного по своему усмотрению.

В-пятых, исключение или исправление неверных или неполных персональных данных, а также данных, обработанных с нарушением требований ТК РФ или иного федерального закона. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения.

Требование об исключении или исправлении неверных или неполных персональных данных, а также обрабатываемых с нарушением работник вправе заявить в любой форме (устной или письменной). Если устное требование работодатель выполнить откажется, работнику целесообразно воспользоваться правом на подачу письменного заявления о несогласии с соответствующим обоснованием.

Например, если сведения неточные, то после подтверждения факта неточности на основании представленных сведений или документов у работодателя есть семь рабочих дней для уточнения персональных данных (ч. 2 ст. 21 Закона)

В-шестых, право на требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

В развитие права потребовать исключения или исправления недостоверных персональных данных работник наделяется правом требовать от работодателя оповестить всех лиц, которым ранее были сообщены неверные или неполные персональные данные, об их изменениях.

А также право на обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите персональных данных работника.

В силу п. 1 ч. 1 ст. 22 ГПК РФ и ст. 382, 391 ТК РФ дела по спорам, возникшим из трудовых правоотношений, подведомственны судам общей юрисдикции. Подсудность определяется по выбору истца - по его месту жительства или по месту нахождения работодателя (ч. 6.1 ст. 29 ГПК РФ).

ГЛАВА 2 ОСНОВЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ И ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ПРОЦЕССЕ ТРУДОВЫХ ОТНОШЕНИЙ

2.1. Отдельные особенности обработки персональных данных при трудоустройстве

Обработка персональных данных в трудовых отношениях - это непрерывный процесс, начинающийся с решения соискателя предложить свою кандидатуру тому или иному работодателю и предоставляющий ему необходимую информацию для найма, осуществляется на протяжении всего периода работы на предприятии: на испытательном этапе, при оценке выполненной работы, расчета и выплаты заработной платы, а также в иных непосредственно связанных процессах, которые продолжаются в том числе и после расторжения трудового договора.

В результате этой длительной процедуры возникают многочисленные вопросы права на применение, цель настоящей главы заключается в рассмотрении основных.

При этом, в процессе деятельности работодатель постоянно сталкивается с необходимостью найма персонала, в этой связи необходимо обраться к рассмотрению особенностей связанных с защитой персональных данных соискателей.

Обработка персональных данных в рамках трудовых отношений осуществляется без согласия работника.

Однако до заключения трудового договора трудовых отношений еще не возникло, а соискатель (субъект персональных данных) работником еще не является. Следовательно, обработка персональных данных соискателя должна осуществляться с его согласия.

В Разъяснениях Роскомнадзора об обработке персональных данных работников подробно рассмотрены вопросы обработки персональных данных соискателей.

В случае отказа в приеме на работу сведения, предоставленные соискателем, должны быть уничтожены в течение 30 дней, за исключением случаев, предусмотренных законодательством о государственной гражданской службе, где срок хранения персональных данных соискателя определен в течение 3 лет.

Получение согласия также является обязательным условием при направлении работодателем запросов в иные организации, в том числе по прежним местам работы, для уточнения или получения дополнительной информации о соискателе.

Исключение составляют случаи заключения трудового договора с бывшим государственным или муниципальным служащим. В соответствии со ст. 64.1 ТК РФ работодатель при заключении трудового договора с гражданами, замещавшими должности государственной или муниципальной службы, перечень которых устанавливается нормативными правовыми актами РФ, в течение 2 лет после их увольнения с государственной или муниципальной службы обязан в 10-дневный срок сообщать о заключении такого договора представителю нанимателя (работодателю) государственного или муниципального служащего по последнему месту его службы в порядке, устанавливаемом нормативными правовыми актами РФ.

Например, в соответствии со статьей 332 трудового кодекса Российской Федерации, заключению трудового договора предшествует избрание по конкурсу для замещения должности работника, связанным с работой в организации, которая осуществляет образовательную деятельность по реализации образовательных программ высшего образования и дополнительные профессиональных программ, предшествует избрание по конкурсу.

Таким образом, согласие заявителя на обработку его персональных данных, представленных для замены вакантного места в конкурсе, не требуется в связи с тем, что такая обработка напрямую закреплена на законодательном уровне.

В случае, когда заявителем является кадровое агентство, с которым лицо заключило договор, согласие на лечение его работодателя не запрашивается. Поскольку за защиту персональных данных заявителя отвечает соответствующее кадровое агентство, оно обязано предупредить работодателя о необходимости соблюдать конфиденциальность предоставленной информации.

В соответствии с пунктом 4 статьи 21 152-ФЗ, достигнув цели обработки персональных данных, оператор обязан прекратить обработку персональных данных, затем уничтожить их в срок, не превышающий 30 календарных дней с наступления даты достижения установленной цели обработки, в случае если ирное не предусмотрено федеральным законом.

В некоторых случаях при отборе кандидатов запрашивается информация о заявителе на его предыдущих рабочих местах в виде характеристики или рекомендации. Таким образом, работодатель имеет право запросить, а бывший работодатель может предоставить запрашиваемую информации, однако исключительно на основании письменного согласия лица, претендующего на вакантную должность. При этом законодательные требования не будут нарушены.

Однако требование о наличии согласия заявителя не может быть распространено на ситуации, когда трудовой договор заключается с бывшим муниципальным или государственным служащим.

В соответствии со статьей 64.1 трудового кодекса Российской Федерации работодатель, при заключении трудового договора с такими гражданами в течение двух лет после его увольнения с государственной или муниципальной службы, он обязан сообщить о заключении трудового договора работодателю в последнем месте работы, надлежащим образом, это необходимо для обеспечения контроля за соблюдением бывшими государственными и муниципальными служащими ограничений и запретов, установленных законодательством по борьбе с коррупцией.

Главной проблемой при предоставлении и обработке информации является ее актуальность и достоверность, в связи с этим некоторые работодателя могут проводить дополнительные проверки, в том числе с использованием полиграфа.

В действующем законодательстве нет установленного запрета на такие проверки, в отличие, например, от международно-правовых норм. Хотя проверка на полиграфе является добровольной и проводится на основе письменного согласия, кажется, пренебрежительное невнимание законодателя к вопросам регулирования такой процедуры, хотя бы только потому, что случаев вынесения незаконных дисциплинарных взысканий, увольнений и санкций для расторжения трудового договора зачастую связано с проверкой на полиграфе.

Между тем, в законодательства некоторых стран существует прямой запрет на проведение проверок на полиграфе, в качестве примера на такой запрет можно указать Онтарио в Канаде, или Новый Южный Уэльс в Австралии.

Существуют примеры стран, где использование полиграфа осуществляется в соответствии с федеральным законодательством, так, например, в 1988 году в США был принят закон, защищающий работников от использования работодателем полиграфа, в частности закон запрещает использование полиграфа при трудоустройстве, однако действует он только на частные негосударственные организации-работодателей.

В настоящее время существует ряд проблем в области применения полиграфа. Например, отсутствие регулирования проверок на полиграфе затрудняет и ограничивает его использование в правоохранительных целях, создавая при этом угрозу злоупотреблений в его использовании.

Также важно отметить, использование полиграфа для негосударственных организаций вызывает опасения, связанные с отсутствием комплексной утвержденной системы обучения и аттестации экспертов-полиграфологов, может способствовать возникновению нарушений личных прав работников вследствие проведения некомпетентных исследований

Таким образом, подводя итог вышеизложенному, считаем важным для развития современного законодательства о защите персональных данных

рассмотреть вопрос законодательного регулирования и принятия норм необходимых для защиты прав работников от злоупотреблений работодателей.

2.2. Отдельные особенности обработки персональных данных в период трудовой деятельности

После заключение договора согласие работника на обработку его персональных данных не требуется в силу закона, однако согласие работника необходимо в случаях, когда личные данные сотрудников передаются и обрабатываются третьими лицами.

Например, некоторые работодатели для обеспечения кадрового рабочего процесса заключают договор с внешними организациями на предоставление соответствующих услуг по обработке персональных данных по поручению работодателя.

При этом договор поручения должен быть указан перечень действий с личными данными работников, которые должны быть выполнены, закреплено обязательство организации, принимающей персональные данные работников, соблюдать конфиденциальность полученных данных и обеспечивать безопасность их обработки, а также указаны требования к защите обработанной информации. Роскомнадзор также ссылается на необходимость этих условий, объясняя практику привлечения внешних организаций к персоналу и бухгалтерского учета со стороны работодателя.

Необходимо согласие работника для организации деятельностей кредитных организаций, осуществляющих банковское обслуживание работодателя. В свою очередь при заключении договора с кредитными организациями есть несколько исключений. Согласие работников не требуется в случаях:

- если договор о выдаче банковской карты был заключен непосредственно с сотрудником;

- наличие у работодателя полномочий представлять интересы работника при заключении договора с кредитной организацией на выдачу банковской карты и ее последующее обслуживание;

- надлежащая форма и система вознаграждения указаны в коллективном договоре.

Между тем на практике нередко наблюдается несоблюдение работодателями установленных требований.

Еще одним важным обстоятельством, требующим письменного согласия сотрудника, является проведение видеонаблюдения на территории предприятия. В некоторых случаях видеозапись является обязанностью работодателя, например, в учреждениях здравоохранения и образования для обеспечения антитеррористической и противопожарной безопасности.

Некоторые работодатели могут организовать на предприятии системы тайного мониторинга, сотрудник, который подозревает, что он находится под тайным наблюдением, имеет право подать заявление в правоохранительные органы для проведения соответствующей проверки.

В практике существуют случае, когда сотрудник обжаловал примененное к нему дисциплинарное взыскание за задержки, зафиксированные видеокамерами, установленными у входа в офис, мотивировав свое мнение о незаконном характере видеозаписи. Так. не редко встречаются судебные решения по признанию приказа о дисциплинарном взыскании, наложенном на работника недействительным и взысканию компенсацию морального вреда в пользу работника, так как видеозапись осуществлялась на рабочем месте с нарушением закона: локальные нормативные акты работодателя не содержали положений о видеонаблюдении, сотрудники не были уведомлены.

В свою очередь, в научной литературе встречаются интересные предложение внести в закон об обработке персональных данных: "установить запрет для работников организации и посетителей блокировать, закрывать камеры или каким-либо иным образом препятствовать производству видеонаблюдения". Безусловно, представляется правильным не допустить, чтобы работники прерывали деятельность системы наблюдения, обеспечивая ее бесперебойную работу.

Если работодатель планирует установить систему видеонаблюдения только на территории организации, то, на наш взгляд, необходимо уведомлять

сотрудников, а в трудовых договорах с новыми сотрудниками включать право работодателя вести видеозапись на рабочих местах с целями такой записи.

Если в поле зрения камеры, расположенной на территории работодателя, попадают посторонние лица, например, запись видео торговом зале, то положения о системе видеонаблюдения, должны быть включены в политика компании в отношении обработки персональных данных.

Что касается изготовления личного пропуска для сотрудника – как мы видели в предыдущей главе, фотография на пропуске не может быть отнесена к биометрическим данным, поскольку понятие биометрических данных подразумевает не только наличие определенных данных, содержащих информацию о физиологических и биологических характеристиках человека, но и использование биометрических методов идентификации личности. В связи с этим сбор и обработка образа работника в процессе контроля не подразумевают его согласия, при условии, что контрольное предприятие осуществляется работодателем в соответствии с коллективным договором, акты работодателя утверждаются в соответствии со статьей 372 Трудового кодекса.

Для внешнего наблюдения за сотрудниками в основном используются три вида средств: электронные карты, видеонаблюдение и биометрические данные. Эти средства могут использоваться для одной или нескольких целей: контроля и управления доступом в помещения (приборы устанавливаются на входах/выходах из здания, в тамбурах, на офисные двери и т. д.), для мониторинга и контроля процесса производства или производительности работы (приборы контроля (СКУД) могут быть установлены на рабочем месте для мониторинга непосредственно действий на рабочих компьютеров.

Эти системы мониторинга различаются, причем одни работодатели могут выбрать только одну из них (карты/видеонаблюдение/биометрия), а другие - всю доступную область средств. Существует также третья категория работодателей, использующих средства мониторинга, где эти современные устройства используются наряду с другими традиционными средствами, такими, как посты охраны и журналы посещений для контроля доступа и проверки рабочего

времени. Многие работодатели предоставляют информационные ресурсы и различные технологии в распоряжение своих сотрудников, чтобы те могли лучше выполнять свои профессиональные обязанности: доступ в Интернет, электронные счета, электронную подпись, электронные устройства для определения местоположения и т.д.

Здесь важно отметить, что например, Суд Европейского союза (CJEU) счел, что запись рабочего времени, указывающая в отношении каждого работника время начала и окончания рабочего времени, а также соответствующие перерывы и интервалы, подпадает под понятие «персональные данные», к примеру постановление суда по делу от 19 июня 2014 года, [Pharmacontinente - Saúde e Higiene SA and Others v Autoridade Para As Condições do Trabalho (ACT), Case C-683/13 (ECLI:EU:C:2014:2028]

С помощью специального программного обеспечения работодатели могут контролировать, каким образом их сотрудники используют Интернет:

- на какие сайты заходят или какие учетные записи электронной почты используют для выполнения служебных обязанностей.

- либо чтобы весело провести время на рабочем месте (общение в социальных сетях, игры онлайн и т. д.),

или сделать некоторые другие личные дела (запись на прием к врачу, приобретение предметов личного пользования, и т. д.).

Кроме того, работодатели могут контролировать использование своим персоналом ИТ-оборудования для обеспечения надлежащего функционирования и безопасности сети и коммуникаций работодателя.

Правила защиты данных в контексте мониторинга внешнего и внутреннего поведения сотрудников. Некоторые люди могут возразить, что нет никакой частной жизни на рабочем месте, которое является открытым или общественным местом, поскольку эта концепция применима только в тесном окружении, специфичном для дома и семьи. В соответствии с этим мышлением работодатель был бы свободен в оценке деятельности своих работников без каких-либо ограничений.

Никто не может отрицать законной заинтересованности работодателя в контроле за исполнением обязанностей работниками и достижением поставленных целей в их работе. С другой стороны, каждый работодатель должен иметь в виду, что работники по-прежнему имеют индивидуальные права, такие как неприкосновенность частной жизни.

Именно поэтому решение о внедрении и использовании новых ИТ-технологий для достижения вышеуказанных целей должно быть результатом справедливого баланса законных интересов работодателя и основных прав работников. Эти общие идеи также применимы, когда речь идет о мониторинге поведения сотрудников на рабочем месте. [OPRE, ȘANDRU, c. 200]

Нет сомнений, что используя эти средства для контроля сотрудников вмешательство в их право на неприкосновенность частной жизни возникает, поскольку они будут чувствовать себя под пристальным вниманием и поэтому они меняют их обычное поведение, привычки и предпочтений; в случае используется биометрия, некоторые люди даже думают, что их достоинство остается под вопросом, поскольку принято считать, что сбор и хранение отпечатков пальцев человека обычно связаны с преступным поведением.

Когда мы уравновешиваем интересы работодателя и право работников на неприкосновенность частной жизни, в каждом конкретном случае можно дать три ответа:

- наблюдение не допускается ни при каких обстоятельствах;

- какой-то вид наблюдения может быть разрешен при определенных обстоятельствах.

- комбинированная зона средств наблюдения допускается при определенных, строгих условиях.

Установление определенных правил защиты данных являются ключевыми для того, чтобы сделать правильный анализ для получения правильного ответа, какой ответ является наиболее приемлемым.

Во-первых, любой работодатель должен прибегнуть к оценке воздействия, разных средств мониторинга на частную жизнь работников, прежде чем принять

решение прибегнуть к определенным средствам, которые могут нанести ущерб человеческому достоинства или частной жизни его работников.

Однако вместо мониторинга персональных данных работодатель может отдать предпочтение превентивным мерам – например, использовать фильтры, блокирующие доступ к конкретным операциям в Интернете. [OPRE, ȘANDRU, c. 201]

Обобщая вышеизложенное необходимо отметить, что при определении основных положений и правил об обработке ПД, введения отдельных средств мониторинга и назначении ответственного лица работодатель должен проверить влияние средств мониторинга на частную жизнь своих работников, с целью исключить избыточность обработки персональных данных, утвердить цели обработки в рамках мониторинга, закрепить их в локальных актах, ознакомить работников с такими актами, затем утвердить список лиц, имеющих доступ к обработанным личным данным, заключить с этими лицами обязательства не разглашать конфиденциальную информацию, полученную при исполнении служебных обязанностей.

2.3. Отдельные особенности обработки персональных данных по окончанию трудовой деятельности

В соответствии со статьей 22.1 Федерального закона от 22 октября 2004 г. N 125-ФЗ "Об архивном деле в Российской Федерации» все архивные документы устанавливается, что созданные до и после 2003 года. Например, документы по персоналу, созданные до 2003 года, сохраняются, по меньшей мере, 75 лет с момента создания, а документы по персоналу, созданные начиная с 2003 года, сохраняются не менее 50 лет с даты создания.

К документам, содержащим персональные данные, относят:

- документы об организации труда, нормировании, выставлении счетов, оплате и документы о работе с персоналом: прием, перевод, увольнение работников, повышение квалификации, сертификация и награждение. Большая часть документов должна храниться до момента ликвидации, безусловно, долгосрочное хранение связано с возможной необходимостью запрашивать дополнительную информацию, например, для подтверждения страхового стажа при выдаче досрочной пенсии по старости.

Следует отметить тот факт, что в ряде нормативных правовых актов, включая упомянутый перечень, сроки хранения некоторых кадровых документов, содержащих персональные данные сотрудников, отличаются от сроков, предусмотренных статьей 22.1 125-ФЗ. Похоже, что скоро эти акты будут скорректированы до 125-ФЗ.

В обязанности работодателя при ликвидации входит передача кадровых документов, сформированных в ходе его деятельности, срок временного хранения которых не истек, для хранения в соответствующем государственном или муниципальном архиве на основании договора.

В соответствии с пунктом 8 пункта 1 статьи 24 Налогового кодекса РФ устанавливается обязанность по обеспечению сохранности документов, необходимых для расчета, удержания и перевода налогов в течение 4 лет. Статья 29 Федерального закона от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»

определяет, что организации обязаны хранить бухгалтерскую документацию в периоды, установленные в соответствии с правилами организации государственного архива, но минимальный срок хранения не может быть менее 5 лет.

К обязанностям работодателя-оператора также относится предоставление необходимых финансовые, материально-технические и другие условия для сбора, хранения, регистрации и использования архивных документов.

В соответствии с пунктом 2 части первой статьи 6 152-ФЗ и с учетом объяснений Роскомнадзора получение согласия уволенных работников на обработку их персональных данных в вышеуказанных случаях не требуется.

Суммируя рассматриваемые ситуации обработки персональных данных во время найма, во время трудовой деятельности и после увольнения сотрудника, можно отметить следующее:

- при передаче персональных данных сотрудника третьим лицам необходимо получить согласие сотрудника;

- если на территории работодателя проводится видеозапись, работник должен быть уведомлен, местный нормативный акт организации отражает его цели, ответственных сотрудников и время хранения записанной информации.

- работодателю необходимо принять положение об обработке и назначить ответственного лица, утвердить список лиц, имеющих доступ к обработанным персональным данным, заключить с этими лицами обязательства не разглашать конфиденциальную информацию, полученную при исполнении служебных обязанностей, и включить соответствующие обязанности в их должностные инструкции;

- при обеспечении хранения персональных данных сотрудников работодатель должен соблюдать условия обеспечения безопасности персональных данных и исключать несанкционированный доступ к ним, а обработанная информация не должна быть избыточной;

- данная цель обработки по которым выполнена должны быть обезличенные установленный срок, следовательно, у работодателя есть право хранить

персональные данные заявителей-не более 30 дней после закрытия вакансии, соответствующей, и документы по персоналу и организации труда, в течение периода, установленного законом о хранения файлов Российской Федерации.

Наиболее проблемным, на наш взгляд, моментом в регулировании защиты персональных данных в трудовых отношениях является отсутствие единообразной интерпретации термина биометрические данные, в частности присвоение работникам фото - и видеоизображений и, соответственно, понимание того, какие человеческие данные могут быть биометрическими.

На данный момент в отношении идентификации фотографического изображения в качестве биометрических данных существует единственный документ, а разъяснения в отношении присвоения фото-видеоизображений биометрическим данным предоставляются контрольным органом, полномочия которого не включают толкование законодательства, и поэтому эти разъяснения носят консультативный характер.

На практике указанная проблема приводит к расхождениям в законодательстве, в том числе со стороны регулятора, и, соответственно, к дополнительным санкциям в отношении работодателя, принявшего "неправильную сторону" интерпретации. На основании чего мы считаем отсутствие четкой позиции по выделению фото - и видеоизображений пробелом в современном законодательстве, который необходимо устранить.

ГЛАВА 3 ПРИВЛЕЧЕНИЕ К ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЕ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ. ОСОБЕННОСТИ РАССМОТРЕНИЯ СПОРОВ МЕЖДУ РАБОТНИКОМ И РАБОТОДАТЕЛЕМ

3.1. Виды ответственности и меры наказания за нарушения законодательства в области защиты персональных данных работников. Сравнительная характеристика законодательства РФ и зарубежных стран

Общие положения об ответственности лиц, осуществляющих обработку закреплены ст. 24 152-ФЗ, ст. 90 ТК РФ.

В первую очередь для обеспечения прав баланса прав работников как субъектов персональных данных и работодателей как операторов необходимо детально рассмотреть вопрос ответственности за нарушение законодательства об обработке персональных данных и определить достаточны ли санкции, установленные законом и соотносимы ли, они с последствиями нарушения.

Согласно ст. 2.4 КоАП РФ под должностными лицами следует понимать, в частности, совершившие административные правонарушения в связи с исполнением организационно-административных и хозяйственных функций руководителей и других сотрудников организаций.

Работодатель обязан возместить работнику как моральный вред, возникший в результате незаконного распространения информации о персональных данных работника, так и возместить работнику, ответственному за распространение персональных данных, прямой и действительный ущерб, причиненный ему.

Например, суд взыскал с работодателя в пользу работника компенсацию морального вреда за размещение ксерокопии паспорта работника на стене комнаты проходной организации. Сумма взысканной компенсации составляет 2 тысячи рублей (первоначальные требования - 200 тысяч рублей, первая инстанция взыскала 5 тысяч рублей). [Кассационное определение СК по гражданским делам Верховного суда Удмуртской Республики от 11 августа 2010

г. по делу № 33-2625]

Представляется что столь малые суммы штрафа и компенсаций за нарушения прав работников не стимулируют операторов-работодателей к созданию условий для сохранности персональных данных работников.

В странах европейского союза сегодня действует регламент 2016/679 от 27.04.2016, General Data Protection Regulation сокращенно «GDPR»).

Штрафные санкции за нарушение законодательства в области персональных данных, согласно регламенту, могут достигать 20 млн евро.

В сравнении, например с европейским законодательством, представляется, что у операторов гораздо больший стимул к соблюдению установленных требований обеспечения безопасности при обработке персональных данных, поскольку сумма штрафных санкций во много раз превышает расходы на создание адекватной системы обработки персональных данных. Предполагаем, что необходимо увеличить штрафные санкции, предусмотренные статьей 13.11, КОАП РФ ст. в 10-15 раз.

Кроме того, за игнорирование требования работника об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, работодатель может быть привлечен к административной ответственности (ч. 5 ст. 13.11 КоАП РФ) в виде предупреждения или наложения административного штрафа:

- на граждан в размере от 1 до 2 тыс. руб.;
- на должностных лиц - от 4 до 10 тыс. руб.;
- на индивидуальных предпринимателей - от 10 до 20 тыс. руб.;
- на юридических лиц - от 25 до 45 тыс. руб.

Сроки, в которые работодатель обязан выполнить требования работника, установлены в ст. 21 Закона о персональных данных

Рассмотрим некоторые практические примеры

Суд признал законным увольнение истца за разглашение заработной

платы работникам, определив следующее.

Работая системным администратором, сотрудник имел доступ к программе 1С и, следовательно, к личным данным других работников. Трудовой договор предусматривал обязательство не раскрывать информацию о системе, условиях и заработной плате предприятия. Кроме того, во время найма работник ознакомился с местными правилами работодателя, в частности, касающимися обработки персональных данных.

Однако системный администратор начал распространять среди других сотрудников информацию о повышении зарплаты одного из менеджеров компании. Поскольку данные о заработной плате являются личными данными, системный администратор имел доступ к этим данным в связи с выполнением своих служебных обязанностей. Отчет о размере заработной платы менеджера был признан грубым нарушением системным администратором трудовых обязанностей, что послужило причиной его увольнения со стороны ст. 81 ТК РФ. [Апелляционное решение Московского городского суда от 14.06.2016]

Передача информации в рамках дела в суд не является разглашением персональных данных третьим лицам.

В гражданском деле работник подал в суд документы, содержащие личные данные других работников, в том числе информацию о заработной плате. Суд счел, что это прямо не доказывает, что работник распространил информацию третьим лицам, и не является однозначным основанием для увольнения ст. 81 ТК РФ. [Апелляционное решение Московского городского суда от 20.11.2018]

Увольнение за представление персональных данных сотрудников правоохранителям незаконно.

При заключении трудового договора работник подписал обязательство о конфиденциальности информации, содержащей персональные данные. При этом работник отвечал за ведение, хранение, регистрацию и выдачу трудовых книжек.

Вечером работнику позвонили на мобильный телефон неизвестных лиц и, выдав себя за представителей Следственного комитета, попросили о помощи и немедленно прибыли на рабочее место.

О выходе на рабочее место истец не уведомил свою администрацию. Кроме того, перед прибытием на рабочее место истец сообщил по телефону неустановленным лицам о местонахождении кадровых документов.

Прибыв на рабочее место, истец не проверил документы проверяющих, но им были переданы оригиналы документов персонала, в том числе трудовые книжки и карточки Т-2 сотрудников учреждения. Истец покинул рабочее место, когда в отделе кадров все еще были посторонние люди.

После проведения служебной проверки сотрудник был уволен. Тем не менее, суд признал увольнение незаконным, установив (в частности, на основе свидетельских показаний), что правоохранительные органы действительно проводилась проверка до возбуждения уголовного дела (начались позже) и, таким образом, документы были переданы сотруднику правоохранительных органов в связи с выполнением процессуальных действий по поручению следователя, следовательно, действия работника, не может быть квалифицирован в качестве дисциплинарного нарушения и ситуации, являются обоснованными и законными. [Апелляционное решение Московского городского суда от 22.10.2018]

В результате незаконного распространения информации о персональных данных работника последний может понести моральный ущерб, который может быть возмещен работодателем. В этом случае, если работодатель возместил работнику, в отношении которого была нарушена обработка персональных данных, моральный вред, он вправе потребовать от работника-нарушителя возместить прямой и эффективный ущерб, причиненный в соответствии со ст. 243 ТК РФ материальная ответственность в общей сумме причиненного ущерба возлагается на работника в случае разглашения информации, составляющей охраняемую законом тайну.

Сотрудники могут быть привлечены к уголовной ответственности в следующих случаях.

137 УК РФ предусматривает ответственность за незаконное распространение информации о частной жизни лица, составляющей его личную или семейную тайну, без его согласия или распространение этой информации в публичном выступлении, публично выставляемом произведении или в средствах массовой информации, выполняемой лицом в пользовании его служебным положением. За эти деяния предусмотрено наказание в размере от 100 до 300 тысяч рублей. лишение права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет, или принудительный труд на срок до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового, или арест на срок до 6 месяцев, либо лишением свободы на срок до 4 лет, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет.

Ст. 140 УК РФ предусматривает ответственность за неправомерный отказ должностного лица предоставить собранные в установленном порядке документы и материалы, непосредственно затрагивающие права и свободы гражданина, или предоставление гражданину неполной или заведомо ложной информации, если эти действия нанесли ущерб законным правам и интересам граждан. Эти действия наказываются штрафом до 200 тысяч рублей или лишение права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет.

Статья 272 УК РФ предусматривает ответственность за неправомерный доступ к защищенной законом компьютерной информации, если данное деяние привело к уничтожению, блокированию, изменению или копированию компьютерной информации, совершенной лицом с использованием его служебного положения. За эти деяния предусмотрен штраф до 500 тысяч рублей с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет, или ограничением свободы на

срок до 4 лет, или принудительные работы на срок до 5 лет, или лишение свободы на тот же срок.

В п. 43 Постановления Пленума Верховного Суда РФ от 17.03.2004 № 2 "О применении судами Российской Федерации Трудового кодекса Российской Федерации" даны разъяснения, что в случае оспаривания работником увольнения по пп. "в" п. 6 ч. 1 ст. 81 ТК РФ (за разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника) работодатель обязан представить доказательства, свидетельствующие о том, что сведения, которые работник разгласил, в соответствии с действующим законодательством относятся к государственной, служебной, коммерческой или иной охраняемой законом тайне либо к персональным данным другого работника, эти сведения стали известны работнику в связи с исполнением им трудовых обязанностей и он обязывался не разглашать такие сведения.

То есть для применения дисциплинарного взыскания за разглашение персональных данных необходимо одновременно наличие следующих обстоятельств:

- разглашенные сведения в соответствии с действующим законодательством отнесены к персональным данным другого работника;

- разгласившему работнику такие сведения стали известны в связи с исполнением им трудовых обязанностей;

- работник обязался не разглашать такие сведения.

В п. 8 ст. 86 ТК РФ закреплено, что работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

Согласно ч. 4 ст. 57 ТК РФ в трудовом договоре могут предусматриваться дополнительные условия, не ухудшающие положение работника по сравнению с установленным трудовым законодательством и иными нормативными

правовыми актами, содержащими нормы трудового права, коллективным договором, соглашениями, локальными нормативными актами, в частности, о неразглашении охраняемой законом тайны (государственной, служебной, коммерческой и иной).

Таким образом, ТК РФ не устанавливает обязательного требования об оформлении с работником обязательства о неразглашении персональных данных других работников, которые ему стали известны при исполнении должностных обязанностей, а предусматривает необходимость ознакомить с документами, содержащими порядок обработки персональных данных, права и обязанности работника в этой области, а также возможность включения условия о неразглашении в трудовой договор.

Как показывает судебная практика, если работник ознакомлен с локальными правовыми актами, в которых к обязанностям работника отнесено неразглашение персональных данных, полученным при исполнении трудовых обязанностей, либо обязанности по неразглашению предусмотрены трудовым договором, то можно считать, что работник обязался не разглашать такие сведения. [Апелляционное определение Московского городского суда от 30.05.2018 № 33-23467/2018]

Еще в одном деле суд посчитал, что отсутствие у работодателя режима конфиденциальности, а также положения о персональных данных не может исключать ответственность работника за разглашение персональных данных, поскольку в трудовом договоре работника указано на недопустимость распространения без разрешения работодателя информации, составляющей служебную или коммерческую тайну. [Апелляционное определение Московского городского суда от 18.04.2016 № 33-10533/2016].

Однако также на практике достаточно часто встречаются случаи, когда помимо ознакомления с политикой об обработке и защите персональных данных работники подписывают обязательство о неразглашении, в котором они подтверждают, что ознакомлены с перечнем информации, составляющей коммерческую тайну, персональные данные и другую информацию

ограниченного доступа организации, и обязуются ее не разглашать. В таких случаях при увольнении работников по пп. "в" п. 6 ч. 1 ст. 81 ТК РФ суды также не находят оснований для признания увольнения незаконным [Апелляционное определение Московского городского суда от 14.02.2017 № 33-5694/2017, Определение Московского городского суда от 20.07.2017 № 4г-7032/2017].

Если работники имеют доступ к персональным данным других работников, целесообразно оформлять с ними обязательство о неразглашении персональных данных. Сведения о заработной плате работника являются его персональными данными. То есть, даже если такие сведения отнесены к коммерческой тайне, на них распространяется режим персональных данных.

Иногда на работников возлагается только обязанность по неразглашению коммерческой тайны. При этом работодатели ошибочно полагают, что персональные данные могут являться коммерческой тайной.

Если работник будет ознакомлен только с положением о неразглашении коммерческой тайны и впоследствии распространит сведения о персональных данных другого работника (его заработной плате), суд может не усмотреть нарушений со стороны работника и признать, что обязательство по неразглашению персональных данных им не принималось, а коммерческой тайной такие сведения не являются [Кассационное определение Верховного суда Республики Татарстан от 29.07.2010 № 8674/10]

Рассмотрим несколько примеров из судебной практики, когда передача персональных данных работников признавалась нарушением обязанностей по обработке персональных данных со стороны работников.

В организации были приняты локальные правовые акты, определяющие порядок работы с документами, содержащими конфиденциальную информацию (в том числе персональные данные клиентов), установлен перечень сведений конфиденциального характера, режим хранения конфиденциальных документов, порядок обращения с конфиденциальными документами и уничтожения.

В частности, предусматривалось, что документы должны храниться в сейфах, металлических шкафах или стеллажах, которые по окончании рабочего

дня запираются и опечатываются работниками. Уничтожение документов производится путем измельчения (использования шредера), исключающего восстановление текста документа. Контроль за соблюдением вышеизложенных требований возлагается на руководителя подразделения банка.

Однако сотрудниками подразделения в связи с недостатком бумаги повторно использовались документы, содержащие персональные данные клиентов. То есть документы не были уничтожены в установленном порядке и не хранились в сейфах.

При уборке помещения стопки документов с персональными данными клиентов были выброшены. В этот же день в СМИ блогером размещена информация о том, что в мусорном контейнере, расположенном рядом с подразделением банка, находится документация, содержащая персональные данные клиентов. Текст был сопровожден фотографиями, на которых видны коробки с анкетами, содержащими персональные данные клиентов банка.

Суд пришел к выводу, что разглашение банковской тайны и конфиденциальных данных клиентов, которые были переданы банку как оператору персональных данных таких лиц, произошло вследствие нарушения руководителем подразделения возложенных должностных обязанностей, а именно неосуществления контроля за исполнением работниками требований по хранению, уничтожению документов, что позволило иным сотрудникам беспрепятственно получить к ним доступ, выбросить их в мусорный контейнер и, как следствие, допустить размещение фотографий и публикаций в Интернете. [Апелляционное определение Московского городского суда от 16.02.2017 № 33-2761/2017].

При этом важно отметить, что Роскомнадзор может проверить любую организацию (ИП), поскольку все они имеют дело с персональными данными и являются их операторами. постановлением Правительства Российской Федерации от 13 февраля 2019 г. № 146 были утверждены правила организации и осуществления государственного контроля и надзора за обработкой персональных данных, согласно которым его должностные лица будут выяснять,

соблюдаете ли вы обязательные требования при работе с персональными данными своих сотрудников (в том числе кандидатов, которых вы рассматриваете на должности в компании), в том числе если вы собираете их данные через сайт. В некоторых случаях плановая проверка бывает чаще - раз в два года (обычно - раз в три года). Например, если организация (ИП) собирает биометрические данные.

Внеплановые проверки могут проводиться как по жалобам сотрудников, чьи персональные данные вы обрабатываете, так и по инициативе самого проверяющего органа. Дело в том, что Роскомнадзор может, например, изучать на вашем сайте правильность оформления отношений с соискателями в сфере персональных данных и по итогам таких мероприятий прийти с внеплановой проверкой. При этом, особо высокая вероятность проверки у тех работодателей, кто:

• имеет большое число сотрудников;

• использует формы обратной связи на сайтах.

Плановые проверки проводятся раз в два-три года. План утверждается ежегодно. однако, в Единый реестр проверок сведения о проверках Роскомнадзора в сфере персональных данных не включаются, так как на эти проверки Закон N 294-ФЗ не распространяется.

Статистика Роскомнадзора подтверждает рост вероятности проведения проверки в сфере персональных данных: рост количества жалоб в Роскомнадзор с 32 000 в 2017 г. до 50 000 в 2019 г. Процент выявления нарушений при плановых проверках (по данным годовой отчетности Роскомнадзора по защите прав субъектов персональных данных) 70 - 80%. Процент выявления нарушений при внеплановых проверках - 30%.

Однако необходимо отметить, что ресурсы Роскомнадзора не позволяют проводить сплошные проверки организаций работодателем, однако с ростом использования средств автоматизации, представляется возможным прогнозировать рост количества проверок.

3.2. Организация системы защиты персональных данных работников в условиях развития цифровых технологий. Сравнительный анализ российского и зарубежного опыта.

С целью полного разбора темы организации системы защиты персональных данных работников стоит разобрать несколько примеров из зарубежной практики, понять, что сегодня является недостаточно урегулированным в части организации систем и детально разобрать комплекс технических, организационных и юридических мер существующих в развитых правовых системах.

Системы защиты персональных данных работников в США.

Так для начала следует остановиться на специальной публикация National Institute of Standards and Technology (NIST) № 800-122 «Руководство по защите конфиденциальности персональной идентифицируемой информации (PII)». которая была утверждена Соединённых штатах Америки для обеспечения сохранности персональных данных.

В данном руководстве изложены как меры технического характера, так и меры касающегося юридического и организационного характера.

Прежде всего в важно отметить, важное место занимает обучение сотрудников правилам работы с персональными данным и системами, которые осуществляют их обработку и защиту различными способами.

Таким образом сотрудники должны быть обучены следующим крайне важным навыкам:

- определение того, что является персональными данными, их вычленение из общего объема информации;
- умение использовать законодательные акты для организации комплексной системы защиты персональных данных сцелью обеспечения прав субъектов персональных данных;
- досконально знать существующие ограничения на обработку отдельных категорий персональных данных, правила их обезличивания и уничтожения;

- Уметь действовать при обнаружении нарушений доступа к персональным данным, их кражи, а также нарушений правил их обработки.

К мерам защиты согласно документу относят:

- Подготовку и проведение внутреннего и внешнего аудита с целью проверки правильности обработки персональных данных

- организации управления доступом сотрудников к информационным системам, содержащим персональные данные;

- определения правил многоступенчатой аутентификации и идентификации для доступа в системы для лиц, ответственных за обработку персональных данных;

- Подготовку работы с материальными носителями информации, с физическими носителями информации, правила их оборота внутри организации-оператора.

Также в руководстве по защите конфиденциальности персональной идентифицируемой информации (PPI), отмечены основные типы рисков, связанных с утечкой персональных данных, и в зависимости от полноты украденных персональных данных человек может понести социальный, экономический или физический ущерб. Если утерянная информация достаточна для использования похитителем личных данных, человек может пострадать, например, от кражи денежных средств с банковской карты, компрометации медицинских записей, угроз и/или преследований со стороны третьих лиц с целью получения выгоды. Человек может понести огромные потери времени и денег, чтобы устранить ущерб.

Сами организации-операторы также сталкиваются с рисками, в частности с риском потери собственной репутации и доверия сотрудников.

Кроме того, восстановление после серьезного нарушения в системе защиты персональных данных работников является дорогостоящим для многих организаций с точки зрения времени, затрачиваемого ключевыми сотрудниками на координацию и выполнение соответствующих мер реагирования.

В случае, если утрата персональных данных представляет собой нарушение законодательства, организация и/или ее ответственное лицо могут быть привлечены к уголовной или административной ответственности.

Еще один серьезный риск для организаций-работодателей заключается в том, что их общественная репутация и общественное доверие могут быть утрачены, что может поставить под угрозу способность организаций выполнять свои задачи.

Кроме того, ключевыми вопросами для американской системы организации персональных данных работников для являются законодательные требования ограничения на обработку персональных данных (например, закона о неприкосновенности частной жизни)

В соответствии со справедливой информационной практикой ограничения сбора и использования персональных данных работодателю в США необходимо определить являются ли собранные персональные данные абсолютно необходимыми для ведения бизнеса. Во многих случаях защита персональных данных аналогична защите других данных и включает в себя: защиту конфиденциальность, целостность и доступность информации. Большинство элементов управления безопасностью, используемых для других типов данных, также применимы к их защите.

Существует несколько конкретных гарантии конфиденциальности, такие, как анонимность, минимизация сбора персональных данных и обезличивания.

Помимо требований к защите, существуют и другие требования к обращению с персональными данными.

Справедливая информационная практика содержит рекомендации по наилучшей практике, такие как спецификация (определение) цели, подотчетность и качество проверки безопасности данных (проведение аудита).

Системы защиты персональных данных работников в Европе.

В странах европейского союза, в частности, действует регламент 2016/679 от 27.04.2016, General Data Protection Regulation сокращенно «GDPR»). «Прозрачность способствует честности», такой принцип лежит в основе

определения сферы применения статьи 6 GDPR включает в себя пять законных оснований для обработки:

- Если обработка персональных данных необходима для исполнения договора;

- для выполнения задач органов государственной власти

- для выполнения юридического обязательства,

- в целях защиты законных интересов оператора или третьих лиц,

- или в случае необходимости для защиты жизненно важных интересов субъекта персональных данных.

Организации-операторы обязаны уведомлять субъектов данных о том, кто владеет их данными, Какие типы данных были получены, как эти данные будут использоваться и, как долго они будут использоваться и будут ли данные сохранены. Организации-операторы также должны информировать субъектов данных о сборе и обработке данных если они получены без согласия субъекта. Статья 14 содержит два исключения из этого требования об уведомлении:

- если “предоставление такой информации окажется невозможным или потребует несоразмерных усилий”;

- если требование об уведомлении может сделать невозможным или серьезно затруднить достижение целей такой обработки

Внедрение регламентов также затронуло и изменило многие национальные правовые регулирования по вопросу персональных данных.

Так, к примеру, в Словакии 29 ноября 2017 года был принят закон № 18/2018 СБ о защите персональных данных, подписанный президентом Словацкой Республики 19 декабря 2017 года, которым было создано Управление по защите персональных данных.

В Польше 21 февраля 2019 года Сейм (нижняя палата польского парламента) принял закон от 21 февраля 2019 года «О внесении изменений в некоторые законы в связи с применением GDPR» (так называемый «выравнивающий закон»).

Этот Закон направлен на приведение формулировок соответствующих положений трудового законодательства в соответствие со статьей 6 раздела GDPR, которая вводит существование «юридического обязательства» в качестве предварительного условия для сбора персональных данных. Этот закон вносит поправки в более чем 160 различных законодательных актов, включая Трудовой кодекс.

В Венгрии законодатель принял Национальный закон, дополняющий GDPR, на своей внеочередной сессии 17 июля 2018 года.

Правительство также ввело в действие закон (Закон XIII от 2018 года), определяющий венгерское агентство по защите данных и свободе информации в качестве надзорного органа Венгрии по GDPR, который вступил в силу 30 июня 2018 года., проект закона о секторальном внедрении GDPR был представлен в парламент 7 февраля 2019 года. Проект предполагает внести изменения в 86 законодательных актов, приведя их в соответствие с положениями GDPR.

С 24 апреля 2019 года в Чешской Республике действует новый закон, касающийся обработки персональных данных, который определяет и дополнительно регулирует обработку персональных данных в соответствии с GDPR. Сопутствующий закон регулирует другие 39 связанных с ним правовых актов, таких как Уголовно-процессуальный кодекс, Закон о борьбе с отмыванием денег, закон о свободе информации и др. [Pikulík, Štarchoň, c. 1176]

Начиная с 90-х гг. прошлого века, в трудовых отношениях, для контроля выполнения работником его трудовой функции, начали использоваться контрольные механизмы, которые осуществляются не представителем работодателя, а при помощи информационно-телекоммуникационных сетей (в т.ч. при помощи Интернет, использования мобильного телефона, средств аудио и видеонаблюдения). Основной причиной использования информационных технологий для осуществления контрольной функции работодателя стало появление дистанционного труда и необходимость контроля осуществления трудовой функции работниками, которые работают удаленно. В научной

литературе такой контроль получил название «информационного» («informational»).

В Кодексе практики МОТ по защите персональных данных работников отмечается, что проблемы, связанные с использованием более сложных методов мониторинга, является схожими с проблемами, возникающими при использовании таких традиционных методов наблюдения, как например, прослушивание телефонных переговоров или осуществление видеонаблюдения. Системы мониторинга, установленные для других целей, как например, учет, запись и анализ трудового процесса, позволяют собирать персональные данные, которые можно легко преобразовать в материалы мониторинга (п. 6.13).

В этой связи представляется необходимым создать единый документ, утвержденный постановлением правительства, который бы установил общие правила по организации и проведению аудита инцидентов информационной безопасности; правила и документы (включая типовые формы) необходимые для:

- организации управления доступом сотрудников к информационным системам, содержащим персональные данные;

- определения правил многоступенчатой аутентификации и идентификации для доступа в системы для лиц, ответственных за обработку персональных данных

- Подготовку работы с материальными носителями информации, с физическими носителями информации, правила их оборота внутри организации-оператора, использование криптографических средств защиты и правила работы и хранения биометрических персональных данных.

- организации системы мониторинг работоспособности информационной системы защиты персональных данных и отслеживания соблюдения работодателем законности в использовании персональных данных работников (специально сертифицированные или аттестованные организации и введение законодательных требований о наличии аттестации систем защиты персональных данных).

- введение квалификационных требований для лиц, ответственных за обработку персональных требований и необходимость прохождения специального обучения по правильной организации систем защиты персональных данных.

Подводя итоги вышесказанному, можно отметить следующее:

- даже если в трудовом законодательстве отсутствуют специальные нормы, посвященные отдельным видам мониторинга деятельности работников, следует учитывать, что такой мониторинг представляет собой обработку персональных данных работников;

- в условиях цифровой экономики и современных информационных технологий, которые позволяют осуществлять мониторинг деятельности работников, без установления законодательных пределов их использования, можно ожидать существенного ограничения трудовых прав работников,

- в связи с этим необходимо внесение изменений в российское законодательство, направленных на обеспечение соблюдения баланса интересов работника и работодателя при проведении мер мониторинга (и осуществление такой проверки судами), обеспечение защиты персональных данных работников.

В частности, необходимо установить запрет постоянного непрерывного мониторинга, а также предусмотреть необходимость учета мнения профсоюза при введении того или иного вида мониторинга.

На текущий момент для развития законодательства о защите персональных данных прежде всего, необходимо принятие стандартов организации систем защиты персональных данных, которые вводили бы не только общее описание и требования к техническим и физическим мерам защиты, но и в том числе, общие требования к квалификации сотрудников, ответственных за обработку персональных данных у работодателей, а также требования по реакции сотрудников на обнаружение нарушений доступа к персональным данным, их кражи, а также нарушений правил их обработки.

ЗАКЛЮЧЕНИЕ

Одной из основных целей работы было детальное рассмотрение положений и требования закона в сфере обработки персональных данных работников, был сделан акцент на наиболее сложных и спорных вопросах которые возникают в связи с обработкой персональных данным при трудоустройстве, в процессе трудовых отношений, рассмотрены особенности хранения и обращения с данными после увольнения.

Центральной идеей работы было на основании имеющейся судебной практики выявить имеющиеся проблемы в законодательстве, непосредственно связанные с обработкой персональных данных работников, а также рассмотреть возможные пути их решения. Также на рассмотрение были поставлены меры ответственности оператора-работодателя за нарушения законодательства о персональных данных и их достаточность в современных реалиях.

Также стоит обратить отдельное внимание, на проблематику связанную с тем, что на настоящий момент не предлагается четкого толкования и ясности в отношении биометрических персональных данных. С учетом того, что в настоящее время не существует какого-либо действительного инструмента, позволяющего идентифицировать фотографические изображения работников в качестве биометрических данных, и что контрольный орган не обладает компетенцией толковать законодательство, мы считаем, что нет четкой позиции по этому вопросу в качестве пробела в современном законодательстве, который необходимо устранить.

Кроме того, были освещены вопросы, касающиеся правомерности использования работодателями проверок на полиграфе как соискателей, так и работников, в результате были выявлены случаи нарушения прав работников, к которым можно отнести необоснованные дисциплинарные взыскания и увольнения.

С учетом проанализированных данным представляется необходимым введение отдельного нормативного акта регулирующего введения правил

использования работодателями полиграфа, поскольку применение данного устройства на настоящий момент в правоохранительных целях и создает условия для злоупотребления этим методом.

Были исследованы проблемы, возникающими при использовании таких традиционных методов наблюдения, как например, прослушивание телефонных переговоров или осуществление видеонаблюдения. Системы мониторинга, установленные для других целей, как например, учет, запись и анализ трудового процесса, позволяют собирать персональные данные, которые можно легко преобразовать в материалы мониторинга.

Прежде всего, рассматривая вопрос об организации обработки персональных данных работников, необходимо рассмотреть определение персональных данных с целью определить, что может представлять собой персональные данные и как их определить в общем массиве информации имеющей отношение к работнику.

В законодательстве, отсутствует четкое разграничение того, что можно определить как персональные данные, а что нет. При наличии такой неопределенности существуют проблемы отнесения к ним той или иной информации или совокупности набора отдельных данных, хранящихся у работодателя. На текущий момент представляется необходимым разработка четких критериев отнесения информации к персональным данным, которыми могли бы руководствоваться как работодатели-операторы, так и контролирующий орган - Роскомнадзор.

Следующим наиболее проблемным, на наш взгляд, моментом в регулировании защиты персональных данных в трудовых отношениях является отсутствие единообразной интерпретации термина биометрические данные, в частности присвоение работникам фото - и видеоизображений и, соответственно, понимание того, какие человеческие данные могут быть биометрическими.

На данный момент в отношении идентификации фотографического изображения в качестве биометрических данных существует единственный

документ, а разъяснения в отношении присвоения фото-видеоизображений биометрическим данным предоставляются контрольным органом, полномочия которого не включают толкование законодательства, и поэтому эти разъяснения носят консультативный характер.

На практике указанная проблема приводит к расхождениям в законодательстве, в том числе со стороны регулятора, и, соответственно, к дополнительным санкциям в отношении работодателя, принявшего "неправильную сторону" интерпретации. На основании чего мы считаем отсутствие четкой позиции по выделению фото - и видеоизображений пробелом в современном законодательстве, который необходимо устранить.

Если в результате нарушения правил, регулирующих хранение, обработку и использование персональных данных работника, ему причинен материальный или моральный ущерб, он подлежит денежной компенсации в соответствии с положениями Гражданского кодекса РФ.

В ходе исследования были выявлены практические и теоретические проблемы, некоторые пробелы и коллизии существующих правовых норм, предложены варианты их решения:

Как упоминалось ранее, в Кодексе практики МОТ по защите персональных данных работников отмечается, что проблемы, связанные с использованием более сложных методов мониторинга, является схожими с проблемами, возникающими при использовании таких традиционных методов наблюдения, как например, прослушивание телефонных переговоров или осуществление видеонаблюдения. Системы мониторинга, установленные для других целей, как например, учет, запись и анализ трудового процесса, позволяют собирать персональные данные, которые можно легко преобразовать в материалы мониторинга.

В этой связи представляется необходимым создать единый документ, утвержденный постановлением правительства, который бы установил общие правила по организации систем защиты персональных данных работников и ряд

обязательных требований, среди которых из зарубежной практики можно выделить:

- необходимость закрепления алгоритма по проведению аудита инцидентов информационной безопасности;

- закрепление ряда правил и документов (включая типовые формы) необходимые для:

- организации управления доступом сотрудников к информационным системам, содержащим персональные данные;

- определения правил многоступенчатой аутентификации и идентификации для доступа в системы для лиц, ответственных за обработку персональных данных

- Подготовку работы с материальными носителями информации, с физическими носителями информации, правила их оборота внутри организации-оператора, использование криптографических средств защиты и правила работы и хранения биометрических персональных данных.

- организации системы мониторинг работоспособности информационной системы защиты персональных данных и отслеживания соблюдения работодателем законности в использовании персональных данных работников (специально сертифицированные или аттестованные организации и введение законодательных требований о наличии аттестации систем защиты персональных данных).

- определить правила использования работодателями психологических тестирований и полиграфа в исследовании работников.

- введение квалификационных требований для лиц, ответственных за обработку персональных требований и необходимость прохождения специального обучения по правильной организации систем защиты персональных данных.

- Введением мер, направленных на обеспечение соблюдения баланса интересов работника и работодателя при проведении мер мониторинга.

Кроме того данным документом, необходимо установить запрет постоянного непрерывного мониторинга, а также предусмотреть необходимость учета мнения профсоюза при введении того или иного вида мониторинга, а также четко определить границы такого мониторинга, к примеру установить перечень вопросов, которые недопустимо включать в анкеты соискателей, напрямую не позволяющие работодателю оценить профессиональные и деловые качества работника (о планах на личную жизнь, вероисповедании и др.)

Так, к примеру, считаем необходимым отражение в документе определенных наборов данных работников, которые в своей совокупности можно определить в качестве персональных данных, например что ФИО работника + номер его мобильного телефона могут быть определены в качестве персональных данных, номер его страхового индивидуального лицевого счета или индивидуальный номер налогоплательщика без указания его ФИО или телефона не определялись бы как персональные данные, которым требуется особый режим правовой охраны.

На основе анализа норм, действующих в странах европейского союза, в частности, регламента 2016/679 от 27.04.2016, General Data Protection Regulation сокращенно «GDPR») было определено, что штрафные санкции за нарушение законодательства в области персональных данных, согласно регламенту, могут достигать 20 млн евро.

В сравнении, например с европейским законодательством, представляется, что у операторов гораздо больший стимул к соблюдению установленных требований обеспечения безопасности при обработке персональных данных, поскольку сумма штрафных санкций во много раз превышает расходы на создание адекватной системы обработки персональных данных. В этой работе было предложено увеличить размер административных штрафов, предусмотренных статьей 13.11. КоАП РФ, в целях предотвращения нарушений правового порядка сбора, хранения, использования или распространения персональных данных примерно в 15-20 раз.

Важным остаётся вопрос квалификации лица, ответственного за организацию систем защиты и обработки персональных данных в организации.

Так, например, в Соединённых штатах Америки для обеспечения сохранности персональных данных было утверждена Специальная публикация National Institute of Standards and Technology (NIST) № 800-122 «Руководство по защите конфиденциальности персональной идентифицируемой информации (PII)».

В данном руководстве изложены как меры технического характера, так и меры касающегося юридического и организационного характера. Прежде всего в важно отметить, важное место занимает обучение сотрудников правилам работы с персональными данным и системами, которые осуществляют их обработку и защиту различными способами.

Таким образом сотрудники должны быть обучены следующим крайне важным навыкам, которые должны быть закреплены в подзаконном акте:

- определение того, что является персональными данными, их вычленение из общего объема информации;

- умение использовать законодательные акты для организации комплексной системы защиты персональных данных с целью обеспечения прав субъектов персональных данных;

- досконально знать существующие ограничения на обработку отдельных категорий персональных данных, правила их обезличивания и уничтожения;

- Уметь действовать при обнаружении нарушений доступа к персональным данным, их кражи, а также нарушений правил их обработки.

К мерам защиты согласно документу относят:

- Подготовку и проведение внутреннего и внешнего аудита с целью проверки правильности обработки персональных данных

- организации управления доступом сотрудников к информационным системам, содержащим персональные данные;

- определения правил многоступенчатой аутентификации и идентификации для доступа в системы для лиц, ответственных за обработку персональных данных;

- Подготовку работы с материальными носителями информации, с физическими носителями информации, правила их оборота внутри организации-оператора.

Подводя итоги вышесказанному, можно отметить следующее:

- даже если в трудовом законодательстве отсутствуют специальные нормы, посвященные отдельным видам мониторинга деятельности работников, следует учитывать, что такой мониторинг представляет собой обработку персональных данных работников;

- в условиях цифровой экономики и современных информационных технологий, которые позволяют осуществлять мониторинг деятельности работников, без установления законодательных пределов их использования, можно ожидать существенного ограничения трудовых прав работников,

- в связи с этим необходимо внесение изменений в российское законодательство, направленных на обеспечение соблюдения баланса интересов работника и работодателя при проведении мер мониторинга (и осуществление такой проверки судами), обеспечение защиты персональных данных работников.

В частности, необходимо установить запрет постоянного непрерывного мониторинга, а также предусмотреть необходимость учета мнения профсоюза при введении того или иного вида мониторинга.

На текущий момент для развития законодательства о защите персональных данных прежде всего, необходимо принятие стандартов организации систем защиты персональных данных, которые вводили бы не только общее описание и требования к техническим и физическим мерам защиты, но и в том числе, общие требования к квалификации сотрудников, ответственных за обработку персональных данных у работодателей, а также требования по реакции сотрудников на обнаружение нарушений доступа к персональным данным, их кражи, а также нарушений правил их обработки.

Была отмечена практическая проблема участия работника в полной материальной ответственности за разглашение персональных данных работников из-за отсутствия соответствующих норм в федеральных законах.

Таким образом, проанализировав все основные вопросы правового регулирования защиты персональных данных работников, с учетом научными аргументами и фактами, действующего законодательства, судебной практики и применения законодательства, пробелы, конфликты, практические проблемы и разработаны рекомендации для их решения и избрана форма для их закрепления, мы считаем, что цель данного исследования была достигнута.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Нормативно-правовые акты

1.1. Всеобщая декларация прав человека: принята Генеральной Ассамблеей ООН 10 декабря 1948 г. // Российская газета. – 1995. – № 67.

1.2. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбурге 28.01.1981) // Консультант Плюс: справочно-правовая система. (дата обращения 05.09.2020).

1.3. Директива № 2002/22/ЕС Европейского парламента и Совета Европейского Союза "Об универсальных услугах и правах пользователей в отношении сетей электронных коммуникаций и услуг (Директива об универсальных услугах" // Первоначальный текст Директивы на английском языке опубликован в Official Journal of the European Communities № L 108. 24.04.2002. P. 51. URL: http://eur-lex.europa.eu/ (дата обращения 05.11.2020).

1.4. Конституция Российской Федерации: от 12 декабря 1993 г.: по состоянию на 14.03.2020 // Российская газета. 2020. № 144.

1.5. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 31.07.2020)// Собрание законодательства РФ", 05.12.1994, № 32, ст. 3301.

1.6. Трудовой кодекс Российской Федерации» от 30.12.2001 N 197-ФЗ (ред. от 31.07.2020) (с изм. и доп., вступ. в силу с 13.08.2020) // Российская газета, № 256, 31.12.2001.

1.7. Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ (ред. от 15.10.2020, с изм. от 16.10.2020)//Официальный интернет-портал правовой информации http://www.pravo.gov.ru - 15.10.2020).

1.8. Федеральный закон от 27.07.2004 N 79-ФЗ (ред. от 31.07.2020) "О государственной гражданской службе Российской Федерации"//"Парламентская газета", N 140-141, 31.07.2004.

1.9. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 24.04.2020) "О персональных данных"// Российская газета", № 165, 29.07.2006.

1.10.Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 08.06.2020) "Об информации, информационных технологиях и о защите информации" "Российская газета", № 165, 29.07.2006.

1.11.Федеральный закон от 07.05.2013 N 99-ФЗ (ред. от 29.12.2017) "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных" и Федерального закона "О персональных данных"// "Собрание законодательства РФ", 13.05.2013, № 19, ст. 2326

1.12.Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении Перечня сведений конфиденциального характера"// Собрание законодательства РФ", 10.03.1997, N 10, ст. 1127,

1.13.Постановление Минтруда России от 10.10.2003 N 69 (ред. от 31.10.2016)"Об утверждении Инструкции по заполнению трудовых книжек//Российская газета, № 235, 19.11.2003.

1.14.Постановление Правительства РФ от 06.07.2008 N 512 (ред. от 27.12.2012) "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных"// Собрание законодательства РФ" - 31.12.2012).

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

1.16.Постановление Правительства РФ от 16.03.2009 N 22 (ред. от 16.05.2020) "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций" (вместе с "Положением о Федеральной

службе по надзору в сфере связи, информационных технологий и массовых коммуникаций") // Собрание законодательства РФ", 23.03.2009, N 12, ст. 1431

1.17.Постановление Правительства РФ от 04.03.2010 N 125 (ред. от 10.02.2014) "О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию" //"Собрание законодательства РФ", 08.03.2010, N 10, ст. 1103,

1.18.Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"// "Собрание законодательства РФ", 05.11.2012, N 45, ст. 6257,

1.19.Постановление Правительства РФ от 30.06.2018 № 772 «Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации» // Собрание Законодательства РФ. 2018. № 28. Ст. 4234.

1.20.Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 23.03.2017) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" // "Российская газета", № 107, 22.05.2013.

1.21.Приказ ФСБ России от 10.07.2014 N 378 "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//«Российская газета», № 211, 17.09.2014

1.22.Приказ Роскомнадзора от 05.09.2013 № 996 "Об утверждении требований и методов по обезличиванию персональных данных" (вместе с "Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ") // "Российская газета", № 208, 18.09.2013

1.23.Приказ Роскомнадзора от 30.05.2017 № 94 «Об утверждении методических рекомендации по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения// Консультант Плюс: справочно-правовая система. (дата обращения 04.10.2020).

1.24.Приказ Роскомнадзора от 3 декабря 2012 г. № 1255 «Об утверждении положения об обработке и защите персональных данных в центральном Аппарате федеральной службы по надзору в сфере связи, Информационных технологий и массовых коммуникаций// Консультант Плюс: справочно-правовая система. (дата обращения 23.11.2020).

2. Материалы практики:

2.1. Апелляционное определение Московского городского суда от 18.04.2016 № 33-10533/2016. // Консультант Плюс: справочно-правовая система. (дата обращения 10.10.2020).

2.2. Апелляционное определение Московского городского суда от 14.02.2017 № 33-5694/2017// Консультант Плюс: справочно-правовая система. (дата обращения 10.10.2020).

2.3. Апелляционное определение Московского городского суда от 16.02.2017 № 33-2761/2017// Консультант Плюс: справочно-правовая система. (дата обращения 10.10.2020).

2.4. Апелляционное определение Московского городского суда от 30.05.2018 № 33-23467/2018// Консультант Плюс: справочно-правовая система. (дата обращения 10.10.2020).

2.5. Определение Московского городского суда от 20.07.2017 N 4г-7032/2017 // Консультант Плюс: справочно-правовая система. (дата обращения 10.10.2020).

2.6. Кассационное определение Верховного суда Республики Татарстан от 29.07.2010 N 8674/10// Консультант Плюс: справочно-правовая система. (дата обращения 10.10.2020).

2.7. Кассационное определение СК по гражданским делам Верховного суда Удмуртской Республики от 11 августа 2010 г. по делу № 33-2625 // Консультант Плюс: справочно-правовая система. (дата обращения 10.10.2020).

2.8. Постановление Пленума Верховного Суда РФ от 17.03.2004 N 2 (ред. от 24.11.2015) "О применении судами Российской Федерации Трудового кодекса Российской Федерации"//"Российская газета", № 297, 31.12.2006.

2.9. Постановление Пленума ВС РФ от 24 февраля 2005 г. № 3 "О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц"//"Российская газета", № 50, 15.03.2005.

2.10.Постановление Пленума ВС РФ от 16 ноября 2006 г. ред. от 28.09.2010) № 52 "О применении судами законодательства, регулирующего материальную ответственность работников за ущерб, причиненный работодателю" "Российская газета", № 268, 29.11.2006.

2.11.Разъяснения Роскомнадзора: «Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве// http://www.rsoc.ru

по состоянию на 24.12.2012» // Консультант Плюс: справочно-правовая система. (дата обращения 21.10.2020).

2.12.Разъяснения Роскомнадзора от 30.09.2013 «Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки» // Консультант Плюс: справочно-правовая система. (дата обращения 21.10.2020).

2.13.Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»//Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, URL: http://www.rkn.gov.ru/personal-data/p908/ (дата обращения 12.09.2020).

3. Научная литература:

3.1. Агешкина Н.А., Беляев М.А., Белянинова Ю.В., Бирюкова Т.А., Болдырев С.А., Буранов Г.К., Воробьев Н.И., Галкин В.А., Дудко Д.А., Егоров Ю.В., Захарова Ю.Б., Копьёв А.В. Научно-практический комментарий к Уголовному кодексу Российской Федерации от 13 июня 1996 г. N 63-ФЗ.// Специально для системы ГАРАНТ, 2016 г., URL: http://base.garant.ru (дата обращения 20.09.2020).

3.2. Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С. с. 22, Комментарий к Федеральному закону от 27 июля 2006 г. № 152-ФЗ "О персональных данных", ГАРАНТ, 2013 г. URL: http://base.garant.ru, (дата обращения 18.08.2020).

3.3. Бачило И.Л., Лапина М.А. Актуальные проблемы информационного права (для магистратуры и аспирантуры). М.: Юстиция, 2016 г. - 608 с.

3.4. Волкова О.П. Персональные данные работника и их защита //Кадровик. Трудовое право для кадровика, 2008., 2-10 с.

3.5. Горохов Д.И. Конвенция Совета Европы о защите физических лиц при автоматической обработке персональных данных//Национальная безопасность. 2013. № 1 (24). С. 165—170.

3.6. Гусов К.Н., Лютов Н.Л. Международное трудовое право: Учеб. — М.: Проспект, 2013. – 592 с.

3.7. Орловский Ю. П., Нуртдинова А.Ф. Трудовое право России//Юридическая фирма «Контракт», «Инфра-М», 2014. – 608 с.

3.8. Куренной А.М., Маврина С.П., Сафонов В.А., Хохлов Е.Б. Комментарий к Трудовому кодексу Российской Федерации (постатейный) - 3-е издание, пересмотренное / под ред. – М.: "НОРМА", "ИНФРА-М", 2015

3.9. Буянова М. О., Гусов К. Н. (и др.); Комментарий к Трудовому кодексу Российской Федерации / под ред. К. Н. Гусова. – 11 – изд., перераб. и доп. – //ТК Велби, Проспект, 2011. – 896 с

3.10.Лушникова М.В., Лушников А.М. О перспективах развития законодательства, регулирующего обработку персональных данных // Вопросы трудового права. 2013. № 4. С. 13—20

3.11.Лушникова М.В., Лушников А.М. Информация и персональные данные в сфере трудовых отношений: проблемы теории и практики // Вопросы трудового права. 2013. № 4.С. 21—28.

3.12.Лушников А. М. Неприкосновенность частной жизни и персональные данные в сфере трудовых отношений: стратегия правотворчества в контексте мирового опыта // Юридическая техника. 2015. № 9. С. 410-417

3.13.Международные трудовые стандарты и российское трудовое законодательство: монография / Н. Л. Лютов, Е. С. Герасимова. — 2-е изд., доп. и перераб. — М.: Центр социально-трудовых прав, 2015. — 192 с.

3.14.Михайлов А. В. Проблемы становления цифровой экономики и вопросы развития предпринимательского права //Актуальные проблемы российского права. — 2018. — № 11, с. 56-67.

3.15.Подоплелова О., Рудт Ю., Черновол К. Обзор дел, рассмотренных Конституционным Судом Российской Федерации. // Сравнительное конституционное обозрение. 2013. № 5. с 615.

3.16.Пищита А.Н., Гончаров Н.Г. Юридический регламент обработки персональных данных в медицине: научно-практическое руководство для врачей и юристов. - "РМАПО" (Серия: "Медико-правовой регламент оказания медицинской помощи"), 2013 г. URL: http://base.garant.ru/57734690/#ixzz6debFOwJ2, (дата обращения 18.08.2020).

3.17.Орловский Ю.П., Белицкая И.Я. Прием на работу. Заключение трудового договора: учеб.- практ. пособие // Юридическая фирма «Контракт» : Волтерс Клувер, 2011.— 288 с.

3.18.Приезживая А.А. Научно-практический комментарий / Под ред. зам. руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций//Редакция российской газеты, 2015. С. 29-67.

3.19.Приезжевая А.А. Научно-практический комментарий к Федеральному закону "О персональных данных": - выпуск 11 // Российская газета. 2015, с.177.

3.20. Смирнова Е.В. Видеонаблюдение на рабочих местах: законодательство, позиции судов и Роскомнадзора//Управление персоналом. 2015, с. 21-29.

3.21.Савельев А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». — М.: Статут, 2017., 605 с.

3.22.Солдатова В.И. Защита персональных данных в условиях применения цифровых технологий//Lex russica (Русский закон). 2020;1(2): с. 33-43. URL: https://doi.org/10.17803/1729-5920.2020.159.2.033-043 (дата обращения 15.11.2020)

3.23.Талапина Э. В. Защита персональных данных в цифровую эпоху. Российское право в европейском контексте //Труды Института государства и права РАН. — 2018. — Т. 13. — № 5, с 45-56.

3.24.Хохлов Е.Б., Сафонов В.А., Трудовое право России в 2 т.//– 6-е изд., пер. и доп. – М.: Издательство Юрайт, 2015, с. 703.

3.25.Орловский Ю. П., Трудовое право России: учебник для бакалавров // Издательство Юрайт, 2014. — 854 с.

3.26.Куренной А. М. Трудовое право России. 3-е издание//Проспект, 2015. – 570 с.

3.27.Головина С. Ю., Кучина Ю. А. Трудовое право: учебник для бакалавров/под общ. ред. С. Ю. Головиной. — 2-е изд., перераб. и доп. //Издательство Юрайт, 2015, с 505.

3.28.Чесалина О.В. Защита персональных данных занятых лиц в условия цифровой экономики: сравнительно-правовой анализ законодательства и судебной практики федеративной республики германия и российской федерации //Вестник СГЮА. 2020. №3 (134)., с 8-17, URL: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-zanyatyh-lits-v-usloviya-tsifrovoy-ekonomiki-sravnitelno-pravovoy-analiz-zakonodatelstva-i-sudebnoy (дата обращения: 17.11.2020).

3.29.Mondschein C.F., Monda C. (2019) “The EU’s General Data Protection Regulation (GDPR) in a Research Contex”t. In: Kubben P., Dumontier M., Dekker A. (eds) Fundamentals of Clinical Data Science// Springer, Cham. ISBN: 978- 3-319- 99712- 4, с. 45-66.

3.30.Tomáš Pikulík, Peter Štarchoň (2020) «Public registers with personal data under scrutiny of DPA regulators», Published by Elsevier B.V. This is an open access article under the CC BY-NC- ND license URL: (http://creativecommons.org/licenses/by-nc-nd/4.0/), - с. 1175-1169. (дата обращения: 20.11.2020)

3.31.Ancuţa Gianina Opre, Simona Șandru «Protection of employees’ personal data in the public and private sector, in the context of the new it technologies»// Fiat Iustitia №. 1. 2016. с. 199-208, URL: http://oaji.net/articles/2016/2064-1480331162.pdf (дата обращения, 20.11.2020).

3.32.Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)// National Institute of Standards and Technology (NIST) № 800-122, 59 с. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf, (дата обращения: 20.11.2020)