Общество с ограниченной ответственностью «Дентонс Юроп»

УДК 342

№ госрегистрации:

Инв. №

УТВЕРЖДАЮ
управляющий партнер,
кандидат юридических наук

_____В.Б. Наумов
М.П.

«___»_____2018 года

СОГЛАСОВАНО
_____,

_____
М.П.

«___»_____2018 года

ОТЧЕТ
О НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

по теме:

ОПРЕДЕЛЕНИЕ СОСТАВА СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ СООТВЕТСТВЕННО БАНКОВСКУЮ ТАЙНУ, ТАЙНУ СВЯЗИ, ВРАЧЕБНУЮ ТАЙНУ, КОММЕРЧЕСКУЮ ТАЙНУ И ИНЫЕ ВИДЫ ТАЙН, И ПОРЯДКА ИХ ПЕРЕДАЧИ ТРЕТЬИМ ЛИЦАМ

Руководители НИР:

кандидат юридических наук,
управляющий партнер В.Б. Наумов

кандидат юридических наук,
советник В.В. Архипов

Санкт-Петербург 2018

СПИСОК ИСПОЛНИТЕЛЕЙ

Руководители НИР:

Кандидат юридических наук, управляющий партнер ООО «Дентонс Юроп»	_____	В.Б. Наумов (руководство НИР, разделы 4,5)
Кандидат юридических наук, советник ООО «Дентонс Юроп»	_____	В.В. Архипов (руководство НИР, реферат, введение, заключение, разделы 1.1 – 1.3, 4, 5)

Исполнители НИР:

Юрист ООО «Дентонс Юроп»	_____	Р.А. Ахобекова (разделы 1.1 – 1.3, 1.5)
Юрист ООО «Дентонс Юроп»	_____	Т.А. Бовсуновская (разделы 1.1 – 1.3)
Юрист ООО «Дентонс Юроп»	_____	Я.В. Бутримович (раздел 1.4)
Юрист ООО «Дентонс Юроп»	_____	А.В. Грачева (разделы 1.1 – 1.3, 1.5)
Юрист ООО «Дентонс Юроп»	_____	Е.М. Крамм (раздел 6)
Юрист ООО «Дентонс Юроп»	_____	С.П. Лялькова (разделы 1.1 – 1.3, 1.5)
Юрист ООО «Дентонс Юроп»	_____	В.О. Полыгалов (раздел 1.4)
Юрист ООО «Дентонс Юроп»	_____	К.М. Смирнова (разделы 1.1 – 1.3, 1.5, 3)
Юрист ООО «Дентонс Юроп»	_____	Е.В. Тытюк (разделы 1.1 – 1.3, 1.5, 2)

РЕФЕРАТ

Объем отчета 417 с., 1 часть, 539 использованных источников.

Перечень ключевых слов: тайна связи, врачебная тайна, банковская тайна, налоговая тайна, тайна личной жизни, неприкосновенность частной жизни, персональные данные, информационное право.

Объект исследования: действующие нормы права, правоприменительные практики и тенденции регулирования различных видов тайн в исследуемых юрисдикциях (Россия, ЕС, Великобритания, США, Япония, Сингапур, Южная Корея, Израиль, ОАЭ), на уровне действующих международных договоров Российской Федерации, документации международных организаций. Также в объект исследования включен вопрос о методиках расчета ущерба для компаний, а также оценки вреда, который может быть причинен субъектам тайна в случаях разглашения соответствующих сведений.

Цель работы: обобщение актуальной информации, соответствующей объекту исследования и подготовка предложений о возможных для применения в российской правовой системе (с учетом сложившегося уровня развития и тенденций развития технологий, судебной практики) подходов к формированию понятий, критериев и (или) состава сведений, составляющих различные виды тайн, и порядка их обработки и передачи третьим лицам при условии соблюдения и защиты прав субъектов, а также представление предложений по криминализации или декриминализации ответственности за разглашение различных видов тайн.

Методология проведения работы: исследование основано на общенаучной методологии, предусматривающей использование системного подхода к достижению целей и разрешению задач. Дополнительно при решении отдельных задач использован ряд частнонаучных методов, таких как сравнительно-правовой анализ, формально-юридический анализ, метод интерпретации.

Ввиду значительного объема эмпирического материала, соответствующего, в первую очередь, сравнительно-правовому исследованию по различным юрисдикциям, в основу отбора материала, подлежащего включению в отчет, положен принцип построения отчета исходя из репрезентативных примеров, относящихся к нормам права, правоприменительным практикам и тенденциям регулирования. Как правило, если в исследовании отсутствует либо

лишь кратко упоминается какой-либо аспект, относящийся к определенным видам тайн (или же сами виды тайн как таковые), это подразумевает вывод об отсутствии принципиального значения предмета для основной цели работы.

Кроме того, поскольку условиях технического задания исследования содержали указание на открытый перечень тайн и (или) сведений конфиденциального характера, в свете отмеченного выше обстоятельства, отчет организован таким образом, что в центре исследования находятся четыре «основных» вида тайн, значение которых для целей работы обусловлено контекстом и приоритетами условий цифровой экономики, а именно – тайна связи, врачебная тайна, банковская тайна и налоговая тайна. Иные виды тайн и (или) конфиденциальной информации (например, тайна личной жизни или персональные данные), в случае их релевантности целям и задачам исследования, логически соотнесены с указанными четырьмя видами тайн непосредственно в рамках относящихся к ним разделов исследования.

Результаты работы: в рамках исследования изучены подходы к формированию понятий различных видов тайн, принципам формирования состава сведений, составляющих различные виды тайн, составу таких сведений, разграничению между различными видами конфиденциальной информации, механизмам правовой защиты прав субъектов тайн, юридической ответственности за разглашение указанной информации, порядка и условий передачи таких сведений, в том числе трансграничной, изъятий из режимов тайн, случаев и порядка раскрытия указанных сведений, возможностям доступа к таким сведениям с согласия субъекта тайн, установления ограничений на предоставление таких сведений, возможностей предоставления кредитными учреждениями конфиденциальных данных, форм и способов получения согласий от субъектов тайн, прав и обязанностей специальных категорий лиц, обязанностей по обеспечению соблюдения тайны связи, правового режима абонентских номеров и иных идентификаторов, условий реализации контроля за сведениями при использовании средств связи. Также в исследовании отражен обзор существующих и возможных для применения в России методиках расчета ущерба для компаний и оценки вреда, который может быть причинен субъектам тайн, в случаях разглашения соответствующих сведений. Разработаны предложения о возможных для применения в российской правовой системе (с учетом сложившегося уровня развития и тенденций развития технологий, судебной практики) подходов к формированию понятий, критериев и (или) состава сведений, составляющих различные виды тайн, и порядка их обработки и передачи

третьим лицам при условии соблюдения и защиты прав субъектов, а также представление предложений по криминализации или декриминализации ответственности за разглашение различных видов тайн.

Новизна результатов работы: новизна результатов исследования выражается в системном обобщении актуальной информации, соответствующей объекту исследования и соответствующих предложениях о возможных для применения в российской правовой системе (с учетом сложившегося уровня развития и тенденций развития технологий, судебной практики) подходов. Такое исследование в Российской Федерации проводится впервые. Исследование основано преимущественно на первоисточниках, относящихся к действующим нормам права и правоприменительным практикам.

Область применения: результаты данной научно-исследовательской работы могут быть использованы органами государственной власти, а также научными, образовательными и экспертными организациями при реализации мероприятий, связанных с объектом исследования, в первую очередь при реализации Плана мероприятий по направлению «Нормативное регулирование» программы «Цифровая экономика Российской Федерации», утвержденного 18.12.2017 г. Правительственной комиссией по использованию информационных технологий для улучшения качества жизни и условия ведения предпринимательской деятельности.

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ААС – Арбитражный апелляционный суд

АС – Арбитражный суд

ВС РФ - Верховный Суд Российской Федерации

ГК РФ – Гражданский Кодекс Российской Федерации

Госкомсвязь РФ – Государственный комитет Российской Федерации по связи информатизации

ЕСПЧ – Европейский суд по правам человека

Закон о банках и банковской деятельности – Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности»

Закон об информации – Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Закон об ОРД – Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»

Закон об основах охраны здоровья граждан – Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»

Закон о персональных данных – Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Закон о почтовой связи - Федеральный закон от 17.07.1999 №176-ФЗ «О почтовой связи»

Закон о связи - Федеральный закон от 07.07.2003 N 126-ФЗ «О связи»

Законодательство - Законы, иные НПА, применимые к рассматриваемому вопросу

КоАП – «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ

Конституция РФ – Конституция Российской Федерации

КС РФ - Конституционный Суд Российской Федерации

Мининформсвязь - Министерство информационных технологий и связи Российской Федерации

Минкомсвязь – Министерство связи и массовых коммуникаций Российской Федерации

Минюст – Министерство юстиции

МО – Московская область

НК РФ – Налоговый кодекс Российской Федерации (часть первая – от 31.07.1998 г. № 146-ФЗ, часть вторая – от 05.08.2000 г. № 117-ФЗ).

НПА – Нормативный(-е) правовой(-ые) акт(-ы)

ОРД – Оперативно-розыскная деятельность

ОРМ – Оперативно-розыскные мероприятия

РФ – Российская Федерация

ТК РФ – Трудовой Кодекс Российской Федерации

УК РФ - Уголовный кодекс Российской Федерации

УПК – Уголовно-процессуальный кодекс Российской Федерации

ФАС – Федеральный арбитражный суд

ФСБ – Федеральная служба безопасности

ФСТЭК – Федеральная служба по техническому и экспортному контролю

ВВЕДЕНИЕ

Современное состояние общества характеризуется терминами «информационное общество» и «цифровая экономика». Как отмечает А.В. Белов, «теорий информационного общества достаточно много. Однако, по нашему мнению, они достаточно легко группируются в два основных подхода. Первый включает теории, связанные с концепциями постиндустриализма … В целом они, как и постиндустриальная доктрина, лежат в русле того направления европейской философии, в котором эволюцию человечества принято рассматривать сквозь призму прогресса знания. Второй подход связан с концептуальными схемами О. Тоффлера, Р. Дарендорфа, Ф. Феррароти, а также скорректированной теорией Д. Белла [первый подход]. Именно в их фундаментальных трудах были сформулированы основные черты общества, которое Э. Тоффлер назвал «третьей волной». Так, Д. Белл основными признаками нового общества считает превращение теоретических знаний в источник инноваций и определяющий фактор политики».[1] В свою очередь, пдп. «г» п. 4 Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203 определяет «информационное общество» как «общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан».[2]

Как и в случае с понятием информационного общества, имеется несколько подходов к определению понятия «цифровая экономика». Так, согласно одному из возможных подходов, термин «цифровая экономика» обозначает «тип экономики, характеризующийся активным внедрением и практическим использованием цифровых технологий сбора, хранения, обработки, преобразования и передачи информации во всех сферах человеческой деятельности; систему социально-экономических и организационно-технических отношений, основанных на использовании цифровых информационно-телекоммуникационных технологий; сложную организационно-техническую систему в виде совокупности различных

[1] См.: Белов А.В. Информационное общество и информационная культура в России: к постановке проблемы // Вестн. Волгогр. гос. Ун-та. Сер. 7, Филос. – 2009. - № 1 (9). – С. 198-199.

[2] Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы, утв. Указом Президента Российской Федерации от 09.05.2017 г. № 203. – [Электонный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 08.08.2018).

элементов (технических, инфраструктурных, организационных, программных, нормативных, законодательных и др.) с распределенным взаимодействием и взаимным использованием экономическими агентами для обмена знаниями в условиях перманентного развития».[3] В Разделе I Программы «Цифровая экономика Российской Федерации», утвержденной Распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р,[4] понятие цифровой экономики соотносится с тем, что данные в цифровой форме являются ключевым фактором производства во всех сферах социально-экономической деятельности, что повышает конкурентоспособность страны, качество жизни граждан, обеспечивает экономический рост и национальный суверенитет.

С учетом значения информации для данного социально-экономического контекста неудивительно, что особую актуальность в юридической плоскости приобретают подходы к формированию понятий различных видов тайн (представляющих собой информацию, рассмотренную с точки зрения наиболее значимых квалифицирующих признаков), принципам формирования состава сведений, составляющих различные виды тайн, составу таких сведений, разграничению между различными видами конфиденциальной информации, механизмам правовой защиты прав субъектов тайн, юридической ответственности за разглашение указанной информации, порядка и условий передачи таких сведений, в том числе трансграничной, изъятий из режимов тайн, случаев и порядка раскрытия указанных сведений, возможностям доступа к таким сведениям с согласия субъекта тайн, установления ограничений на предоставление таких сведений и иные вопросы, относящиеся к предметной области исследования.

Данные вопросы актуальны как для Российской Федерации, так и для различных зарубежных юрисдикций, чем и обусловлена необходимость проведения сравнительно правового исследования, нацеленного на анализ текущего состояния нормативно-правового регулирования различных видов тайн в мире, что представляется одним из необходимых условий для развития нормативно-правовой базы в связи с реализацией Программы «Цифровая экономика Российской Федерации».

---

[3] См.: Бабкин А.В., Буркальцева Д.Д., Костень Д.Г., Воробьев Ю.Н. Формирование цифровой экономики в России: сущность, особенности, техническая нормализация, проблемы развития // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. – 2017. – Т.10. – №3. – С. 12.

[4] См.: Программа «Цифровая экономика Российской Федерации», утв. Распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. – [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 08.08.2018).

1. СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ ДЕЙСТВУЮЩИХ НОРМ ПРАВА, ПРАВОПРИМЕНИТЕЛЬНЫХ ПРАКТИК И ТЕНДЕНЦИЙ РЕГУЛИРОВАНИЯ

1.1. Тайна связи

Российская Федерация

Понятие и принципы отнесения. Понятие тайны связи определяется в Конституции (ст. 23), Законе о связи (ст. 63), Законе о почтовой связи (ст. 15). Согласно данным НПА тайна связи означает тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электросвязи и по сетям почтовой связи.

В Законодательстве принципы формирования сведений, составляющих тайну связи, не определены. Тем не менее, можно сформулировать следующие принципы на основании системного толкования применимых НПА и судебной практики:

(1) Отнесение к тайне связи любых сообщений вне зависимости от технического способа передачи;

(2) Открытый перечень сведений, относящихся к тайне связи;

(3) Основной критерий отнесения технической информации и персональных данных к тайне связи, который можно сформулировать, несмотря на неоднозначность судебной практики: возможность разглашения любых деталей коммуникации, в том числе факта существования, участников и иных обстоятельств, в случае раскрытия такой информации.

Фактический состав сведений, относящихся к тайне связи. Согласно применимым НПА, правовым позициям КС РФ и судебной практике других судов следующие сведения составляют тайну связи:

(1) Содержание любых сообщений, вне зависимости от средства передачи (через сети почтовой связи, посредством электросвязи, Интернет), в том числе любые вложения, документы, информация, приложенные к таким сообщениям (ст. 63 Закона о связи, ст. Закона о почтовой связи, Постановление КС РФ от 26 октября 2017 г. N 25-П);

(2) Содержание телефонных переговоров, а именно любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры (Определение КС РФ от 2 октября 2003 г. №345 -О);

(3) Сведения о почтовых переводах денежных средств (ст. 63 Закона о связи);

(4) Сведения о передаваемых по сетям электросвязи и сетям почтовой связи сообщениях, о почтовых отправлениях, то есть метаданные (ст. 63 Закона о связи). Интересно, что изначально тайной связи охранялось только содержание самих сообщений. Постепенно состав сведений был расширен и стал включать разного рода метаданные[5].

На данный момент самым неоднозначным является ***вопрос о составе метаданных и технической информации, которая относится к тайне связи***. Применимые НПА не содержат полного перечня таких сведений, понятие тайны связи определено через описательные категории. При этом судебная практика по данному вопросу не является единообразной.

Анализ российской судебной практики позволяет следующим образом определить перечень метаданных и технической информации, составляющих тайну связи:

- Данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи (Определение КС РФ от 2 октября 2003 г. №345 –О, Определение КС РФ от 21 октября 2008 г. №525 – О-О);
- Данные детализации счета абонентов с указанием даты и времени всех состоявшихся соединений, их продолжительности и абонентских номеров, равно как и идентификационный номер абонентского устройства (IMEI), данные о соединениях между конкретными абонентами (дате, времени, продолжительности), IP-адреса в той мере, в которой они позволяют определить коммуникации пользователей услуг связи (Постановление 9ААС от 6 августа 2014 г. по делу № А40-57559/14, Постановление ФАС МО от 12 марта 2014 г. по делу № А40-56142/13-130-551, Постановление 9ААС от 28 ноября 2014 г. по делу № А40-113991/13);

[5] Терещенко Л.К. Отдельные вопросы, возникающие в судебной практике при применении норм о тайне связи [Электронный ресурс] // Комментарий судебной практики / отв. ред. К.Б. Ярошенко. М.: Институт законодательства и сравнительного правоведения при Правительстве РФ, ИНФРА-М, 2016. – С. 145-153. – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 08.08.2018).

- Сведения об адресах электронной почты, в том числе адреса электронной почты, с которых пользователями осуществляется сбор почты, адреса электронной почты, с которыми пользователями осуществляется переписка и на которые перенаправляется переписка (Постановление 9 ААС от 05 мая 2014 г. по делу № А40-153867/13).

Как было отмечено ранее судебная практика по вопросу отнесения абонентских номеров и иных идентификаторов абонентских устройств (в том числе серийный номер мобильного телефона (IMEI), номер IMSI, динамический или статический IP-адрес устройства в сети Интернет, уникальный идентификатор оборудования сетей передачи данных (MAC-адрес) к тайне связи не является однозначной.

Вместе с тем, можно отметить следующее:

(1) Как правило, суды прямо относят IMEI к информации, составляющей тайну связи (см., например, Постановление 9 ААС от 6 августа 2014 г. по делу № А40-57559/14, Постановление ФАС МО от 12 марта 2014 г. по делу № А40-56142/13-130-551, Решение АС г. Москвы от 19 мая 2014 г. по делу N А40-28184/14). Такая практика основывается, главным образом, на правовых позициях, высказанных КС РФ (Определение КС РФ от 2 октября 2003 г. №345 –О, Определение КС РФ от 21 октября 2008 г. №525 – О-О, п. 11 Постановление Пленума Верховного Суда РФ от 01.06.2017 N 19). Есть и противоположная практика: см., например, Постановление ФАС МО от 15 января 2014 г. по делу № А40-56844/13-149-539.

(2) Судебная практика по вопросу отнесения IP-адресов к тайне связи не является столь однозначной. Суды чаще всего не признают IP-адреса информацией, составляющей тайну связи, поскольку такая информация относится к персональным данным абонента (Проставление Курганского областного суда от 15 августа 2015 г., Постановление 8 ААС от 12 октября 2016 г. по делу № А70-5136/2016).

(3) По вопросу об отнесении адресов электронной почты к тайне связи есть прямо противоположные решения (Постановление 9 ААС от 05 мая 2014 г. по делу № А 40-153867/13: адреса были признаны частью тайны связи, Постановление ФАС МО по делу № А40-56844/13-149-539 от 15 января 2015 г.: электронные адреса признаны неохраняемыми тайной связи).

(4) Однако, учитывая последние решения ВС РФ, можно заключить, что судебная

практика складывается таким образом, что определяющее значение для отнесения той или иной технической информации, в том числе абонентских номеров, IMEI, IP-адресов к тайне связи, имеет тот факт, **запрашивается ли такая информация применительно к коммуникациям абонента или самостоятельно.** Например, сами по себе, без привязки к коммуникациям пользователей IP-адреса, как статические, так и динамические, к сведениям составляющим тайну связи, не относятся (хотя, например, Роскомнадзор относит статические IP-адреса к персональным данным). Данная правовая позиция подтверждается постановлением ВС РФ, который указал следующее: «*Судебные инстанции обоснованно исходили из того, что предоставляя органам, осуществляющим оперативно-розыскную деятельность, данные о пользователе услуг связи, установленные как по статистическому IP-адресу (назначаемому оператором связи как постоянный адрес, закрепленный за оконечным пользовательским оборудованием пользователя при заключении договора на оказание услуг доступа к сети Интернет), так и по динамическому IP-адресу, оператор связи не вторгается в охраняемую законодательством тайну связи*» При этом такие ведения могут охраняться как персональные данные. Если же речь идет о предоставлении детализации звонков, иных деталях коммуникации, то IMEI, абонентские номера, IP-адреса и т.д. рассматриваются как сведения, составляющие тайну связи (Постановление ВС РФ от 11 октября 2016 г. N 82-АД16-5).

В судебной практике также прослеживается **разделение между информацией, составляющей тайну связи, и информацией о пользователях услугами связи**, в особенности, если такая информация запрашивается не в связи с сообщениями, переданными такими пользователями. Как правило, суды и иные государственные органы, не относят к тайне связи сведения об абонентах и оказываемых услугах, например, ФИО абонентов, информация о подключениях к Интернет-ресурсам и т.д. (см., например, Постановление Курганского областного суда от 10 августа, 2015 г. № 4А-178/2015, Постановление 8 ААС от 12 октября 2016 г. по делу № А70-5136/2016).

При этом и в данном случае, как показывает складывающаяся судебная практика, ***основным определяющим критерием отнесения той или иной информации к тайне связи является отсутствие или наличие связи такой информации с коммуникациями пользователей***. Если персональная информация абонентов/пользователей услуг связи

запрашивается в связи с коммуникациями абонентов/пользователей, например, детализация звонков, то такая информация может быть отнесена к тайне связи.

Сведения, составляющие тайну связи, могут одновременно охраняться как иные виды тайн и относиться к другим видам сведений ограниченного характера, в том числе:

(1) Относиться к персональным данным;

(2) Охраняться как тайна личной жизни (тайна связи и тайна личной жизни соотносятся как часть и целое);

(3) Охраняться как банковская тайна (информация о почтовых переводах денежных средств одновременно охраняется как банковская тайна и как тайна связи);

(4) Охраняться как государственная тайна (информация, полученная следственными органами и органами, осуществляющими ОРД, в результате установления контроля над телефонными переговорами/корреспонденцией, переходит в режим государственной тайны).

Механизм правовой защиты тайны связи и юридическая ответственность. Механизм правовой защиты субъектов состоит из следующих элементов:

(1) Недопустимости ограничения права на тайну связи иначе, чем на основании федеральных законов и, как правило, при наличии судебного решения (ч. ст. 23 Конституции, ч. 3 ст. 55 Конституции, ч. 4 ст. 63 Закона о связи). Стоит отметить, что в отличие от некоторых других прав и свобод человека и гражданина, предусмотренных Конституцией, в отношении права на тайну связи предусмотрена дополнительная гарантия ее защиты: тайна связи может быть ограничена только в объеме и по основаниям, предусмотренным федеральными законами, ***и в случаях, предусмотренных такими федеральными законами,*** при наличии судебного решения. Важно отметить, что суды ***не вправе*** выносить решения, ограничивающие тайну связи в отсутствие законных оснований, что подтверждается и судебной практикой (Апелляционное определение Ставропольского краевого суда от 10 октября 2014 г. по делу №33-5536/2014). При этом федеральные законы могут содержать дополнительные ограничения тайны связи, когда не требуется наличие судебного решения. Это единичные исключения, которые будут перечислены далее. Таким образом, тайна связи, как правило, за очень редкими исключениями может быть ограничена на основании федеральных законов при наличии судебного решения либо только на основании федеральных

законов, без судебного решения.

(2) Установление обязательств в отношении операторов связи по обеспечению соблюдения тайны связи, в том числе установление обязательных требований к оборудованию, используемому при оказании услуг связи (подробнее см. раздел об информационной безопасности);

(3) Возможность подачи жалоб и претензий в соответствии со специальной процедурой, предусмотренной Законом о связи (статья 55 Закона о связи) и иными НПА, по вопросам, связанным с оказанием услуг связи (стоит отметить, что данная процедура прямо не предусматривает возможность подачи жалоб в связи с нарушением тайны связи);

(4) Право на получение информации об оказываемых услугах связи (см., например «Правила оказания услуг связи по передаче данных», утвержденные Постановлением Правительства РФ от 23.01.2006 №32; аналогичное право предусмотрено в правилах оказания услуг связи иных видов);

(5) Возможность обращения в суд за защитой права на тайну связи с гражданско-правовым иском (в том числе о возмещении морального вреда, материального ущерба, пресечении действий, нарушающих права и т.д.).

За нарушение тайны связи предусмотрены следующие виды ответственности:

(1) Уголовная ответственность в виде штрафа до трехсот тысяч рублей, обязательных работ на срок до четырехсот восьмидесяти часов, либо принудительных работ на срок до четырех лет, либо лишения свободы на срок до четырех лет[6] (ст. 138 УК РФ).

(2) Уголовная ответственность за нарушение тайны личной жизни (поскольку сведения, составляющие тайну связи, представляют собой частный случай тайны личной жизни). Уголовная ответственность в виде штрафа до трехсот тысяч рублей/в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до

[6] Здесь и далее приводятся самые строгие санкции за соответствующие нарушения, предусмотренные, как правило, в случае совершения правонарушения с квалифицирующим составом.

пяти лет или без такового, либо арестом на срок до шести месяцев, либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет (ст. 137 УК РФ).

(3) Административная ответственность в соответствии со ст.13.11 КоАП (нарушение законодательства об обработке персональных данных), ст. 13.14 КоАП (за разглашение сведений конфиденциального характера лицом, получившим доступ к таким сведениям с использованием служебного положения), ч.3 ст.14.1 КоАП (за осуществление предпринимательской деятельности с нарушением требований и условий лицензии). Отдельный состав именно за нарушение тайны связи КоАП не предусмотрен.

(4) Гражданско-правовая ответственность на основании исков о компенсации морального вреда, возмещения убытков, причинении вреда.

(5) При грубом нарушении оператором связи обязательств по сохранению тайны связи и неустранении предписания о прекращении нарушения теоретически возможно также аннулирование лицензии оператора связи.

Тайна связи является одним из видов конституционных прав, гарантируемых Конституцией РФ. Более того, тайна связи относится к основным правам и свободам гражданина. Соответственно, тайна связи охраняется как разновидность конституционных прав.

Порядок и условия предоставления третьим лицам сведений, составляющих тайну связи. Относительно порядка и условий передачи третьим лицам, сведений составляющих тайну связи, можно отметить следующее.

1. Предусмотренные Законодательством случаи и порядок предоставления третьим лицам сведений, составляющих тайну связи, как правило, относятся к ограничениям, установленным в публично правовых целях. В частности:

(1) Предоставление сведений, составляющих тайну связи, допускается только на основании решения суда в объеме и на основаниях, предусмотренных федеральными законами, если иное не установлено федеральными законами (ч. 2 ст. 23 Конституции РФ, ч. 3 ст. 63 Закона о связи, п. 14 Постановлении Пленума Верховного Суда Российской Федерации от 31 октября 1995 г. N 8);

(2) Основными законодательными источниками, определяющими порядок вынесения

судебного решения о предоставлении сведений, составляющих тайну связи, являются УПК и Закон об ОРД.

(3) УПК определяет следующие условия доступа следователей к различным сведениям, составляющим тайну связи:

- К электронным сообщениям и иным сообщениям, передаваемым по сетям электросвязи - при наличии достаточных оснований полагать, что сведения, имеющие значение для уголовного дела, могут содержаться в таких сообщениях (ст.185 УПК РФ);
- К телефонным переговорам путем их записи и контроля - при наличии достаточных оснований полагать, что сведения, имеющие значение для уголовного дела, могут содержаться в переговорах обвиняемого, подозреваемого и других лиц при производстве по делам о преступлениях средней тяжести, тяжких и особо тяжких преступления (ст.186 УПК РФ);
- К информации о соединениях между абонентами и (или) абонентскими устройствами - при наличии достаточных оснований полагать, что эта информация имеет значение для уголовного дела (ст.186.1 УПК РФ).

Доступ к информации, предусмотренной в настоящем пункте, осуществляется при наличии судебного решения, вынесенного в соответствии со ст. 165 УПК РФ. Ст. ст. 186 и 186.1 УПК также содержат нормы о правилах и процедуре получения разрешения суда на доступ к соответствующей информации, в том числе об указании в ходатайстве сведений, необходимых для получения соответствующего судебного решения.

(4) Закон об ОРД предусматривает порядок и основания доступа к информации, составляющей тайну связи, при проведении оперативно-розыскных мероприятии. Органы, ведущие ОРД, получают доступ к соответствующим сведениям при наличии решения суда (ст. 8, 12 Закона об ОРД)[7].

(5) Таким образом, основным основанием предоставления сведений, составляющих тайну связи, является судебное решение[8], которое должно быть мотивированным и

[7] Поскольку в данном случае речь идет не о передаче информации операторами связи, а об установлении контроля переписки и переговоров, Исполнитель не описывает подробно условия предоставления доступа к соответствующим сведениям.

[8] Стоит еще раз отметить, что судебное решение может иметь место только в том случае, если возможность доступа к сведениям, составляющим тайну связи, предусмотрен федеральными законами.

обоснованным, о чем неоднократно высказывались высшие судебные инстанции (определения КС РФ, ВС РФ из ЕСПЧ).

(6) Стоит отметить, что сведения о тайне связи, полученные органами следствия и органами, осуществляющими ОРД, впоследствии переходят в режим государственной тайны и обрабатываются соответствующими органами уже как государственная тайна.

(7) Вынесение судебного решения для передачи сведениям, составляющим тайну связи, не требуется в случаях, предусмотренных Законодательством, в том числе[9] для предотвращения, выявления и пресечения Банком России неправомерного использования инсайдерской информации в части предоставления информации о почтовых переводах денежных средств.

(8) Передача сведений, составляющих тайну связи третьим лицам по иным основаниям, чем судебное решение, не допускается (за исключением случаев, предусмотренных федеральными законами). При этом закон не делает исключений ни для аффилированных лиц, ни для аудиторов, ни для иных третьих лиц, что находит подтверждение в судебной практике (Постановление 9 ААС от 6 августа, 2014 г. по делу № А40-57559/14: в данном деле ОАО «Мегафон» было привлечено к ответственности за предоставление сведений, составляющих тайну связи, своему аффилированному лицу).

Закон о связи предусматривает, что предоставление третьим лицам сведений об абоненте может осуществляться только с их согласия за исключением случаев предоставления органам, осуществляющим ОРД и ФСБ. Правила получения такого согласия определены в Законе о персональных данных. Как было предусмотрено выше, сведения об абонентах также относятся к персональным данным.

2. При этом специальных правил и норм, определяющих порядок передачи (в том числе трансграничной) сведений, составляющих тайну связи, коммерческим организациям, Законодательством не установлено.

Вероятно, это связано с тем, что оператор связи (лицо, оказывающее услуги почтового/иного сервиса) по сути, не является законным обладателем и пользователем информации, составляющей тайну связи, в особенности содержания самих сообщений (это

[9] Остальные случаи относятся к досмотру товаров на таможенной границе, и иным подобным случаям, которые не связаны с коммерческим использованием соответствующих данных.

согласуется с позицией КС РФ по делу Сушкова А.И.). В этом существенное отличие тайны связи от иных видов профессиональной тайны, например, врачебной и банковской тайны, где большая часть сведений, составляющие соответствующие виды тайны, сообщаются банкам/медицинским организациям для целей оказания услуг (лечения). Таким образом, банки/медицинские учреждения являются именно законными пользователями соответствующей информации и остается определить пределы такого использования. Напротив, операторы связи не должны иметь доступа к самим сообщения, телефонным переговорам и т.д., чтобы оказывать услуги: достаточно владеть только персональными данными абонентов.

Работники оператора связи не вправе без законных оснований и решения суда производить осмотр сообщений, вскрывать их и т.д. Такой вывод следует из системного толкования положений законодательства и правоприменительной практики, несмотря на формулировки ч. 3 ст. 63 Закона о связи. Хотя данная норма и говорит об уполномоченных сотрудниках оператора связи, в законодательстве нигде не раскрывается перечень таких лиц «уполномоченных сотрудников», ни основания их доступа к соответствующей информации. Такое толкование подтверждается и в литературе[10].

Учитывая вышеизложенное, логично, что Законодательство не содержит специальных норм относительно правил получения и администрирования согласий, на предоставление третьим лицам сведений, составляющих тайну связи. Тем не менее, возможность доступа к таким сведениям с согласия субъекта тайны следует из некоторых положений Законодательства. Так, Закон об ОРД предусматривает возможность прослушивания переговоров по письменному заявлению лиц, жизни, здоровью, собственности которых угрожает опасность (ст. 8 Закона об ОРД). Следует отметить, что специфика большей части сведений, составляющих тайну связи такова, что, скорее всего, для ее использования и раскрытия согласия одного лица не достаточно, так как такая информация, как правило, представляет собой тайну связи или тайну личной жизни одного и более лиц. Принимая во внимание данный факт, некоторые авторы придерживаются мнения о том, что субъект тайны связи не может предоставлять согласия на использование соответствующей информации[11].

---

[10] Волков Ю.В., Вахрушева Ю.Н. Комментарий к Федеральному закону от 7 июля 2003 г. N 126-ФЗ «О связи» [Электронный ресурс] // отв. ред. Л.К. Терещенко. – 2016. – С. 125

[11] Федотов Н.Н. Тайна связи против технических средств защиты информации в Интернете [Электронный ресурс] / Н.Н. Федотов // «Форензика – компьтерная криминалистика» [Сайт]. – URL: http://forensics.ru/zi-ts.html#lit05 (дата обращения: 08.08.2018).

В том случае, если сведения составляющие тайну связи, включают персональные данные, порядок доступа и использования таких данных регулируется Законом о персональных данных; если речь идет о тайне частной жизни, то доступ и использование может также регулироваться ГК РФ.

Специальных детализированных правил по форме согласия в отношении использования тайны связи Законодательство также не содержит. Однако различные правила оказания услуг связи и Закон о связи предусматривают, что информация об абонентах может предоставляться только с письменного согласия абонентов.

Законодательство не содержит прямых норм, регулирующих порядок доступа специальных категорий лиц (агентов, посредников, подрядчиков, в т.ч. юридических лиц, обслуживающих программно-аппаратные комплексы) к сведениям, составляющим тайну связи. Тем не менее, из законодательства вытекает, что такие категории субъектов не вправе использовать, передавать третьим лицам, разглашать или иным образом обрабатывать сведения, составляющие тайну связи. Как предусмотрено выше, и сами операторы связи, сервисы обмена сообщениями и иные подобные организации, оказывающие услуги в данной области, не являются обладателями информации в том смысле, который предусмотрен Законом об информации, и соответственно не могут ее использовать или определять порядок использования. Такие организации лишь обязаны хранить соответствующие данные с обеспечением законодательных предписаний в части обеспечении безопасности.

В том случае, если сведения, составляющие тайну связи, включают персональные данные, необходимо руководствоваться Законом о персональных данных. В иных случаях – Законом об информации и ГК РФ.

Случаи, условия и порядок использования и получения доступа к информации, составляющей тайну связи, без согласия субъекта тайны, главным образом, определяется УПК и Законом об ОРД.

Если говорить об изъятиях из режима охраны в социальных, государственных, экономических целях предоставления сведений о соединениях по сети электросвязи государственным органам, не осуществляющим ОРД или обеспечение безопасности, в том числе в рамках защиты инсайдерской информации, то единственным изъятием из режима тайны является возможность получения Банком России без решения суда сведений, составляющих тайну вязи в части информации о почтовых переводах денежных средств) и иную охраняемую законом тайну, для целей предотвращения использования инсайдерской

информации. При этом Банк России не вправе получать другие сведения, составляющие тайну связи, без решения суда.

Стоит отметить, что в случаях, которые не терпят отлагательства и могут привести к совершению тяжкого или особо тяжкого преступления, а также при наличии данных о событиях и действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации, на основании мотивированного постановления одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, допускается проведение данных оперативно-розыскных мероприятий с обязательным уведомлением суда (судьи) в течение 24 часов. (ст. 8 Закона ОРД).

Учитывая, специфику сведений, составляющих тайну связи, их раскрытие в форме открытых данных или иным подобным образом Законодательством не предусмотрено. Даже публикация информации об абонентах в общедоступной базе данных об абонентах операторов связи требует согласия абонента (ч.2 ст.53 Закона о связи).

Законодательство, в том числе ТК РФ, Закон о связи, Конституция РФ, прямо не предусматривает возможность установления контроля в отношении служебной корреспонденции работника, телефонными переговорами, Интернет-соединений, осуществляемых в служебных целях. Территориальные органы инспекции труда, должностные лица инспекции труда неоднократно высказывались о том, что видеонаблюдение, прослушивание телефонных переговоров, просмотр корреспонденции и т.п. возможны только с согласия/уведомления работников[12]. Аналогичное мнение высказывается и в литературе[13]. Таким образом, учитывая отсутствие прямого регулирования по вопросу прослушивания телефонных переговоров, просмотра корреспонденции и т.п., работодателям рекомендуется заключать с работниками соглашение, которое будет предусматривать, (а) что с рабочих мест и с использованием рабочего оборудования не будет осуществляться личная переписка и переговоры, (б) что работник имеет доступ к соответствующей информации и может ее проверять в рабочих целях (Постановление КС РФ

[12] См., например, Видеонаблюдение и «прослушка» в офисе: мнение Роструда [Электронный ресурс] // Статья из журнала «ГЛАВНАЯ КНИГА» [Сайт] – 2012. – №9. – URL: http://glavkniga.ru/elver/2012/9/640-videonabludenie_proslushka_ofise_mnenie_rostruda.html (дата обращения 08.08.2018); О некоторых вопросах в сфере трудовых отношений. [Электронный ресурс]: государственная инспекция труда в г. Санкт-Петербург. – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 08.08.2018).

[13] См., например, Юшкевич А.В. Актуальные вопросы соблюдения тайны связи // Правовые вопросы связи – 2008. – № 1. – С. 26-28.

от 26 октября 2017 г. №25-П).

Обзор требований информационной безопасности, предусмотренных для операторов связи. Требования к операторам связи в части обеспечении информационной безопасности, в том числе к использованию сертифицированного оборудования, имеют под собой различные законные основания и включают требования разного характера. В частности, можно выделить следующие элементы:

1. Требования, вытекающие из обязанности к обеспечению защиты персональных данных, которые определяются, в частности, следующими НПА:
   - Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ;
   - Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
   - Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 N 28375);
   - Приказ ФСБ России от 10.07.2014 № 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» (Зарегистрировано в Минюсте России 18.08.2014 N 33620)
2. Требования, вытекающие из характера оказываемых услуг.

   Для обеспечения надлежащего качества услуг и недопущения утечки информации операторы связи обязаны:

   (1) Использовать сертифицированные средства связи (ст. 41 Закона о связи). Детальные требования к порядку сертификация, перечни оборудования и т.д. определяются в подзаконных НПА. В частности, к таким НПА относятся:

- **Постановление Правительства РФ от 13.04.2005 № 214** «Об утверждении Правил организации и проведения работ по обязательному подтверждению соответствия средств связи»;
- **Приказ Минкомсвязи России от 01.02.2016 № 28** «Об утверждении Порядка осуществления контроля за соблюдением держателями сертификатов соответствия и декларантами обязательств по обеспечению соответствия поставляемых средств связи установленным требованиям».
- **Постановление Правительства РФ от 25.06.2009 N 532** «Об утверждении перечня средств связи, подлежащих обязательной сертификации».

(2) Руководствоваться при проектировании, построении, реконструкции, вводе в эксплуатацию и эксплуатации сетей связи нормативными правовыми актами федерального органа исполнительной власти в области связи, осуществлять построение сетей связи с учетом требований обеспечения устойчивости и безопасности их функционирования (ч. 1 ст.46 Закона о связи). Такие требования, в том числе определяются следующими НПА:

- **Приказ Минкомсвязи России от 30.09.2015 N 371** «Об утверждении требований к построению, управлению, нумерации, организационно-техническому обеспечению устойчивого функционирования, условиям взаимодействия, эксплуатации сети связи при оказании универсальных услуг связи» от 12.12. 2015;
- **Приказ Мининформсвязи РФ от 13.02.2008 № 18** «Об утверждении Требований к системному проекту сети связи»

(3) Дополнительные требования также могут предусматриваться в отношении разных видов услуг и оборудования, которое используется операторами связи. Например, следующие НПА предъявляют дополнительные требования к оборудованию, используемому операторами связи, в части обеспечения безопасности информации:

- **Приказ Мининформсвязи России от 08.04.2008 № 38** (ред. от 23.04.2013) «Об утверждении Правил применения аппаратуры повременного учета продолжительности соединения». Так, пункт 22 предусматривает следующие требования к аппаратуре повременного учета продолжительности соединения:

1) ведение перечня информационных массивов АПУС, доступ к которым

контролируется в соответствии с законодательством в области защиты информации и требованиями оператора связи, с указанием уровня полномочий и прав доступа к каждому информационному массиву;

2) ведение перечня лиц, имеющих доступ к штатным средствам и рабочим местам АПУС, с указанием их полномочий;

3) задание матрицы доступа или полномочий субъектов доступа по отношению к защищаемым ресурсам АПУС;

4) проверку правильности предоставления полномочий и прав доступа;

5) идентификацию и аутентификацию персонала, отвечающего за эксплуатацию и техническое обслуживание АПУС;

6) регистрацию в электронных журналах (журналирование) действий персонала.

- **Приказ Мининформсвязи РФ от 02.07.2007 №73** «Об утверждении Правил применения автоматизированных систем расчетов»;
- **Приказ Минкомсвязи России от 19.01.2016 №3** «Об утверждении Требований к порядку организационно-технического взаимодействия операторов подвижной радиотелефонной связи при обеспечении перенесения абонентского номера»;
- **Приказ Минкомсвязи России от 21.03.2017 № 129** «Об утверждении Правил применения оборудования транзитных, оконечно-транзитных и оконечных узлов связи. Часть XV. Правила применения комбинированных телефонных станций, использующих технологии мультисервисных сетей и т.д.

3. Требования, связанные с обязанностью обеспечить возможность проведения оперативно-розыскных мероприятий. В частности, ст. 64 Закона о связи устанавливает объем и сроки хранения результатов коммуникации, а также предусматривает обязанность соответствия используемого оборудования определенным требованиям для возможности проведения ОРМ. Такие требования детализированы в подзаконных НПА, в том числе:
   - **Приказ Госкомсвязи РФ от 20.04.1999 № 70** «О технических требованиях к системе технических средств для обеспечения функций оперативно-розыскных мероприятий на сетях электросвязи Российской Федерации»;
   - **Приказ Минкомсвязи России от 26.02.2018 № 86** «Об утверждении Правил применения оборудования систем коммутации, включая программное

обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть IV..»;

- **Приказ Минкомсвязи России от 12.12.2016 № 645** «Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть I…»;
- **Приказ Минкомсвязи России от 27.06.2016 № 285** «Об утверждении требований к сетям электросвязи для проведения оперативно-розыскных мероприятий. Часть III. Требования к сетям телеграфной связи для проведения оперативно-розыскных мероприятий»;
- **Приказ Минкомсвязи России от 23.07.2015 № 279** «Об утверждении Требований к оборудованию и программному обеспечению операторов почтовой связи для обеспечения доступа к базам данных об оказанных услугах почтовой связи и пользователях услугами почтовой связи при проведении оперативно-розыскных мероприятий»;
- **Приказ Минкомсвязи России от 23.07.2015 N 276** «Об утверждении Требований к оборудованию автоматизированной сортировки почты, обеспечивающему выполнение установленных действий при проведении оперативно-розыскных мероприятий»;
- **Приказ Минкомсвязи России от 16.04.2014 № 83** «Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть III…».
- Иные НПА.

Заслуживает внимания репрезентативная ***судебная практика Российской Федерации и ЕСПЧ*** по вопросам обработки и защиты информации, составляющей соответствующие виды тайн. В частности, можно отметить следующие судебные решения.

Постановление Конституционного Суда Российской Федерации от 26 октября 2017 г. №25-П. Гражданин Сушков А.И. обратился в КС РФ с жалобой о том, что положения п. 5 ст. 2 Закона об информации не соответствуют Конституции РФ в той мере, в какой они позволяют считать правообладателей почтовых и иных подобных сервисов (в рассматриваемом случае ООО «Мэйл.ру») обладателями любой информации и сообщений,

которые направляются пользователями таких сервисов.

Основанием подачи жалобы стало предшествующее судебное разбирательство, в рамках которого решался вопрос относительно законности увольнения Сушкова А.И. в связи с разглашением им коммерческой тайны работодателя, выразившейся в отправке на свой личный почтовый адрес сообщения, содержащего коммерческую тайну работодателя. Суды пришли к выводу о законности увольнения, в связи с тем, что отправку сообщения на личный адрес можно считать разглашением информации, поскольку обладателем отправленной в сообщении информации становится лицо, обслуживающее соответствующий сервис.

КС РФ принял жалобу в связи с важностью поставленного вопроса. Предметом рассмотрения КС РФ был следующий вопрос: «… *законоположение, которое понимается в правоприменительной практике как позволяющее считать лицо, оказывающее услуги электронной почты, обладателем информации, которая содержится в электронных сообщениях, получаемых или отправляемых пользователями этих услуг*». Рассматривая жалобу Сушкова А.И., КС РФ пришел к следующим важным выводам:

(1) Лицо, оказывающее услуги электронной почты, обладателем информации, которая содержится в электронных сообщениях, получаемых или отправляемых пользователями этих услуг, **не является** в соответствии с Законом об информации.

(2) Обладателем информации является пользователь почтовых услуг – отправитель электронных сообщений.

(3) Статус почтового сервиса (иных лиц, которые оказывают подобные услуг в сети Интернет) схож со статусом операторов связи, несмотря на то, что Законодательство прямо об этом не говорит. В этой связи лица, оказывающие соответствующие услуги, иные организаторы распространения информации в сети Интернет, обязаны обеспечивать тайну связи, предпринимать технические и организационные меры, направленные на недопущение разглашения.

Постановление ЕСПЧ по делу Романа Захарова против Российской Федерации от 4 декабря 2015 г. Роман Захаров обратился в ЕСПЧ в связи с тем, что, по его мнению, система тайного прослушивания мобильной телефонной связи в Российской Федерации нарушила его право на уважение личной жизни и переписки и что у него отсутствовали эффективные средства правовой защиты в этом отношении. По мнению Романа Захарова, система прослушивания телефонных переговоров не предусматривает гарантий, предотвращающих произвольное и незаконное прослушивание, а также не предоставляет

возможности обжаловать незаконное прослушивание переговоров.

ЕСПЧ оценивал доступность внутригосударственного законодательства, сферу действия и продолжительность меры скрытого наблюдения, процедуры хранения, доступа, изучения, использования, передачи и уничтожения полученных данных, процедуры санкционирования, порядок надзора за осуществлением мер скрытого наблюдения, любые механизмы уведомления и средства правовой защиты, предусмотренные национальным законодательством.

Исследовав названные выше вопросы, ЕСПЧ пришел к выводу о том, что предусмотренные в России правила прослушивания телефонных переговоров, в том числе основания, объемы прослушивания, возможность обжалования пришел к выводу о том, что законодательство Российской Федерации не соответствует требованию «качества закона» и не в состоянии определять «вмешательство» в рамках того, что является «необходимым в демократическом обществе», и присудил выплатить Роману Захарову компенсацию.

Ниже приведены некоторые из основных аргументов ЕСПЧ, которые были положены в основу решения:

(1) Законодательство Российской Федерации не дает гражданам каких-либо указаний на обстоятельства, при которых материал прослушивания может храниться после окончания судебного заседания. Исходя из изложенного Европейский Суд считает, что внутригосударственное законодательство не является достаточно точным в этой части.

(2) Процедуры разрешения, предусмотренные законодательством Российской Федерации, не способны обеспечить того, чтобы меры скрытого наблюдения не назначались случайно, беспорядочно и без соответствующего рассмотрения.

(3) Прокурорский надзор за прослушиванием в том виде, в котором он в настоящее время действует, не способен обеспечить адекватные и эффективные гарантии против произвола

(4) Законодательство Российской Федерации не предусматривает эффективных средств правовой защиты для лица, которое подозревает, что подверглось скрытому наблюдению. Лишая прослушиваемое лицо реальной возможности обжаловать прослушивание ретроспективно, законодательство Российской Федерации, таким образом, избегает важной гарантии против неправомерного использования мер скрытого наблюдения.

Определение КС РФ от 2 октября 2003 г. № 345-О и Определение КС РФ от 21 октября 2008 г. № 528-О-О. Названные определения КС РФ содержат важные для понимания содержания тайны связи правовые позиции. В частности, КС РФ высказал позицию о том, что тайной связи должны охраняться следующие сведения: «*…к информации, составляющей охраняемую Конституцией Российской Федерации и действующими на территории Российской Федерации законами тайну телефонных переговоров, относятся любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи; для доступа к указанным сведениям необходимо получение судебного решения*». Тем самым КС РФ дал основание судам и иным правоприменительным органам для широкого толкования метаданных о коммуникациях, которые должны охраняться тайной связи. Впоследствии данные определения КС РФ сыграли важную роль для формирования российской судебной практики по вопросу о содержании тайны связи.

Определение КС РФ от 25 января 2018 г. № 189-О. С жалобой в КС РФ обратился подозреваемый по уголовному делу, которому было отказано в признании недопустимыми доказательствами сведений, которые были получены в ходе взлома и извлечения информации из телефона, обнаруженного при его задержании и обыске. Телефон был взломан, а содержимое, в том числе корреспонденция, были изучены без судебного решения в соответствии со ст. 165 УПК РФ. КС РФ вынес определение об отказе в рассмотрении и высказал следующую позицию: «*Проведение осмотра и экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения*».

Постановление ФАС МО по делу № А40-56844/13-149-539 от 15 января 2015 г. (Рамблер и ЦБ РФ), Постановление 9 ААС от 05 мая 2014 г. по делу № А 40-153867/13 (Мэйл.Ру и ЦБ РФ), Постановление ФАС МО от 12 марта 2014 г. по делу № А40-56142/13-130-551 (МТС и ЦБ РФ), Постановление 9ААС от 28 ноября 2013 г. по делу № А40-113991/2013 (Мегафон и ЦБ РФ). Все названные решения вынесены в рамках рассмотрения обоснованности привлечения к административной ответственности за непредставление ФСФР (а затем и ЦБ РФ) сведений, относящихся к пользователям услуг

связи/почтовых сервисов. Несмотря на отсутствисте полного единообразия правовых позиций судов, данные решения имели большое значение для формирования судебной практике по тайне связи, в частности по вопросу о содержании тайны связи:

(1) IMEI, детализация счета были отнесены к сведениям, составляющим тайну связи (Мегафон и ЦБ РФ, МТС и ЦБ РФ).

(2) Адрес электронной почты был отнесен к сведениям, составляющим тайну связи (Мэйл.Ру и ЦБ РФ). К противоположному решению пришел суд в деле Рамблера и ЦБ РФ.

Апелляционное определение Ставропольского краевого суда от 10 октября 2014 г. по делу №33-5536/2014.

В данном деле суд отметил, что предоставление сведений, составляющих тайну связи, в рамках гражданского судопроизводства является нарушением обязательств оператора связи по защите тайны связи. Данное решение было вынесено судом, несмотря на наличие судебного определения, разрешающего предоставить соответствующие сведения.

Такое решение мотивировано тем, что, по мнению суда, сведения составляющие тайну связи могут предоставляться по решению суда и только в случаях, прямо предусмотренных законом. Законом не предусмотрено предоставление информации, составляющей тайну связи, в рамках гражданского судопроизводства.

Правовая позиция суда: «*Таким образом, по мнению судебной коллегии, действия директора Ставропольского филиала ОАО «ВымпелКом» З. по выдаче сведений составляющих охраняемую законом тайну и ограничению конституционных прав Б., без соблюдения соответствующей процедуры, являются незаконными, поскольку выдача оператором связи данной информации, в том числе, по решению суда, возможна исключительно в рамках уголовного судопроизводства.*»

Решение Хамовнического районного суда города Москвы от 22.03.2016 N 12-590/2016

В данном дело суд встал на сторону ООО «Яндекс», которое отказалось выдавать по запросу Находкинской таможни электронное сообщение пользователя сервиса Яндекс. Почта даже несмотря на тот факт, что к запросу таможни прикладывалось решение Находкинского городского суда. Суд мотивировал свое решение тем, что требование таможни не основано на законе.

Апелляционное определение Московского городского суда от 16 сентября 2015 г.

по делу № 33-30344.

Фабула

Пользователь почтового сервиса gmail обратился в суд с иском к ООО «Гугл», посчитав, что его право на тайну связи нарушено, поскольку правообладатель сервиса читает его корреспонденцию. Такое предположение было сделано пользователем на основании показанной ему контекстной рекламы, которая содержала элементы, соответствующие по содержанию тексту электронной переписки истца.

По мнению ООО «Гугл» право истца на тайну связи не было нарушено, так как просмотр электронных сообщений и составление рекламы на его основе осуществляет робот, также ООО «Гугл» фактически не оказывает потовые услуги и не размещает рекламные объявления, которые размещаются и настраиваются пользователями сервиса AdWords.

Решение и правовые позиции

Мосгорсуд согласился с доводами истца и привлек ООО «Гугл» к ответственности на основании следующего:

«*21 февраля 2014 года при прочтении своей электронной почты с почтового ящика с адресом "*****@gmail.com" Б. обнаружил, что рекламные слоганы основаны на тексте письма, при этом из представленного скриншота электронного сообщения следует, что реклама, как и письмо, выполнено на национальном языке с использованием кириллицы. Данный факт ответчиком не оспаривался.*

Таким образом, судебная коллегия приходит к выводу, что ответчик ООО "Гугл" при исполнении обязательств перед третьими лицами по договорам размещения рекламы и ее эффективного распространения в своем сегменте продукта Google, проводит мониторинг в том числе электронных писем, и осуществляет размещение данные рекламные сообщения в том числе и в частной переписке пользователей Российской Федерации, воспользовавшихся продуктом Google на основании результатов мониторинга конкретного пользователя продукта».

Постановление 9ААС по делу № А40-14902/16. ПАО «МГТС» было привлечено к административной ответственности в соответствии со ст. 14.1 КоАП (осуществление предпринимательской деятельности с нарушением условий лицензии) за предоставление сведений об абонентах, включающие поисковые запросы абонентов, интернет – адреса веб-страниц, посещаемых абонентами, тематику информации, размещенной на посещаемых абонентами Интернет-ресурсах, IP-адрес абонента, достаточной для формирования его

рекламного профиля, необходимого для предоставления абоненту таргетированной адресной рекламы.

Суды руководствовались следующим при вынесении решения:

(1) Предоставление третьим лицам сведений об абонентах-гражданах может осуществляться только с их согласия, за исключением случаев, федеральными законами.

Сведения, подтверждающие наличие согласия абонентов на передачу сведений об абонентах, ПАО «МГТС» не представило.

(2) Данные, позволяющие идентифицировать абонента или его оконечное оборудование являются: - фамилия, имя, отчество или псевдоним абонента-гражданина, - адрес абонента - адрес установки оконечного оборудования, абонентские номера - другие данные, позволяющие идентифицировать абонента или его оконечное оборудование, сведения баз данных систем расчета за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонента.

(3) Не только данные, позволяющие идентифицировать абонента, но

также и сведения баз данных систем расчета за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонента, также относятся к сведениям об абонентах и в соответствии с пунктом 1 статьи 53 Закона о связи и предоставление таких сведений может осуществляться только с их согласия.

(4) Информация о соединениях и трафике абонента (в том числе случайный идентификатор (Cookie «UID») в HTTP-запросе

пользователя, позволяющий отличить трафик пользователя от трафика других

пользователей для получения списка его предпочтений; IP-адрес из IP-пакета HTTP-запроса пользователя, позволяющий получить географическое положение пользователя с точностью определения до названия населенного пункта; User-Agent HTTP-запроса пользователя, позволяющий получить модель устройства или типа браузера, используемого пользователем; время просмотра веб-страниц (HTTP-запроса пользователя), позволяющее оценить частоту, с которой пользователь проявляет те или иные предпочтения; URL-адрес и заголовок Referrer HTTP-запроса пользователя, позволяющее определить предпочтения пользователя; Hash-ID линии пользователя, позволяющий определить линии, абоненты которых выразили несогласие с обработкой данных.) относится к сведениям об абонентах.

(5) Предоставление указанных выше сведений об абоненте является нарушением тайны личной жизни. При этом суд сослался на Определении КС РФ от 09.06.2005г. № 248-0.

Судебные решения, в рамках которых высказывалась позиция о разграничении информации об абонентах и сведений, составляющих банковскую тайну. Постановление Курганского Областного суда от 10 августа 2015 г. №4А-178/2015, Постановление Курганского областного суда от 18.09.2015 N 4А-255/2015, Решение АС г. Москвы от 19 мая 2014 г. по делу N А40-28184/14, Постановление АС Уральского округа от 31 мая 2016 г. по делу № А50-21341/2015, Постановление ВС РФ от 30 марта 2016 г. N 82-АД16-1, Проставление ВС РФ от 11 октября 2016 г. N 82-АД16-5.

В названных решениях суды разграничивают сведения, относящиеся к абонентам (которые рассматриваются в качестве персональных данных), и сведения, составляющие тайну связи.

Так, Курганский областной суд высказывал правовую позицию о том, что «*положения действующего законодательства о сохранении тайны телефонных переговоров, почтовых, телеграфных и иных сообщений, требующие особой гарантии в виде судебного разрешения на доступ третьих лиц (в том числе органов, осуществляющих оперативно-розыскную деятельность, органов предварительного расследования и суда) к передаваемой информации, не распространяются на сведения о зарегистрированных пользователях услугами связи (абонентах), обязанность предоставления которых операторами связи органам, осуществляющим оперативно-розыскную деятельность, предусмотрена федеральным законодательством, в том числе п. 4 ч. 1 ст. 13 Федерального закона от 7 февраля 2011 г. N 3-ФЗ «О полиции», ст. 15 Федерального закона от 12 августа 1995 г. N 144-ФЗ «Об оперативно-розыскной деятельности*». При этом к сведениям об абоненте были отнесены: фамилия, имя, отчество или псевдоним абонента-гражданина, наименование (фирменное наименование) абонента - юридического лица, фамилия, имя, отчество руководителя и работников этого юридического лица, а также адрес абонента или адрес установки оконечного оборудования, абонентские номера и другие данные, позволяющие идентифицировать абонента или его оконечное оборудование, сведения баз данных систем расчета за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонента (Постановление Курганского Областного суда от 10 августа 2015 г. №4А-178/2015). Курганский областной суд не раз высказывал в своих решениях похожие правовые позиции

(см., например, Постановление Курганского областного суда от 18.09.2015 N 4А-255/2015).

Похожие правовые позиции в своих решениях высказывает Восьмой Арбитражный Апелляционный суд, который посчитал, что сведения о принадлежности IP-адреса, осуществлявшем выход в Интернет-ресурс в конкретное время, а также IMEI для Wi-Fi модема. По мнению суда, сведения, перечисленные в ч. 1 ст. Закона о связи относятся к сведениям об абоненте, а не к сведениям, составляющим тайну связи. На этом основании Восьмой ААС посчитал, что запрос антимонопольного органа о предоставлении информации об IMEI абонента и принадлежности IP-адреса является законным и должен быть удовлетворен.

Другой подход относительно сведений, составляющих тайну связи, был высказан судами в ряде других решений. Например, Арбитражный суд города Москвы посчитал, что IMEI, будучи технической информацией об оконечном оборудовании абонента, к сведениям о самом абоненте не относится. IMEI содержится только в детализации звонков, которая охраняется тайно связи, соответственно, IMEI невозможно предоставить, не нарушив тайну связи. Ниже приводятся аргументы суда:

«*В соответствии с п. п. 19 и 20 Правил идентификационный номер абонентского устройства IMEI не относится к условиям договора об оказании услуг подвижной связи, поэтому не может быть установлен на основании положений, заключенных с абонентами договоров.*

Заключая договоры об оказании услуг подвижной связи с абонентами, оператор связи предоставляет последним не телефонные аппараты, а модули идентификации абонента (SIM-карты) с соответствующим абонентским номером. Абонентские устройства приобретаются абонентом самостоятельно в торговой сети, которая реализует их без предъявления документа, удостоверяющего личность, в связи с этим IMEI-код абонентского устройства не относится ни к оператору связи, ни к самому абоненту.

Абонент вправе использовать любые абонентские устройства и оператор связи не обязан вести базу данных, содержащую сведения об этих устройствах.

Информация об идентификационных номерах абонентских устройств IMEI «регистрируется» (устанавливается) аппаратурой связи лишь при телефонных соединениях, то есть содержится только в протоколах соединений(детализациях) конкретных абонентов, SIM-карты которых использовались в данном телефонном аппарате.

С учетом анализа приведенных норм, суд считает, что в настоящем случае,

истребованные в п. 1 предписания сведения в пункте 1 статьи 53 Федерального закона от 07.07.2003 N 126-ФЗ «О связи» в отношении всех пользователей услуг связи, которым выделялся абонентский номер с указанием, в том числе периода использования данного номера каждым из пользователей услуг связи, идентификационных номерах абонентских устройств (IMEI) оконченного оборудования, использовавшегося в каждый период, с приложением копий документов, подтверждающих изложенную информацию, в том числе договоров, соглашений, анкет клиентов, а также изменений и дополнений к данным документам составляют тайну».

Также интерес представляет решение Арбитражного суда Уральского округа. В данном деле суд признал правомерным отказ оператора связи предоставить сведения об абоненте, который был идентифицирован ЦБ РФ через IP-адрес, так как данные сведения охраняются тайной связи.

«*С учетом того, что IP-адрес присваивается абоненту аппаратурой связи при присоединении к сети Интернет на время сессии доступа; определение по времени присоединения и номеру IP-адреса относятся к сведениям конкретных абонентов и содержатся в протоколах соединений, суды пришли к обоснованному выводу о том, что запрошенная Банком России информация о лице, использовавшем IP-адрес 178.161.155.6 при соединении с сетью Интернет в определенные даты и в определенное время (п. 1 требования о предоставлении документов), относится к охраняемой законом тайне связи*».

Таким образом, суд косвенно признал, что IP- адреса составляют тайну связи в той мере, в какой они позволят определить абонента, лицо, которое осуществляет коммуникацию.

Также суд отнес следующие сведения к тайне связи: информация о лице(ах), использовавшем(их) IP-адрес 178.161.155.6 при соединении с информационно-телекоммуникационной сетью «Интернет» в определенные даты и время; 2) копии всех договоров о предоставлении услуг, заключенных обществом с лицом(ами), указанным(и) в пункте 1 требования, со всеми приложениями и дополнениями (далее - договоры), а также доверенностями, уполномочивающими кого-либо действовать от имени указанного(ых) лица (лиц); 3) справку, содержащую сведения обо всех способах оплаты услуг общества, оказываемых в рамках договоров, использованных за период с 01.01.2013 по дату получения требования

Как видно, в вопросе об отнесении технической информации, позволяющей

определить оконечное оборудование абонента (в том числе IP-адрес и IMEI), не наблюдается единства в судебной практике.

Вместе с тем, два недавних решения Верховного суда позволяют сделать вывод о том, что отнесение таких сведений к тайне связи зависит от того, позволяют ли они раскрыть детали коммуникации абонента.

Проставлением от 11 октября 2016 г. N 82-АД16-5 ВС РФ отменил одно из решений Курганского областного суда, который посчитал правомерным запрос следователя МВД о предоставлении в связи с расследованием уголовного дела сведений о том, выходил ли на связь в сети МТС сотовый телефон с IMEI-кодом <...> в период с 01.11.2014 по настоящее время, а также о том, какие абонентские номера работали сданным телефоном, и о предоставлении данных их владельцев. По мнению ВС РФ, запрашиваемые сведения представляют собой детализацию звонков абонента и относятся к тайне связи, почему не могут быть выданы по запросу без законных оснований и судебного решения.

Напротив, запрос сведений об абоненте, который был идентифицирован через IP-адрес, ВС РФ посчитал правомерным, т.к. это не тайна связи о сведения об абоненте (Постановление ВС РФ от 30 марта 2016 г. N 82-АД16-1).

Судебные решения о незаконном распространении рекламы, в рамках которых высказывались правовые позиции о тайне связи. Постановление Арбитражного суда Поволжского округа от 31.03.2016 N Ф06-25874/2015 по делу N А65-26711/2014, Постановление ФАС Северо-Западного округа от 29.04.2014 N Ф07-2577/2014 по делу N А66-3211/2013, Апелляционное определение Омского областного суда от 23.04.2014 по делу N 33-2579/2014, Постановление 9 ААС от 26 апреля 2018 г. по делу № А40-236273/16.

В рамках дел о привлечении к ответственности операторов связи за незаконную рассылку сообщений рекламного характера, операторы связи неоднократно высказывали аргументы о том, что они не являются рекламораспространителями, и проверять характер отправляемых сообщений не могут, так как сообщения составляют тайну связи. Суды как, правило, принимали сторону операторов связи (Постановление Арбитражного суда Поволжского округа от 31.03.2016 N Ф06-25874/2015 по делу N А65-26711/2014, Постановление ФАС Северо-Западного округа от 29.04.2014 N Ф07-2577/2014 по делу N А66-3211/2013, Апелляционное определение Омского областного суда от 23.04.2014 по делу N 33-2579/2014). Хотя бывали и дела, в некоторых случаях (в зависимости от договорных связей между операторами связи и лицами, заинтересованными в рекламе) операторов связи

привлекали к ответственности (Постановление Верховного Суда РФ от 27.07.2015 N 305-АД15-7742 по делу N А40-60684/2014). Вне зависимости от решения по вопросу о привлечении к ответственности, суды, как правило, не давали развернутой оценки доводам операторов связи, относящимся к тайне связи.

Между тем, в одном из недавних решений, суд прямо высказал позицию о том, что сообщения рекламного характера, разного рода массовые рассылки тайной связи не охраняются, так как их рассылка осуществляется не в рамках предоставления услуг связи абоненту (Постановление 9 ААС от 26 апреля 2018 г. по делу № А40-236273/16, данное решение обжаловано, следующее заседание назначено на 7 августа 2018 г.). В этой связи привлечение к ответственности оператора связи было признано законным. Ниже приводятся аргументы судов, в том числе суда кассационной инстанции, который направил дело на новое рассмотрение:

(1) Рассылкой по сети подвижной радиотелефонной связи является массовая отправка одинаковых коротких текстовых сообщений (SMS) с целью распространения какой-либо информации (адресная электронная рассылка по целевой аудитории с целью доведения определенной информации).

(2) Следовательно, к рассылкам по сети подвижной радиотелефонной связи не может быть отнесена передача абонентам индивидуальных сообщений, содержащих цифровые, буквенные или буквенно-цифровые сочетания (коды, пароли), а также иные адресные сообщения, содержащие различную информацию.

(3) В соответствии с пунктами 1, 2 статьи 44 Закона о связи на территории Российской Федерации услуги связи оказываются операторами связи пользователям услуг связи на основании договора об оказании услуг связи, заключаемого в соответствии с гражданским законодательством и правилами оказания услуг связи, утверждаемым Правительством Российской Федерации.

(4) Таким образом, на сообщения рекламного характера, рассылка которых осуществляется вне договора на оказание услуг связи, не распространяется режим тайны связи, предусмотренный Конституцией Российской Федерации и статьи 63 Закона о связи.

Некоторые дела о предоставлении информации о клиентах при уступке прав требования. Постановление ФАС ПО от 28 апреля 2012 г. по делу № А06-3953/2011, Апелляционное определение Самарского областного суда от 4 мая 2016 г. по делу N 33-5524/2016.

Управление Роскомнадзора по Астраханской области привлекло оператора связи (ЗАО «Комстар-регионы») к ответственности за предоставление сведений об абоненте с целью взыскания задолженности без получения письменного согласия абонента.
Суды поддержали позицию Управления Роскомнадзора, сославшись на п. 4 Правил оказания услуг связи для целей телевизионного вещания.

Прямо противоположное решение в похожем деле было вынесено Самарским областным судом, который указала следующее: «Руководствуясь вышеуказанными положениями Федерального закона N 152-ФЗ «О персональных данных», учитывая, что истцом задолженность по договору не погашена, судебная коллегия приходит к выводу, что действия ПАО «Мобильные ТелеСистемы» по передаче персональных данных истца в целях осуществления мероприятий по погашению задолженности по договору и продолжении обработки персональных данных без согласия субъекта (истца) персональных данных соответствуют требованиям законодательства Российской Федерации в области защиты персональных данных и не нарушают прав истца, как субъекта персональных данных».

Апелляционное определение Санкт-Петербургского городского суда от 28 ноября 2017 г. N 33-23320/2017.

В данном деле суд высказал позицию о том, что оператор связи не обязан предоставлять абоненту информацию о соединениях с конкретными сетевыми ресурсами в отношении оборудования с определенным IP-адресом, в том числе и потому что это может нарушить права третьего лица, которое использует данное оборудование.

«*Также судебная коллегия обращает внимание, что при заключении договора между истцом и ответчиком не было идентифицировано оконечное оборудование абонента, вследствие чего им может пользоваться третье лицо, о чем свидетельствует сам факт обращения истца за получением информации о посещении IP-адресов за период с 16:50 по 17:35 11 августа 2016 года, что может свидетельствовать о том, что истец либо лишен доступа к оборудованию, либо третье лицо могло удалить информацию о посещенных сайтах из оборудования истца, вследствие чего предоставление доступа к указанной информации может являться нарушением прав неустановленного лица*».

Постановление Магаданского городского суда Магаданской области от 27.04.2018 N 1-213/2018

Сотрудник оператора связи (ЗАО «РТК») был привлечен к уголовной ответственности в соответствии со ст. 138 УК РФ за предоставление третьему лицу детализации звонков

абонента.

Постановление Индустриального районного суда города Хабаровска от 07.12.2016 по делу N 1-863/2016

Сотрудник оператора связи (ПАО «Вымпел-Коммуникации») был привлечен к уголовной ответственности в соответствии со ст. 138 УК РФ за предоставление третьему лицу детализации звонков абонента.

Европейский союз

Конфиденциальность коммуникаций гарантируется в соответствии с международными нормами, касающимися прав человека, а также конституциями государств-членов ЕС. Как было указано выше, право на тайну корреспонденции прямо закреплено в статье 8 Европейской конвенции о защите прав человека и основных свобод и статье 7 Хартии Европейского союза об основных правах.

На уровне Европейского союза следует выделить два ключевых документа, регулирующих правоотношения в данной сфере, а именно:

1. Директива № 2002/58/ЕС «В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи)»[14] (далее - «Директива ePrivacy»);

2. Проект Регламента Европейского парламента и Совета Европейского Союза в отношении уважения частной жизни и защиты персональных данных в секторе электронных средств связи взамен Директивы 2002/58/ЕС[15] (далее - «Регламент ePrivacy»).

В настоящий момент применяется Директива ePrivacy, однако в силу развития технологий и неактуальности ряда положений, а также необходимости приведения регулирования в соответствие с GDPR. очевидно, что в ближайшем будущем будет принят новый акт, положения которого будут базироваться на Регламенте ePrivacy, поэтому мы

[14] В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи) [Электронный ресурс] // директива Европейского парламента и Совета Европейского Союза. – № 2002/58/ЕС – 12.07.2002. – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 08.08.2018).

[15] Proposal for a regulation of the European parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC [Electronic resource] : Regulation on Privacy and Electronic Communications. – January 10, 2017 // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0010:FIN (accessed: 30.07.2018).

полагаем необходимым привести основные нормы и этого документа тоже. Кроме того, как было отмечено в официальной позиции Европейского инспектора по защите данных[16], Регламент ePrivacy является одной из ключевых инициатив в рамках развития Стратегии единого цифрового рынка[17], которая призвана обеспечить высокий уровень защиты для граждан и участников рынка на территории всего ЕС. Регламент будет иметь прямое действие на территории ЕС и применяться ко всем типам коммуникаций, включая мессенджеры, платформы, IP-телефонию (VOIP), коммуникации в рамках Интернета вещей (IoT, M2M) и т.д.

В соответствии с п.1 ст. 5. Директивы ePrivacy конфиденциальность передаваемых сообщений и относящихся к ним данных трафика предполагает установление запрета государствами-участниками ЕС на «прослушивание, несанкционированное подключение, хранение или другие виды перехвата или слежки за сообщениями и относящимися к ним данными трафика лицами, не являющимися пользователями, без согласия заинтересованных пользователей»[18]. Аналогичное положение содержится и в ст. 5 Регламента ePrivacy. Режим конфиденциальности означает, что информация, которой обмениваются стороны при участии внешнего провайдера, включая информацию о времени отправки, отправителе и адресате, не должна быть известна кому-либо кроме сторон.

Директива ePrivacy делит информацию на а) «данные трафика» (*traffic*) т.е. данные, обработанные в целях осуществления передачи сообщения по сети электронной связи или в целях формирования счета за пользование услугами электронной связи (п. b ст. 2), и «сообщения» (*communication*), под которыми понимается любая информация, которой обмениваются или которая передается между ограниченным кругом лиц посредством общедоступных услуг электронной связи. «Трафик данных, *inter alia*, включает сведения о направлении, длительности, времени передачи или объеме передаваемого сообщения, используемом протоколе, месте положения терминального оборудования отправителя или получателя сообщения, сети, по которой начинается или заканчивается соединение, начале,

[16] EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation) [Electronic resource]: European Data Protection Supervisor. – Opinion 6/2017 // The European Data Protection Supervisor (EDPS) [Site]. – URL: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf (accessed: 30.07.2018).

[17] Digital single market [Electronic resource] // European Commission [Site]. – URL: https://ec.europa.eu/commission/priorities/digital-single-market_en (accessed: 30.07.2018).

[18] В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи) / Там же.

конце, продолжительности соединения»[19]. Регламент ePrivacy в целом сохраняет данный подход, однако использует иную терминологию, подразделяя данные на метаданные (*electronic communications metadata*) и содержание данных электронной связи (*electronic communications content*), которые в совокупности образуют данные электронной связи (*electronic communications data*) (ст. 4). Данные электронной связи определяются максимально широко и технологически нейтрально с целью охватить любую информацию, включая содержание передаваемых данных и информацию, касающуюся пользователей, обрабатываемую для целей передачи данных (включая данные об отправителе и адресате, их месте нахождения, дате, времени, продолжительности и типе коммуникации).

Таким образом, предметом охраны являются любые данные, передаваемые посредством сетей связи общего пользования и общедоступных услуг электронной связи, за исключением тех, которые предназначаются для потенциально неограниченного круга лиц и передаются в рамках широкого оповещения общественности по сети электронной связи. Передаваемые данные могут одновременно являться и сведениями ограниченного доступа, и персональными данными физических лиц. В этом случае подлежат применению и соблюдению положения GDPR, о чем прямо говорится в Директиве и Регламенте ePrivacy. В частности, в части требований к согласию пользователя содержится прямая отсылка к GDPR[20]. Более того, GDPR должен будет применяться и в тех случаях, когда пользователями являются юридические лица (п. 3 преамбулы Регламента ePrivacy).

По общему правилу в соответствии с Директивой ePrivacy на оператора возлагаются обязанности по обеспечению конфиденциальности передаваемых данных; получению согласия абонента в установленных законом случаях; применению необходимых технических и организационных мер для обеспечения безопасности предоставляемых услуг; предоставлению возможности отменить показ определения вызывающего номера в отношении каждого вызова, а вызываемому абоненту возможности отклонять входящие вызовы, по которым не отменен показ вызывающего номера; уничтожению или анонимизации данных трафика, если в них нет дальнейшей необходимости для передачи сообщения; информированию абонента или пользователя о видах данных трафика, находящихся в обработке, и о длительности такой обработки для установленных целей и др.

[19] В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи) / Там же.

[20] Согласие должно быть свободное, конкретное, содержательное и определенное в соответствии с GDPR.

Директива ePrivacy закрепляет, что обработка сообщений и трафика без согласия пользователей не допускается, за исключением случаев установленных национальным законодательством в целях обеспечения национальной безопасности, расследования преступлений и т.д. Это, однако, не исключает возможность технического хранения данных, необходимого для передачи сообщения с соблюдением требований конфиденциальности. Дополнительно, «установленные требования не должны затрагивать законодательно разрешенную запись сообщений и относящихся к ним данных трафика, когда такая запись производится в ходе законной деловой практики для целей предоставления доказательства совершения коммерческой сделки или осуществления любого другого делового взаимодействия»[21] (ст. 5 Директивы ePrivacy). Также прямо разрешается обработка данных трафика, необходимых для формирования счетов абонента за пользование связью и межсоединение в течение определённого периода времени, (ст. 6 Директивы ePrivacy).

Регламент ePrivacy исходит из того, что обработка данных может генерировать большую пользу, как для пользователей и общества, так и для бизнеса, и предлагает закрепить следующие основания для обработки данных. По общему правилу обработка любых данных допускается для целей передачи сообщений и обеспечения безопасности соединения. Метаданные также могут обрабатываться с согласия лица, для целей обеспечения необходимого уровня сервиса, осуществления биллинга или предотвращения мошенничества и иного противоправного использования. Наконец, содержание данных электронной связи может обрабатываться также для цели предоставления пользователю сервиса, если пользователь выразил свое согласие и предоставление сервиса невозможно без обработки таких данных, или если все пользователи выразили свое согласие на обработку содержания данных для определенных целей, которые не могут быть достигнуты с использованием анонимизированных данных. Операторы обязаны удалять или делать анонимным содержание данных электронной связи после получения таких данных адресатом.

Согласно Директиве для обработки данных трафика в целях продвижения услуг электронных коммуникаций или дополнительных услуг провайдером общедоступных услуг электронной связи требуется получить предварительное согласие лица. Данные трафика подлежат удалению или анонимизации после достижения цели передачи сообщения. Третьи лица, действующие под руководством провайдеров, могут осуществлять обработку данных

[21] В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи) / Там же.

трафика в пределах, необходимых для управления трафиком или биллингом, рассмотрения требований клиентов, обнаружения случаев мошенничества, продвижения услуг электронной связи или предоставления дополнительных услуг при условии соблюдения установленных требований (п. 5 ст. 6 Директивы ePrivacy). Иные случаи привлечения третьих лиц и передачи им данных в Директиве ePrivacy прямо не урегулированы. Аналогично отсутствуют специальные положения о трансграничной передаче сведений и передаче сведений третьим лицам без согласия пользователей. Соответственно, в этой части применяются положения GDPR. На это прямо указывается в статье 7 Регламента ePrivacy, в соответствии с которой содержание данных электронной связи может быть записано или иным образом сохранено пользователем или третьим лицом, которому пользователем поручена запись, хранение или иная обработка данных в соответствии с GDPR.

Директива ePrivacy разрешает обработку данных о географическом местонахождении терминального устройства пользователя (*location data*) либо с согласия пользователей, либо после того, как такие данные будут сделаны анонимными. Регламент ePrivacy включает такие данные в понятие метаданных.

Как в Директиве, так и в Регламенте ePrivacy сохраняется подход, согласно которому для рассылки маркетинговых сообщений требуется получить предварительное согласие пользователя (*opt in*), за исключением случаев, когда используются данные лица, которое предоставило их при приобретении товаров или услуг. В последнем случае использование данных в указанных целях допускается при условии предоставления лицу возможности запретить такое использование / отказаться от рассылки (*opt out*) в любой момент времени.

Одним из знаковых изменений, предлагаемых в Регламенте ePrivacy, называют упрощение процедуры предоставления и отзыва согласия пользователями на использование файлов *cookie*, позволяя сделать это с помощью настроек браузера вместо использования всплывающих окон.

Раскрытие данных допускается посредством включения в публичные справочники. Статья 12 Директивы ePrivacy устанавливает обязательство по «информированию лиц о цели (целях) печатного или электронного справочника абонентов, находящегося в свободном доступе <…>, и о любых дальнейших возможностях использования данных, основанных на функциях поиска, встроенных в электронные версии справочника»[22]. Регламент ePrivacy

[22] В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи) / Там же.

ужесточает требования и предлагает закрепить необходимость получения согласия абонента для включения его данных в публично доступные справочники.

В соответствии с ранее действовавшей Директивой 2006/24/EC о хранении данных[23], операторы были обязаны хранить значительный перечень данных, включая телефонные номера абонентов, международные идентификаторы мобильного оборудования (IMEI), международные идентификаторы мобильных абонентов (IMSI), ID-адреса и т.д. Решением Европейского суда данная Директива была признана недействительной. Подробнее об этом деле в разделе, посвященном судебной практике. По смыслу Регламента ePrivacy указанные идентификаторы можно отнести к данным о терминальных устройствах пользователей, обработка которых должна быть запрещена, за исключением следующих случаев:

1. обработка необходима для цели передачи сообщения посредством электронных средств связи;
2. пользователь дал согласие на обработку;
3. обработка необходима для целей предоставления информационных услуг (*information society service*) по запросу потребителя, под которыми понимается широкий спектр сфер экономической деятельности, которые осуществляются в режиме онлайн, включая продажу товаров в Интернете, использование Интернет поисковиков, онлайн рекламу и маркетинг, использование видео-сервисов и т.д.;
4. обработка требуется для подсчета аудитории вэб-сервиса, если такой подсчет осуществляется лицом, оказывающим информационные услуги, запрошенные пользователем.

Обработка данных, созданных терминальным устройством в результате подключения к другому устройству или сетевому оборудованию, также должна быть запрещена, за исключением случаев, когда это требуется для установления соединения или при условии отображения ясного и наглядного уведомления об условиях и цели сбора данных, о лице, осуществляющем обработку, а также иных данных в соответствии с GDPR. В уведомлении должно быть четко указано, какие меры может предпринять пользователь для прекращения или уменьшения объема обрабатываемых данных.

[23] On retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EC [Electronic resource]: the European parliament and of the Council Directive – № 2006/24/EC. – 15 March 2006 // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006L0024 (accessed: 30.07.2018).

Каждому пользователю предоставляются меры защиты аналогичные предусмотренным в ст. 77 (право на подачу жалобы в надзорный орган), 78 (право подать жалобу на надзорный орган) и 79 (право на эффективное средство судебной защиты) GDPR. Ответственность за нарушение требований конфиденциальности данных включает в себя административные штрафы в размере не более 20 000 000 Евро или в случае предприятия, в размере не более 4% от общего годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше.

Отдельное внимание также следует уделить ***судебной практике***, и в качестве репрезентативных дел допустимо привести следующие.

Дело Digital Rights Ireland. Дело касалось признания недействительной Директивы 2006/24/ЕС о хранении данных, полученных или обрабатываемых в связи с предоставлением общедоступных услуг электронной связи или сетей общего пользования. Иск был подан небольшой неправительственной организацией Digital Rights Ireland и около 12 000 австрийских жителей.

Директива была принята после ряда террористических актов в Мадриде и Лондоне в 2005 году. Директива требовала хранить данные фиксированной, мобильной телефонной связи, интернет-телефонии, а также сообщений электронной почты от шести месяцев до двух лет. Такое регулирование было введено для целей обеспечения доступности данных на время проведения расследований, выявления тяжких преступлений, как они определены в национальном законодательстве. Положения Директивы были весьма спорными, в том числе, в аспекте соответствия ее положений национальным конституциям. Споры привели к рассматриваемому решению Суда ЕС[24].

Суд ЕС установил, что Директива приводит к серьезному вмешательству в права, гарантированные статьями 7 и 8 Хартии Европейского союза по правам человека. Хотя Суд ЕС признал, что такое вмешательство пропорционально цели, ради которой оно осуществляется (борьба с тяжкими преступлениями и, как следствие, обеспечение общественной безопасности), Суд ЕС установил, что вмешательство не соразмерно целям Директивы. Так, вмешательство не дифференцировало средства связи, виды данных или типы

[24] Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others [Electronic resource]: Judgment of the Court (Grand Chamber) of April 8, 2014, ECR [2014] I-238 (Joined Cases C-293 & C-594/12) // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CC0293 (accessed: 30.07.2018).

пользователей. Кроме того, не была определена процедура доступа к данным. При этом сроки хранения данных также не были определены объективно.

В то время как данное решение не получило серьезного освещения в СМИ, оно выявило еще один пробел в регулировании защиты персональных данных в ЕС. Кроме того, данный случай достаточно выраженно признал опасности, связанные со сбором Больших данных (Big Data). Например, в той части, что такой сбор может позволять делать очень точные выводы относительно частной жизни отдельных физических лиц.

Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others (C-203/15 and C-698/15).[25] В соответствии со ст. 15(1) Директивы ePrivacy государства-члены ЕС вправе принимать законодательные меры для ограничения прав и обязанностей, предусмотренных некоторыми статьями Директивы, если такое ограничение представляет собой необходимую, соответствующую и пропорциональную меру в рамках демократического общества для осуществления защиты национальной (государственной) безопасности, обороны и общественной безопасности, предотвращения, расследования, обнаружения и судебного преследования преступных действий или несанкционированного использования системы электронной связи. В свете данного положения возникли вопросы, какие именно действия по хранению данных допустимы в соответствии с Директивой.

«При рассмотрении объединенных дел Европейский суд изучал законодательные акты двух государств-членов ЕС на момент рассмотрения дела – Швеции (Data Retention Directive) и Великобритании (Data Retention and Investigatory Powers Act 2014) – согласно которым данные всех подписчиков и зарегистрированных пользователей о трафике и местонахождении, касающиеся любых средств электронной связи, должны храниться на общих и недискриминационных началах. Суд пришел к выводу, что данные законы ограничивают основные права на частную жизнь и защиту персональных данных. Эти ограничения не были признаны объективно оправданными в силу их многочисленности, а также малого объема предусмотренных гарантий, даже когда их целью выступала борьба с серьезными преступлениями. Однако все же подобная цель может выступать основанием для

[25] Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others [Electronic resource] : Judgment of the European court of justice (Grand Chamber) dated December 21, 2016 (Joined Cases C-203/15 and C-698/15) // The Court Of Justice Of The European Union [Site]. – URL: http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=26020 (accessed: 30.07.2018).

хранения таких данных при условии, что оно будет ограничено рамками строго необходимого. То есть храниться могут только определенные категории данных, относительно указанных видов средств связи, данные конкретных лиц, а также в течении фиксированного срока»[26].

Барбулеску против Румынии (Barbulescu v. Romania) N 61496/08.[27] Заявитель работал в бухарестском представительстве румынской частной компании в качестве инженера отдела продаж. По просьбе работодателя, чтобы отвечать на запросы покупателей, заявитель создал электронный адрес для общения в реальном времени в программе обмена мгновенными сообщениями компании Yahoo, в которой текст передавался по Интернету в режиме реального времени. В компании действовала внутренняя политика, запрещавшая сотрудникам компании использовать ресурсы компании для личных целей. Тем не менее, заявитель использовал сервис Yahoo для общения со своими родственниками по личным вопросам. Указанное обстоятельство стало известно работодателю, который принял решение о расторжении трудового договора с заявителем. Заявитель обратился в суд с требованием отменить решение о его увольнении, обязать работодателя выплатить ему задолженность по заработной плате и иным выплатам и компенсацию морального вреда, восстановить его в должности. Суд отклонил жалобу заявителя и подтвердил законность его увольнения.

ЕСПЧ установил нарушение ст. 8 Конвенции о защите прав человека и основных свобод. Суд пришел к выводу, что национальные власти не установили необходимый уровень защиты прав заявителя на уважение личной жизни и корреспонденции. В частности, не был соблюден баланс интересов работника и прав работодателя контролировать работу его компании. Национальные суды не установили, уведомлялся ли работник о том, что содержание его сообщений может быть доступно третьим лицам, также власти не приняли в расчет тот факт, что заявитель не был проинформирован ни о содержании контрольных процедур, ни о его границах контроля. Более того, власти не определили, был ли у работодателя другой способ или возможность достигнуть необходимые цели, и чем был оправдан такой контроль со стороны работодателя. Заявителю было присуждено 1365 евро за

[26] Постникова Е.В. Некоторые аспекты правового регулирования защиты персональных данных в рамках внутреннего рынка Европейского союза [Электронный ресурс] / Постникова Е.В. Право в современном мире – 2018. // Право. Журнал Высшей школы экономики [Сайт]. – URL: https://law-journal.hse.ru/data/2018/04/19/1150474169/%D0%BF%D0%BE%D1%81%D1%82%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2%D0%B0.pdf (дата обращения: 30.07.2018).

[27] Barbulescu v. Romania [Electronic resource]: Judgement of the European Court of Human Rights dated September 05, 2017. // Marina Castellaneta [Site]. – URL: http://www.marinacastellaneta.it/blog/wp-content/uploads/2017/09/CASE-OF-BARBULESCU-v.-ROMANIA.pdf (accessed: 30.07.2018).

понесенные расходы, так как ЕСПЧ пришел к выводу, что сам факт признания нарушения является достаточной справедливой компенсацией морального вреда.

Германия

Понятие тайны связи определяется в Основном законе ФРГ (Конституции)[28] (статья 10), Законе о связи (§ 88), Уголовном кодексе ФРГ (§ 206). Комплексное толкование данных положений позволяет прийти к выводу, что тайна связи означает тайну телефонных переговоров, переписки, почтовых и любых иных сообщений, передаваемых по сетям электросвязи и по сетям почтовой связи.

Принцип, по которому те или иные сведения относятся к тайне связи, можно назвать открытым в связи с формулировкой «иные сообщения».

К сведениям, составляющим тайну связи, относится содержание переписки, телефонных переговоров и иных сообщений, факт участия лица в телефонных переговорах, а также в процессе переписки / отправке сообщений (§ 88(1) Закона о связи и § 206(5) Уголовного кодекса ФРГ).

В части вопроса о разграничении сведений, составляющих банковскую тайну, и сведений ограниченного доступа между собой следует отметить, что институт сведений ограниченного доступа в законодательстве и судебных решениях не выявлен.

Тайна связи включает в себя персональные данные в той части, в которой они идентифицируют лицо или могут идентифицировать его.

Механизм правовой защиты субъектов состоит из следующих элементов:

(1) недопустимость ограничения права на тайну связи иначе, чем на основании закона (п. 2 ст. 10 Основного закона ФРГ);

(2) установление обязательств в отношении операторов связи по обеспечению соблюдения тайны переписки (п. 2 §88 Закона о связи);

(3) установление обязательных требований к техническому оборудованию, используемому при оказании услуг связи, обеспечивающему защиту тайны связи и защиту персональных данных (§109 Закона о связи);

(4) возможность подачи жалобы в надзорный орган по месту проживания, работы

[28] Basic Law for the Federal Republic of Germany [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: http://www.gesetze-im-internet.de/gg/GG.pdf (accessed: 08.08.2018).

или места предполагаемого нарушения (ст.77 GDPR).

За нарушение тайны связи предусмотрена уголовная ответственность в виде штрафа либо лишения свободы на срок до пяти лет (§ 206 Уголовный кодекс ФРГ).

Лица, привлекаемые к уголовной ответственности:

(1) лицо, неуполномоченное на разглашение третьим лицам сведений, составляющих тайну связи, которые стали ему известны в рамках оказания таким лицом услуг связи;

(2) лицо, которому поручено осуществлять контроль за оператором связи, предоставлять услуги связи, установить оборудование, используемое оператором связи;

(3) лицо, являющееся владельцем или сотрудником компании, упомянутой в пункте 1, если такое лицо, например, вскрыло или иным образом, используя технические средства, узнало содержание закодированного сообщения, переданного оператору связи для последующей передачи; блокирует отправку сообщения.

В части нарушения требований к обработке персональных данных ответственность предусмотрена в Законе о ПД.

Соотношение тайны связи с другими конституционными правами оценивается с использованием общего подхода пропорциональности ограничения прав (по критериям адекватности, необходимости и приемлемости)[29]. Как правило, тайна связи ограничивается со стороны государства путем вмешательства, контроля, мониторинга переписки, телефонных разговоров и т.д. В качестве примеров можно привести несколько знаковых дел.

Klass and Others v. Germany[30]

Заявители полагали, что Закон от 13 августа 1968 г. «Об ограничении тайны переписки, почтовых отправлений и связи» (Закон Об ограничении тайны связи)[31] уточняющий положения п.2 ст.10 Основного закона ФРГ (Конституции), ограничивает право заявителей на тайну переписки, почтовых отправлении, телефонных разговоров. Заявители

[29] A. Barak. Proportionality. Constitutional Rights and their Limitations [Electronic resource]: International Journal of Constitutional Law, Volume 13, Issue 2, 1 April 2015 // Oxford Academic. International Journal of Constitutional Law [Site]. – URL: https://doi.org/10.1093/icon/mov028 (accessed: 07.08.2018).

[30] Klass and Others v. Germany [Electronic resource]: Judgement of European Court of Human Rights dated of 6.09.1978 // European Court of Human Rights [Site]. – URL: http://hudoc.echr.coe.int/eng?i=001-57510 (accessed: 08.08.2018).

[31] New version of the law was accepted in 2001: Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10) 26.06.2001 [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/g10_2001/G_10.pdf (accessed: 08.08.2018).

полагали, что данные положения нарушают ст.8 Конвенции, поскольку не требуют уведомлять заинтересованных лиц об использовании ограничительных мер. До обращения в ЕСПЧ заявители обращались в Конституционный суд Германии, который признал, что Закон Об ограничении тайны связи не соответствует Основному закону ФРГ в той части, в которой он не предусматривает уведомление лица, за которым устанавливается наблюдение, даже для тех случаев, когда такое уведомление может быть сделано без ущерба целям предпринимаемых мер. Однако суд посчитал конституционным остальные положения, в том числе те, которое наделяли надзорными функциями два специальное создаваемые органа. Заявители не были удовлетворены данным решением, поскольку посчитали, что замена судебной защиты прав в данной сфере надзорными функциями двух специальных органов несовместима с гарантиями основных прав и свобод человека. Заявители полагали, что это ограничивает их право на судебную защиту.

ЕСПЧ вынес решение об отсутствии нарушений п.1 ст.6 (право на беспристрастное судебное разбирательство в гражданском и уголовном суде), ст.8 (право на уважение личной и семейной жизни, неприкосновенности жилища и корреспонденции) и ст. 13 (право на эффективные средства правовой защиты перед национальным органом в случаях нарушения прав, изложенных в Конвенции).

Основной вопрос, который разрешал ЕСПЧ касался того, пропорционально ли вмешательство в данные права и оправдывается ли оно условиями п.2 ст.8 Конвенции, в котором предусматривается возможность ограничения права в определенных случаях и целях. Так, было установлено, что цели ограничений, установленных Законом Об ограничении тайны связи, заключаются в сохранении государственной безопасности, предотвращении беспорядков, преступлений. Суд признал, что с учетом существования двух факторов (изощренные формы шпионажа и терроризм) наличие подобного законодательства допустимо в указанных выше целях и пропорционально ограничивает право граждан на тайну связи.

Аналогичным образом впоследствии было рассмотрено и дело Weber and Saravia v. Germany[32], в котором заявители также ссылались на непропорциональное ограничение их прав Законом Об ограничении тайны связи и принятыми к нему изменениями.

[32] Weber and Saravia v. Germany. [Electronic resource]: Judgement of European Court of Human Rights dated of 29.06.2006 // European Court of Human Rights [Site]. – URL: http://hudoc.echr.coe.int/eng?i=002-3235 (accessed: 08.08.2018).

Позиция Конституционного суда по вопросу о превентивном мониторинге телекоммуникаций (*preventive telecommunication surveillance)* [33]

В своем решение суд указал, что такой мониторинг приемлем только тогда, когда есть высокая угроза для законных интересов и определенная ситуация, свидетельствующая о возможности совершения преступления в будущем. Поскольку невозможно предугадать содержание бесед, Конституционный суд указал, что правоохранительные органы должны немедленно прекратить мониторинг, если разговор будет касаться частной жизни. Кроме того, в качестве гарантии защиты тайны частной жизни Суд потребовал запретить хранение и дальнейшее использование таких разговоров. То есть после сбора такой информации она должна быть немедленно удалена.

Порядок и условия передачи сведений, составляющих тайну связи, в той части, в которой они относятся к персональным данным, определены в Законе о ПД и GDPR. Порядок и условия передачи таких сведений, в том числе трансграничной, аналогичны общим требованиям GDPR к обработке персональных данных. Однако отметим, что в разделе 92 Закона о связи[34] содержится ограничение в части трансграничной передачи персональных данных, согласно которому такая передача допускается при условии соблюдения законодательства о защите персональных данных, а также, если это необходимо для оказания услуг связи, подготовки или выставления счетов (раздел 97), борьбы с мошенничеством.

В отношении случаев, условий и порядка передачи сведений, составляющих тайну связи третьим лицам без согласия субъектов можно отметить следующее. Такая передача допускается, прежде всего, в случаях, когда имеются иные основания обработки персональных данных. Например, в параграфах 110-113 Закона о связи установлены законные основания для систематического доступа к данным со стороны правоохранительных органов и разведки. Так, провайдеры связи обязаны собирать определенные данные о своих клиентах (имя, адрес, телефонный номер) до начала оказания услуг. Эта информация именуется инвентарной информацией, которая отправляется автоматизированный банк данных Федерального агентства сетей Германии. В соответствии с

[33] Beschluss des Entscheidungen des Bundesverfassungsgerichts vom. 27.07.2005 – 1 BvR 668/04 [Electronic resource] // Deutschsprachiges Fallrecht (DFR) [Site]. – URL: http://www.servat.unibe.ch/dfr/bv113348 (accessed: 08.08.2018).

[34] Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 10 Absatz 12 des Gesetzes vom 30. Oktober 2017 (BGBl. I S. 3618) geändert worden ist [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/tkg_2004/TKG.pdf (accessed: 08.08.2018).

параграфом 112 Закона о связи государственные органы могут автоматически запрашивать информацию из этой базы данных. Основания для обоснования такого доступа не требуют существенного доказывания. Так, сотрудники правоохранительных органов и разведки могут запрашивать информацию из банка данных, когда это необходимо для выполнения их юридических функций.

Помимо этого доступ может осуществляться на основании отдельных положений Уголовно-процессуального кодекса Германии[35]. В частности, может осуществляться следующее:

- контроль, запись телефонных и иных переговоров, получения информации по техническим каналам связи, «прослушка» (§ 100a);
- подключение с использованием технических средств к информационно-вычислительной системе, используемой подозреваемым и сбор данных/информации, хранящейся там (Online-обыск) (§ 100b);
- оперативно-розыскные мероприятия с использованием технических средств с целью проверки мобильных устройств. С использованием технических средств можно установить номер мобильного устройства и номер СИМ-карты, вставленной в мобильное устройство, а также местонахождение мобильного устройства (§ 100i).

Указанные мероприятия могут быть совершены, если:

- существуют основания подозревать, что субъект является исполнителем или соучастником совершенного преступлении, либо имело место покушение на совершение преступление, если за покушение предусмотрена уголовная ответственность, либо осуществлял действия, направленные на приготовление к преступлению,

- преступление является тяжким или особо тяжким и

- расследование фактов или определение местонахождения обвиняемого/ подозреваемого было бы значительно сложнее.

В § 100d Уголовно-процессуального кодекса ФРГ имплементированы следующие требования, сформулированные Конституционным судом в деле о превентивном мониторинге телекоммуникаций:

(1) если имеются основания полагать, что какое-либо из мероприятий,

[35] Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 des Gesetzes vom 30. Oktober 2017 (BGBl. I S. 3618) geändert worden ist [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/stpo/StPO.pdf (accessed: 08.08.2018).

совершаемых в соответствии с §100a-100c Уголовно-процессуального кодекса ФРГ, само по себе дает представление об основной области частной жизни, то такое мероприятие является недопустимым.

(2) сведения о частной жизни, которые были получены в соответствии с §§ 100a-100c Уголовно-процессуального кодекса ФРГ, не могут быть использованы. Записи о таких сведениях должны быть немедленно удалены.

В законодательстве Германии не установлены прямые изъятия из режима охраны сведений, составляющих тайну связи, в целях обеспечения возможности обработки накопленных данных для достижения социальных, государственных, экономических целей. Однако, как указывалось выше, в законодательстве содержатся определенные случаи ограничения тайны связи в целях обеспечения государственной безопасности. Кроме того, необходимо отметить возможность обработки анонимизированных данных.

Раскрытие сведений, составляющих тайну связи, в форме открытых связи и принципы раскрытия законодательно не определены.

Вопрос о возможности доступа третьих лиц к данным, составляющим тайну связи, был раскрыт выше. Администрирование согласий субъектов тайны связи на обработку сведений, составляющих тайну связи и/или их передачу третьим лицам (в т.ч. наличие права субъекта определять порядок использования таких сведений, делегирования права на выдачу согласий, отзыва согласий на их сбор, обработку и/или передачу и т.д.) подчиняется общим правилам, установленным в GDPR.

Специальные нормы по идентификации субъектов тайн (в т.ч. их законных представителей) не выявлены.

В отношении форм и способов получения согласий, порядка фиксации и хранения подтверждения согласий следует отметить, что согласие на обработку сведений, составляющих тайну связи, аналогично согласиям на обработку иных персональных данных. Способ получения, передачи и хранения также аналогичен общим требованиям, установленным GDPR. При этом дополнительно в § 94 Закона о связи указывается, что согласие может быть получено в электронной форме, если поставщик услуг гарантирует следующее:

- пользователь осознанно и явно дал свое согласие
- согласие учитывается
- пользователь может получить содержание согласия в любое время

- пользователь может отозвать свое согласие в любое время.

Права и обязанности специальных категорий лиц в части доступа к сведениям, составляющих тайну связи, а также случаи такого доступа не выявлены.

Обязанность операторов связи по обеспечению соблюдения тайны связи раскрыта в разделе 88 Закона о связи. Так, содержание и детали коммуникации, в частности, было ли лицо вовлечено в процессы коммуникации является тайной связи. Конфиденциальность также распространяется на звонки, оставшиеся без ответа. Каждый провайдер услуг обязан сохранять тайну связи. Обязательство сохранять тайну связи продолжает применяться также и после окончания деятельности. Кроме того, провайдерам услуг запрещено получать (для себя или для других лиц) любую информацию о содержании коммуникации, помимо той, которая необходима им для предоставления услуг связи, в том числе для защиты их технических систем. Передача таких данных третьим лицам допускается только в той мере, в которой допустимо Законом (в Законе о связи такие случаи не предусмотрены).

Согласно п.1 раздела 95 Закона о связи провайдер услуг на основании договора с другим провайдером услуг может собирать и использовать данные о своих абонентах, а также абонентов такого другого провайдера услуг в объеме, необходимом для выполнения договора между провайдерами услуг. При этом передача данных абонентов третьим лицам допускается только с согласия абонента. После завершения договорных отношений абонентские данные должны быть удалены провайдером услуг по истечении одного календарного года, следующего за годом прекращения договора (в том числе применяются положения Закона о ПД).

Правовое основание распределения и использования IMSI – это план нумерации IMSI. В плане указывается, как структурируются номера, цель использования, условия использования и т.д. План нумерации вступил в силу 07.04.2016[36] и заменил предыдущее регулирование. С момента вступления в силу плана нумерации так называемые MVNO (виртуальные операторы мобильной связи) могут также участвовать в распределении IMSI-блоков[37]. Изменениями, внесенными в план, было разрешено экстерриториальное

[36] Nummernplan Internationale Kennungen für Mobile Teilnehmer vom 06.04.2016 [Electronic resource] // Bundesnetzagentur [Site]. – URL: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/TechnischeNummern/IMSI/IMSI_NP.pdf?__blob=publicationFile&v=3 (accessed: 09.08.2018).

[37] Более подробно см. Internationale Kennungen für mobile Teilnehmer (IMSI) [Electronic resource] // Bundesnetzagentur [Site]. –

использование номеров (ранее Федеральное сетевое агентство исходило из недопустимости экстерриториального использования номеров, то есть номера IMSI не могли использоваться за пределами юрисдикции, для которой они изначально были распределены, за исключением случаев временного роуминга, например, когда они использовались путешественниками)[38]. То есть становится возможным использование зарубежных IMSI для M2M сервисов, предоставляемых в Германии, а также немецких сервисов с использованием немецких IMSI за рубежом. Это необходимо, прежде всего, для служб связи, используемых в подключенных транспортных средствах или иных устройствах.

IMEI ранее регулировался временными правилами присвоения IMEI, однако они были отменены в 2010 году[39].

Что касается сбора указанных данных (IMEI, IMSI, MAC-адрес), то в Германии отсутствует специальное регулирование. Однако отметим, что оно может появиться после принятия на уровне ЕС обновленного e-Privacy Регламента[40].

Говоря об IP-адресах необходимо упомянуть позицию Европейского суда от 19 октября 2016 года по делу Partick Breyer v. Germany (Case 582/14)[41], в котором Европейский суд указал, что динамический IP адрес в некоторых случаях является персональными данными (а следовательно, требуется согласие лиц на обработку таких данных). В указанном деле было отмечено, что динамический IP адрес прямо не идентифицировал заявителя, однако он мог идентифицировать заявителя косвенно с использованием IP адрес и данных аккаунта, имеющихся у интернет провайдера (ISP). Ключевой вопрос заключался в том,

---

URL: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/TechnischeNummern/IMSI/IMSI_node.html (accessed: 09.08.2018).

[38] Verfügung Nr. 33/2016, Amtsblatt Nr. 11/2016 vom 15.06.2016 [Electronic resource] // Bundesnetzagentur [Site]. – URL: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/TechnischeNummern/IMSI/IMSI_exterritNutzung.pdf?__blob=publicationFile&v=1 (accessed: 09.08.2018).

[39] Internationale Kennungen für mobile Endeinrichtungen [Electronic resource] // Bundesnetzagentur [Site]. – URL: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/TechnischeNummern/IMEI/imei_node.html (accessed: 09.08.2018).

[40] См. проект Регламента по состоянию на 4 мая 2018: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC [Electronic resource] // The International Association of Privacy Professionals [Site]. – URL: https://iapp.org/media/pdf/resource_center/Draft-ePriv-Reg-May-2018.pdf (accessed: 09.08.2018).

[41]Patrick Breyer v. Bundesrepublik Deutschland [Electronic resource]: Judgement of the Court of Justice of the European Union dated of 19.10.2016 No. C-582/14 // The Court Of Justice Of The European Union [Site]. – URL: http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1116945 (accessed: 09.08.2018).

является ли тест для определения возможности идентифицировать лицо:

- объективным (то есть IP адрес – это персональные данные всегда, потому что интернет провайдер всегда может связать IP адрес с другими данными), либо же
- относительным (то есть IP адрес – это персональные данные для интернет провайдера, но не персональные данные для других лиц, у которых нет доступа к аналогичной информации, которая есть у интернет провайдера).

Хотя суд прямо не разрешил этот вопрос, из позиции суда в целом следует, что он пришел к выводу об относительности данного теста. Суд указал, что динамический IP адрес будет являться персональными данными для оператора интернет-сайта если:

- есть другая сторона (например, интернет провайдер), который может связать динамический IP адрес и идентифицировать лицо;

- оператор веб-сайта имеет законные основания для получения доступа к информации, имеющейся у интернет-провайдера, для идентификации личности.

Данная позиция была высказана до вступления в силу GDPR, в котором в отношении критерия идентифицируемости лица указывается, что необходимо учитывать все средства, которые разумно могут быть использованы *(all the means reasonably likely to be used)* для идентификации лиц. Поскольку суд не рассматривал данный аспект, в последующем позиция может быть скорректирована.

Контроль за сведениями о соединениях, содержании переговоров и переписки работника по сети связи, осуществляемых при использовании телефонной связи, доступа в интернет для служебных целей регулируется Законом о ПД (раздел 26). Согласно п.1 ст.26 персональные данные работников могут быть обработаны в целях, связанных с трудовыми отношениями, когда это необходимо для найма на работу, после него, для заключения или расторжения трудового договора, осуществления, удовлетворения прав работников. Кроме того, данные могут быть обработаны для обнаружения преступлений, только если имеются документально подтвержденные причины полагать, что субъект совершил такое преступление во время работы, и такие данные необходимы для расследования преступления. При этом, такая обработка должна быть пропорциональна законным интересам работника. Фактически, только это основание позволяет осуществлять контроль за сведениями о соединениях, содержании переговоров, переписки работников.

Приведем примеры привлечения работодателей к ответственности в случаях, когда ими осуществлялся такой контроль с нарушениями.

В 2009 году на Deutsche Bahn AG (немецкая компания, основной железнодорожный оператор) был наложен штраф в размере 1,1 млн евро Управлением по защите персональных данных Берлина за нарушение законодательства об обработке персональных данных[42]. Было выявлено, что с 2002 по 2005 год Deutsche Bahn проверяла большое количество данных о сотрудниках и сравнивала их с данными своих поставщиков в целях выявления коррупции. Такая деятельность не была связана с какими-то конкретными случаями коррупции и не относилась к конкретным лицам. Кроме того, с 2006 по 2007 год компания осуществляла мониторинг сообщений электронной почты сотрудников, которые использовали внешние учетные записи электронной почты на работе. Целью такого мониторинга было выявление связей с журналистами и работниками федерального парламента для того, чтобы обнаружить, какие из сотрудников компании раскрывают данные о компании.

В еще одном деле была сформулирована позиция, согласно которой не допускается осуществление мониторинга работников на рабочем месте, если конкретные подозрения в совершении какого-либо уголовного преступления или нарушения трудовых обязанностей отсутствуют[43]. В том числе, не допускается кейлоггинг (использование программного обеспечения или аппаратных устройств, регистрирующих различные действия пользователей на компьютере). В указанном деле было установлено, что работодатель подозревая работника в том, что большую часть своего рабочего времени он тратит не на выполнение своих служебных обязанностей, установил на его рабочий компьютер кейлоггер. Данная программа осуществляла мониторинг и запись всей информации, вводимой с клавиатуры в течение длительного периода времени. Кроме того, программа периодически делала скриншоты с экрана компьютера и сохраняла их. После анализа записанных программой данных было установлено, что в действительности большую часть рабочего времени работник посвящал компьютерной игре о космических кораблях, а кроме того, занимался обработкой заказов логистической компании своего отца, в том числе, разработал программу для обработки таких заказов. Работник был уволен, после чего обратился в суд. Суд пришел к выводу, что такой мониторинг нарушает Закон о ПД, и работник должен был быть предупрежден о

[42] Deutsche Bahn on track for million Euro fine [Electronic resource] // A Trend Micro Blog by Rik Ferguson [Site]. – URL: http://countermeasures.trendmicro.eu/deutsche-bahn-on-track-for-million-euro-fine/ (accessed: 09.08.2018); Es sind unzweifelhaft Straftaten geschehen 21.10.2009 [Electronic resource] // Suddeutsche Zeitung [Site]. – URL: https://www.sueddeutsche.de/wirtschaft/datenaffaere-bei-der-bahn-es-sind-unzweifelhaft-straftaten-geschehen-1.29461 (accessed: 09.08.2018).

[43] Bundesarbeitsgericht Urteil vom 27.7.2017, 2 AZR 681/16 [Electronic resource] // Bundesarbeitsgericht [Site]. – URL: http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=en&nr=19516 (accessed: 09.08.2018).

применении таких мер, либо у работодателя должны были быть конкретные основания полагать совершение работником недопустимых на рабочем месте действий, чего в данном случае не было.

Помимо этого обработка данных работника может осуществляться на основе его согласия. Однако согласно разделу 26 Закона о ПД теперь согласие на обработку персональных данных работника может использоваться, например, если сотрудник получает какое-либо преимущество от дачи такого согласия. В качестве примера такого преимущества можно привести обеспечение медицинского обслуживания.

В отношении требований по информационной безопасности при сборе, обработке, передаче, хранении сведений, составляющих тайну связи, необходимо отметить следующее. Прежде всего, требования к информационным системам, содержащим сведения, относящиеся к тайне связи, закреплены в Законе об информационной безопасности[44]. Кроме того, обязанности по обеспечению информационной безопасности провайдерами связи закреплены в разделе 109 Закона о связи. В частности, провайдер связи обязан принять соответствующие технические меры для обеспечения защиты тайны связи и персональных данных, а также предотвращения неавторизованного доступа к телекоммуникационным системам и системам обработки данных. Более подробная и детализированная информация о требуемых мерах безопасности доступна на сайте Федерального сетевого агентства Германии[45]. Помимо этого, требования к безопасности систем, содержащих персональные данные, предусмотрены в GDPR.

Испания

Тайна связи предусмотрена ч. 1 ст. 39 Закона о связи Испании (Общий закон о связи № 9/2014 от 9 мая (Ley 9/2014, de 9 de mayo, General de Telecomunicaciones)[46]. В ч. 2 ст. 39 Закон также содержит общую норму, согласно которой операторы, использующие сети

[44] BSI Act of 14 August 2009 (Federal Law Gazette I p. 2821) [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/englisch_bsig/englisch_bsig.html (accessed: 08.08.2018).

[45] Bundesnetzagentur [Electronic resource] – URL: https://www.bundesnetzagentur.de/EN/Home/home_node.html (accessed: 08.08.2018).

[46] Ley 9/2014, de 9 de mayo, General de Telecomunicaciones [Electronic resource]: Jefatura del Estado «BOE» núm. 114, de 10 de mayo de 2014 // Agencia Estatal Boletin Oficial del Estado [Site]. – URL: https://www.boe.es/buscar/pdf/2014/BOE-A-2014-4950-consolidado.pdf (accessed: 31.07.2018).

электронной коммуникации или оказывающие неопределенному услуги электронной связи, должны гарантировать тайну связи в соответствии с ч. 3 ст. 18 и ч. 2 ст. 55 Конституции, и для этого они должны принимать необходимые технические меры, но параллельно с этим они также должны принимать за свой счет меры, которые необходимы для исполнения запросов о предоставлении информации в соответствии со ст. 579 Уголовного кодекса Испании и Органического закона № 2/2002 от 6 мая о предоставлении данных Национальному разведывательному центру. Дополнительно ст. 41 Закона о связи Испании предусматривает, что операторы связи должны гарантировать при осуществлении своей деятельности защиту персональных данных в соответствии с действующим законодательством.

Общее понятие тайны раскрывалось в Испании еще на уровне судебной практики, по мере развития соответствующих спорных ситуаций. Доктрина[47] рассматривает в качестве репрезентативных примеров судебные дела, начиная с S.T.C. 114/1984 от 29 ноября, в которой указано, что тайна, с точки зрения содержания коммуникации, представляет собой «формальное понятие» и охватывает содержание коммуникации в любом случае, независимо от того, включается ли в эту коммуникацию область личного, интимного или ограниченного к доступу. Аналогичный подход повторен в более поздних решениях S.T.C. 34/1996 от 11 марта и S.T.C. 70/2002 от 3 апреля и последующих судебных решениях.

Общий принцип формирования тайны связи определяется с учетом системного толкования ст. 39 Закона о связи Испании и положений Конституции Испании (ч. 3 ст. 18 и ч. 2 ст. 55), на которые в нем содержится отсылка. Согласно ч. 3 ст. 18 Конституции Испании, гарантируется тайна связи, в том числе почтовых, телеграфных и телефонных коммуникаций, и она может быть ограничена только на основании судебного решения. Ч. 2 предусматривает порядок и обстоятельства отдельных ограничений конституционных прав, включая тайну связи, в отношении отдельных лиц в случаях расследования деятельности вооруженных преступных группировок или террористических сообществ.

В испанской правовой доктрине термин «связь» рассматривается как охватывающий все современные средства коммуникации, существующие сейчас и которые могут появиться впоследствии по мере технологического развития, и включает в себя, в том числе,

[47] Urgell A.M. Analisis juriprudenceial del derecho al secreto de las comunicaciones (art. 18.3 C.E.) [Electronic resource] // Diposit de la Recerca de Catalunya [Site]. – URL: https://www.recercat.cat/bitstream/handle/2072/9115/treballrecerca.pdf;jsessionid=C6A2AE06E8DA7C4B7A127B7D6F2BE9A6.recercat1?sequence=1. – P. 56 (accessed: 31.07.2018).

электронную почту и видеоконференции в сети Интернет.[48] Основным принципом толкования понятия «связь» рассматривается опосредованность общения между субъектами коммуникации, но при этом тайна связи естественным образом предполагает наличие закрытого канала связи – коммуникация не должна быть публичной. То же самое относится к любым средствам коммуникации в Интернете, за исключение случаев общения неопределенного круга лиц между собой.[49]

Для Испании остается актуальным принцип, высказанный в судебном решении S.T.C. 114/1984 от 29 ноября, согласно которому понятие тайны охватывает не только содержание коммуникации, но и также другие ее аспекты, такие как, например, личность субъектов коммуникации. В доктрине высказывается позиция, что «аспекты процесса коммуникации, которые **не являются очевидными для третьих лиц** (выделено мною – ***В.А.***) также должны охраняться ст. 18.3 К.И. [Конституции Испании]»[50] и что «определение тайны по ст. 18.3 К.И. охватывает лишь те обстоятельства, окружающие процесс коммуникации, в той степени, в которой они остаются тайной по отношению к третьим лицам».[51]

Из отдельных репрезентативных примеров судебной практики, в частности в решениях S.S.T.S. 316/2000 от 3 марта, 1235/2000 от 27 июня и 1.086/2003 от 25 июля, также были отражены подходы, согласно которым в случае, если полиция ограничила анализ памяти телефона сопоставлением номеров конкретных телефонных номеров, соответствующих допустимому объему вмешательства в тайну связи, это не является нарушением в конкретном случае.

С учетом указанных оговорок, принцип формирования сведений можно считать «открытым», содержание тайны связи определяется в конкретном случае.

Из определенной судебной практики следует, например, что в состав сведений, составляющих тайну связи, включается содержание телефонных переговоров (см. напр. Решение Конституционного Суда Испании 145/2014 от 22 сентября[52]). В отдельной судебной

---

[48] Urgell A.M. Analisis juriprudenceial del derecho al secreto de las comunicaciones (art. 18.3 C.E.) [Electronic resource] // Deposit de la Recerca de Catalunya [Site]. – URL: https://www.recercat.cat/bitstream/handle/2072/9115/treballrecerca.pdf;jsessionid=C6A2AE06E8DA7C4B7A127B7D6F2BE9A6.recercat1?sequence=1. – PP. 48 – 51 (accessed: 31.07.2018).

[49] Ibid.

[50] Morales M.R. El regimen constitucional del secreto de las comunicaciones. – Madrid: Civitas, 1995. – PP. 56-58.

[51] Rodriguez R.B. El secreto de las comunicaciones: tecnologia e intimidada. – Madrid: Mc Graw Hill, 1998. – P. 74.

[52]La Sala Segunda del Tribunal Constitucional TRIBUNAL CONSTITUCIONAL DE ESPAÑA [Site]. – URL: http://hj.tribunalconstitucional.es/es/Resolucion/Show/24106 (accessed: 31.07.2018).

практике, как было указано ранее, и как известно из судебных решений S.T.S. от 25 сентября 2003 г. и S.T.C. 56/2003 от 24 марта, личность субъектов коммуникации также охватывается тайной связи. Дополнительно в решении S.T.S. от 25 сентября 2003 г. к содержанию тайны связи было также отнесено содержание памяти мобильных телефонов задержанных граждан.

В целом же состав сведений, составляющих тайну связи, можно считать нормативно неопределенным, и он подлежит определению в каждом конкретном случае сообразно принципам формирования.

С учетом вышеизложенного, в испанской доктрине подчеркивается, что категория тайны [связи] является очень широкой, и пересекается с правом на неприкосновенность частной жизни.[53] В ст. 41 Закона о связи Испании содержится требование об установлении мер защиты персональных данных. Функционально, это отдельная норма права, и допустимо считать данные виды информации отдельными охраняемыми объектами.

Это, в частности, подтверждается и в недавних примерах доктрины, развивающих толкование упоминавшегося решения S.T.C. 114/1984 от 29 ноября. Тайна связи рассматривается как отдельное конституционное право, хотя и упоминаемое в одном контексте с правом на неприкосновенность частной жизни.[54]

Из системного толкования ст. 39 и ст. 42 Закона о связи Испании, а также с учетом положений ч. 3 ст. 18 Конституции Испании и доктринальных положений, можно сделать вывод о том, что тайна связи и иные виды тайн могут по аналогии рассматриваться как отдельные квалифицирующие признаки информации в том же смысле, в котором это рассматривается в законодательстве и практике Российской Федерации. На практике, однако, наибольшее значение имеет разделение между тайной связи и персональными данными, поскольку для каждого из указанных аспектов актуальны свои составляющие механизма правовой защиты.

Помимо общего механизма правовой защиты субъектов, ст. 41 Закона о связи предусматривает минимальный набор необходимых мер (гарантий) для защиты персональных данных, который включает в себя следующее: (1) только уполномоченные

---

[53] Urgell A.M. Analisis juriprudencial del derecho al secreto de las comunicaciones (art. 18.3 C.E.) [Electronic resource] // Diposit de la Recerca de Catalunya [Site]. – URL: https://www.recercat.cat/bitstream/handle/2072/9115/treballrecerca.pdf;jsessionid=C6A2AE06E8DA7C4B7A127B7D6F2BE9A6.recercat1?sequence=1. – P. 60 (accessed: 31.07.2018).

[54] Fernández M.A. El secreto de las comunicaciones en el proceso penal [Electronic resource] // Universidad Pontificia. Facultad del derecho [Site]. – URL: https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/593/TFG000519.pdf?sequence=1 (accessed: 31.07.2018).

работники имеют доступ к персональным данным для целей, установленных законом; (2) защита персональных данных от случайного или неправомерного уничтожение или изменения и иных подобных обстоятельств; (3) реализация действенной политики безопасности обработки персональных данных.

Тайна связи и защита конституционных прав в Испании находится в непосредственном отношении. Это вытекает и из общего подхода, в соответствии с которым Закон о связи Испании (ст. 39) содержит прямые отсылки к Конституции Испании (ч. 3 ст. 18 и ч. 2 ст. 55), и из судебной практики. Положения и принципы защиты тайны связи как конституционного права раскрывается преимущественно в практике интерпретации различных положений законодательства, прямо или косвенно связанного с ограничениями тайны связи, в положениях решений Конституционного Суда Испании. Например, уже упомянутое Решение Конституционного Суда Испании 145/2014 от 22 сентября,[55] в отношении тайны телефонных переговоров опирается в подавляющем большинстве случаев именно на правовые принципы, развитие в рамках конституционной юстиции. Кроме того, как показывают иные решения Конституционного Суда Испании, например, недавнее Решение Конституционного Суда Испании от 26/2018 от 5 марта,[56] тайна связи нередко рассматривается не только в контексте специальной ч. 3 ст. 18, но и в контексте общей ч. 1 ст. 18 Конституции Испании, которая закрепляет общее право на честь, личную и семейную тайну и собственное изображение (в части личной тайны). В том же судебном решении право на тайну связи рассматривается в одном контексте с конституционным правом на неприкосновенность жилища.

Трансграничная передача сведений, составляющих тайну связи, не урегулирована специально, и случаи трансграничной передачи подлежат общему регулированию на основании GDPR и национального законодательства о персональных данных.

Эстония

Тайна связи является конституционным правом по законодательству Эстонии. В

[55] La Sala Segunda del Tribunal Constitucional TRIBUNAL CONSTITUCIONAL DE ESPAÑA [Site]. – URL: http://hj.tribunalconstitucional.es/es/Resolucion/Show/24106 (accessed: 31.07.2018).

[56] La Sala Primera del Tribunal Constitucional Sala Primera. SENTENCIA 26/2018, de 5 de marzo (BOE number 90, of 13 April 2018) TRIBUNAL CONSTITUCIONAL DE ESPAÑA [Site]. – URL: http://hj.tribunalconstitucional.es/en/Resolucion/Show/25597 (accessed: 31.07.2018).

частности, в соответствии со статьей 43 каждый имеет право на тайну сообщений, передаваемых ему или им самим по почте, телеграфу, телефону или иным общеупотребительным способом. Исключения допускаются с разрешения суда в целях пресечения преступления или установления истины в ходе производства по уголовным делам в установленных законом случаях и порядке[57].

Применимое регулирование закреплено в Законе об электронной связи[58], вступившем в силу 1 января 2005 года в редакции от 23 мая 2018 года (далее - «Закон Эстонии о связи»). Как указано в ст. 1 Закона, его целью является создание условий для развития электронной связи, сетей связи и услуг без предоставления преференций каким-то отдельным технологиям в целях обеспечения и защиты интересов пользователей. Обеспечению безопасности предаваемых данных посвящена глава 10 (*Security and protection of data*).

В соответствии со ст. 101 Закона о связи Эстонии оператор связи обязан гарантировать безопасность сети связи и предотвращать несанкционированный доступ третьих лиц к информации. В частности на оператора связи возлагается обязанность сохранять конфиденциальность данных, касающихся пользователей и иных лиц, которые используют средства связи с согласия пользователей, а именно:

1. информации об использовании средств связи (*information concerning specific details related to the use of communications services*);
2. содержание и формат передаваемых сообщений (*the content and format of messages transmitted over the communications network*);
3. сведения о порядке и времени передачи (*information concerning the time and manner of transmission of messages*).

Данные, передаваемые посредством электронной связи, могут одновременно являться и сведениями ограниченного доступа, и персональными данными физических лиц. Перечень сведений является открытым, квалифицирующим критерием является способ распространения сведений.

Оператор связи обязан проинформировать пользователя об обработке такой информации таким образом, чтобы пользователь имел возможность отказаться от обработки. Без согласия пользователя допускается обработка данных для целей:

---

[57] The Constitution of the Republic of Estonia [Electronic resource]: entered into force of June 28, 1992 (as revised May 06, 2015) // Vabariigi Presidendi Kantselei [Site]. – URL: https://www.president.ee/en/republic-of-estonia/the-constitution/index.pdf (accessed: 30.07.2018).

[58] Electronic Communications Act [Electronic resource]: Riigikogu, December 08, 2004 (as revised May 02, 2018) // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/530052018001/consolide (accessed: 30.07.2018).

1. записи сообщений в ходе законной деловой практики для целей предоставления доказательства совершения коммерческой сделки или осуществления любого другого делового взаимодействия;

2. непосредственного предоставления услуг связи по запросу пользователя;

3. выставления счетов.

На оператора связи возлагается обязанность хранить информацию для целей осуществления следующих действий:

1. отслеживание и идентификация источников информации;

2. идентификация адресата информации;

3. идентификация даты, времени и продолжительности взаимодействия;

4. идентификация типа коммуникационного сервиса;

5. идентификация терминального оборудования или предполагаемого оборудования пользователя;

6. определение места нахождения терминального оборудования.

Дополнительные специальные обязанности по хранению данных в течение одного года с даты осуществления коммуникации возлагаются на операторов телефонной связи и Интернет провайдеров. В частности, операторы стационарной или мобильной связи обязаны хранить данные в отношении того, кто звонил и кому звонили, в том числе, телефонные номера, данные о времени и продолжительности звонков, серийные номера мобильных телефонов (IMEI), номера IMSI, сведения о локации и д.р. Интернет провайдеры, включая почтовые сервисы и провайдеров IP-телефонии, обязаны хранить ID-данные пользователей, телефонные номера, сведения о конкретной Интернет-сессии, IP-адреса устройства в сети Интернет, цифровые абонентские линии и т.д. Операторы обязаны обеспечить безопасность таких данных. Одновременно, указанные данные могут быть переданы в правоохранительные органы, органом безопасности, Инспекцию по защите данных, органам финансового, экологического надзора, полицию, службе внутренней безопасности, таможенные и налоговые службы, суды и органы надзора за указанными службами. Следует отметить, что с учетом последней практики ЕС в отношении массового хранения данных (дело *Digital Rights Ireland*, уже упомянутое в настоящем отчете) законность указных положений может быть поставлена под вопрос[59]. Помимо указанного выше Законом Эстонии о связи допускается

[59] Käsper K. On data retention and Estonia [Electronic resource] // Estonian Human Rights Centre [Site]. – URL: https://humanrights.ee/en/2017/12/data-retention-estonia/ (accessed: 30.07.2018).

раскрытие охраняемой информации органам по надзору и безопасности в сфере связи для проведении контрольных и надзорных мероприятий и третьим лицам с согласия пользователя.

Для целей маркетинга допускается использовать контактные данные пользователя - физического лица только с его предварительного согласия, предоставленного в соответствии с требованиями законодательства о персональных данных (*opt in*). Использование для тех же целей контактных данных пользователя – юридического лица допускается при условии предоставления возможности запретить такое использование с использованием электронных средств связи. Допускается использовать контактные данные лица, являющегося покупателем товаров или услуг, без его согласия при условии предоставления ему возможности запретить использование его данных для маркетинга в момент предоставления данных и каждый последующий раз с использованием электронных средств связи (*opt out*). Пункт 4 ст. 103 закрепляет перечень случаев, в которых запрещается использовать данные для целей маркетинга, включающий в себя случаи, когда лицо, от имени которого рассылается реклама невозможно определить, без предоставления лицу возможности отказаться от рассылки и т.д.

Использование данных пользователей в составе различных справочников и справочных сервисов разрешается при условии предварительного информирования пользователей о целях использования, количестве справочников или справочных сервисов, в которых предполагается использование, а также о возможности использования таких данных с использованием электронных поисковиков. Пользователям должно быть предоставлено право контролировать состав данных, а также возможность их изменять. Пользователи вправе в любой момент запретить такое использование, за исключением случаев внесения изменений или удаления данных в уже напечатанных справочниках.

Операторы вправе обрабатывать данные о месте нахождения пользователей (*location data*), если это не охватывается иным законным основанием для обработки из ранее перечисленных, только при условии предварительной анонимизации. Такие данные могут обрабатываться без анонимизации в целях предоставления иных услуг с согласия пользователя, предварительно уведомив его о том, какие данные будут использованы для предоставления иных услуг, целях и сроке использования данных, а также о необходимости передачи данных третьим лицам для целей предоставления услуг. Согласие лица не требуется для целей информирования пользователя об обстоятельствах, угрожающих его жизни или здоровью и мерах безопасности, когда такие сведения были переданы оператору органами

полиции или службами спасения.

Обработка данных осуществляется операторами связи или лицами, уполномоченными операторами в части организации платежей, обработки данных указанных в п.102 (1), ответов на запросы пользователей, выявления угроз, маркетинга услуг связи, перепродажи услуг связи или предоставления иных смежных услуг. Привлечение к обработке лиц в иных целях не допускается. За исключением случаев более длительного хранения, данные должны удаляться или анонимизироваться в течение одного месяца после достижения цели обработки. В установленных случаях данные должны удаляться незамедлительно.

В интересах публичного порядка и национальной безопасности допускается ограничение радиокоммуникаций правоохранительными органами на режимных территориях, на территории тюрем, органами внутренней безопасности на территориях, где требуется обеспечение повышенной безопасности.

В части персональных данных действуют специальные положения статьи 102 Закона Эстонии о связи. Применительно к персональным данным нарушением считается случайное или умышленное незаконное уничтожение, утрата, изменение, раскрытие или предоставление доступа к персональным данным, обрабатываемым с использованием электронных средств связи. В этом случае оператор обязан незамедлительно уведомить Инспекцию по защите данных. Если такое нарушение существенно затрагивает права и интересы субъекта данных, оператор должен уведомить и его при первой же возможности.

Пользователи могут обратиться за защитой своих нарушенных прав в судебном и во внесудебном порядке в Орган технического надзора (*Technical Surveillance Authority*) и в Инспекцию по защите данных. Нарушение обязательств по хранению и логированию данных влечет наложение штрафа на физических лиц в размере до 300 единиц штрафа (порядка 1200 Евро), для юридических лиц – наложение штрафа в размере до 3200 Евро. Ответственность за нарушение обязательств по конфиденциальности для физических лиц составляет штраф в размере до 200 единиц штрафа (порядка 800 Евро), для юридических лиц - штраф в размере до 2000 Евро.

За нарушение тайны сведений, передаваемых посредством почтовых сообщений и иных средств связи установлена уголовная ответственность в форме исправительных работ. В случае если данное преступление совершено лицом в связи выполнением своих должностных обязанностей - исправительные работы или лишение свободы до одного года. Для юридических лиц в обоих случаях установлена ответственность в форме исправительных

работ.

Статья 157 Уголовного кодекса Эстонии устанавливает ответственность за незаконное раскрытие персональных данных. В частности, если преступление совершено лицом, которое имело доступ к данным в связи с исполнением служебных обязанностей, но при этом деяние не содержит признаков преступления, предусмотренного статьёй 1571, то лицо подлежит ответственности в форме штрафа в размере to 300 единиц штрафа (порядка 1200 Евро). Для юридических лиц установлена штраф в размере до 32000 Евро.

Обратимся к репрезентативным примерам ***судебной практики***.

Дело 3-4-1-3-09 о проверке конституционности 50(3) и 461 Регламента № 72 от 30 ноября 2000 «Внутренние правила тюремного заключения».[60] Как следует из отчета от 10 октября 2008 года, из письменной корреспонденции одного из заключенных были изъяты и конфискованы два листа формата А-4. Заключенный обратился в суд с требованием вернуть его корреспонденцию. Как указывал истец, там содержались тексты песен, распечатанные из Интернета, и в соответствии со статьей 44 конституции он был праве получить их. По мнению заявителя, было нарушено его право на тайну корреспонденции, поскольку узнать о содержании бумаг было невозможно без их прочтения. Административный Суд Таллина согласился с заявителем и инициировал рассмотрение вопроса о конституционности соответствующих положений.

Конституционной палатой Верховного суда было установлено, что право на тайну корреспонденции охраняет любые сообщения и в равной степени принадлежит и заключённым. Суд соглашается с тем, что вскрытие корреспонденции и изъятие запрещенных предметов в присутствии лица, которому она адресована, не является нарушением ст. 43 Конституции. Вместе с тем, такое действие может являться нарушением права на невмешательство в частную и семейную жизнь, предусмотренное ст. 26 Конституции, которое также распространяется и на заключенных. В частности, это право подразумевает возможность направления супругом/супругой заключенного лица любых незапрещенных предметов посредством почтовой связи. Конституционная палата соглашается с тем, что внутренними правилами тюремного заключения не могут быть

[60] Review of constitutionality of § 50(3) and § 461 (in the wording in force from 26 September 2008 until 9 January 2009) of the Minister of Justice regulation no. 72 of 30 November 2000 “Internal Rules of Prison” [Electronic resource]: Judgment of the Constitutional Review Chamber of the Supreme Court No. 3-4-1-3-09 of June 25, 2009 // Supreme Court of Estonia [Site]. – URL: https://www.riigikohus.ee/en/constitutional-judgment-3-4-1-3-09 (accessed: 30.07.2018).

установлены дополнительные ограничения права заключённых на получение корреспонденции. По результатам рассмотрения положения 50(3) и 461 Регламента № 72 ль 30 ноября 2000 «Внутренние правила тюремного заключения» были признаны неконституционными.

Дело III-4/A-1/94 о проверке конституционности некоторых положений закона о внесении изменений в Закон о полиции.[61] Положениями оспариваемого закона были установлено, что разрешение на применение оперативных мероприятий может быть выдано с согласия члена Верховного суда. Это вытекает из ст. 43 Конституции Эстонии, гарантирующей каждому право на тайну вязи, которое может быть ограничено с разрешения суда в целях пресечения преступления или установления истины в ходе производства по уголовным делам в установленных законом случаях и порядке, предусмотренных законом. Обращение в суд в данном случае является обязательным требованием Конституции и может быть дозволено только в установленных целях.

Проанализировав оспариваемые нормы Палата пришла к выводу, что установленный порядок и основания применения оперативных мер были определены ненадлежащим образом с точки зрения необходимости защиты фундаментальных прав человека и таили в себе угрозу произвольного применения и неконституционного ограничения прав. Не было подробно указано, что именно понимается под оперативными мероприятиями, а также использовалась неоднородная терминология. В результате закон расширил сферу применения оперативных мероприятий по сравнению с тем, как было определено в Конституции, что привело к необоснованному расширению полномочий правоохранительных органов. Палата указала, что в случае, когда речь идет о конституционных правах личности, недопустимо фактически делегировать полномочия законодательных органов органам исполнительным. Положения закона о внесении изменений в Закон о полиции были признаны неконституционными.

Великобритания

В Великобритания тайна связи гарантируется Европейской конвенцией о защите прав

[61] Review of the petition of the Chancellor of Justice, submitted under § 142(2) of the Constitution, for the declaration of invalidity of subindent 4 of Part II of the Republic of Estonia Police Act Amendment Act under § Article 152(2) of the Constitution [Electronic resource]: Judgment of the Constitutional Review Chamber of the Supreme Court No. III-4/A-1/94 of January 12, 1994 // Supreme Court of Estonia [Site]. – URL: https://www.riigikohus.ee/en/constitutional-judgment-iii-4a-194 (accessed: 30.07.2018).

человека и основных свобод (от 04.11.1950), согласно ст.8 которой каждый имеет право на уважение его личной и семейной жизни, жилища и корреспонденции. При этом корреспонденция понимается в данном случае в широком смысле, а не только как письменная корреспонденция. Так, в деле Kennedy v. UK[62] ЕСПЧ указал, что не оспаривается тот факт, что почтовые отправления, телефонные разговоры и электронная переписка, включая те, которые осуществляются в контексте деловых операций, охватываются понятием «частной жизни» и «переписки» по ст.8 Европейской конвенции о защите прав человека и основных свобод. Также в деле Liberty and others v. UK[63] ЕСПЧ также пришел к выводу о том, что прослушивание телефонных разговоров и их запись является вмешательством в частную жизнь и права на уважение корреспонденции.

В отсутствие понятия тайны связи факт отнесения той или иной информации к ней подлежит исследованию в каждом конкретном деле. В связи с этим, можно сказать, что принцип формирования является открытым.

Состав сведений, составляющих тайну связи, сформулированный в судебной практике приведен выше. В то же время, некоторые сведения, составляющие тайну связи можно вывести из Regulation of Investigatory Powers Act 2000 (RIPA)[64]. Так, согласно его положениям выделяется понятие информации о трафике (traffic data) и данных связи (communication data).

Информация о трафике – это, в том числе, любая информация, идентифицирующая или предназначенная для идентификации любого лица, устройства или местоположение, любые данные, содержащиеся в конкретном сообщении.

Данные связи – это, в том числе, любая информация о трафике, или информация, которая не содержит в себе как таковых сведений о коммуникации, а также любая иная информация, которая хранится или получается в отношении лиц, которым представляется услуги (почтовые или телекоммуникационные).

---

[62] Case of Kennedy v. The United Kingdom [Electronic resource]: Judgment of the European Court of Human Rights dated of 18.05.2010 // Council of Europe Portal [Site]. – URL: https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-98473&filename=001-98473.pdf (accessed: 10.08.2018).

[63] Case of Liberty and Others v. The United Kingdom [Electronic resource]: Judgment of the European Court of Human Rights dated of 01.07.2008. // Centrum för rättvisa [Site]. – URL: http://centrumforrattvisa.se/wp-content/uploads/2011/03/CASE-OF-LIBERTY-AND-OTHERS-v.-THE-UNITED-KINGDOM.pdf (accessed: 10.08.2018).

[64] Regulation of Investigatory Powers Act 2000 [Electronic resource]: of the Parliament of the United Kingdom dated of 28.07.2000 // The National Archives [Site]. – URL: http://www.legislation.gov.uk/ukpga/2000/23 (accessed: 10.08.2018).

В процессе анализа сведения ограниченного доступа не выявлены.

Тайна связи включает в себя персональные данные в той части, в которой они идентифицируют лицо или могут идентифицировать его.

Механизм правовой защиты заключается в обязанности по сохранению конфиденциальности тайны связи, а также возможности лица, чья тайна связи была раскрыта обратиться за защитой права в судебном порядке. Кроме того, в части персональных данных субъект персональных данных может воспользоваться механизмом ст. 77 GDPR.

Согласно RIPA считается преступлением намеренное вмешательство в публичную или частную телекоммуникационную систему. Вмешательство в публичную систему возможно только при наличии законного основания. Вмешательство в частную систему возможно также при наличии законного основания, а также в случае, если лицо, осуществляющее вмешательство вправе контролировать эксплуатацию и использование такой системы или если было получено явное или подразумеваемое согласие на вмешательство. Помимо этого, согласно RIPA вмешательство в публичную телекоммуникационную систему может наказываться штрафом.

Мониторинг и запись телефонных разговоров регулируется двумя основными нормативными правовыми актами: RIPA и Закон о ПД 2018 г.

Положения RIPA применяются, когда лицо может произвести «прослушать (перехватить) сообщение в ходе его передачи». Для этих целей под термином прослушивание понимается мониторинг или вмешательство в частные коммуникации, которые в результате этого становятся доступными для третьих лиц (помимо отправителя и получателя сообщения) (п.4 ст.2 RIPA).

В целом прослушивание сообщений незаконно, и является уголовным преступлением. Однако возможность прослушивания сообщений допускается, если оно осуществляется в соответствии с исключениями, установленными законом.

Как упоминалось выше, вмешательство в телекоммуникационную систему запрещено, если отсутствуют законные основания для этого. Правоохранительным органам или службе разведки (раздел 5 RIPA) может быть выдан ордер на вмешательства в телекоммуникационную систему, если это необходимо для следующего:

- в целях национальной безопасности
- для целей предотвращения или обнаружения тяжкого преступления
- в интересах экономического благосостояния Великобритании в той части, в которой

такие интересы имеют отношение к интересам национальное безопасности

- для целей предотвращения или обнаружения тяжкого преступления в рамках международного договора о взаимопомощи.

При этом установлен специальный режим доступа к данным связи, которые включают метаданые, относящиеся к почтовой связи или телекоммуникациям, а также иную информацию, которую провайдер имеет о потребителе (раздел 21(4) RIPA). Доступ к данным связи может быть разрешен уполномоченным лицом правоохранительных органов.

В ст.22 RIPA сформулированы цели, в которых допускается получение данных связи:

- в целях национальной безопасности
- для целей предотвращения или обнаружения преступления, предотвращения беспорядков
- в интересах экономического благосостояния Великобритании в той части, в которой такие интересы имеют отношение к интересам национальное безопасности
- в интересах общественной безопасности
- в целях защиты общественного здоровья
- в целях оценки размера или сбора налогов, пошлин, сборов или иных обложений, пожертвований, отчислений в пользу государственных учреждений
- в целях предотвращения наступления смерти или нанесения увечий, иного повреждения физического или психического здоровья человека (в экстренных ситуациях), или для минимизации риска наступления таких последствий
- в целях помощи расследований в связи с предполагаемыми судебными ошибками
- с целью оказания помощи в идентификации любого лица, которое умерло не в результате преступления, или которое не может идентифицировать себя из-за физического или психического состояния, или с целью получения информации о ближайших родственниках или других связанных с ним лицах
- с целью осуществления функций, связанных с регулированием финансовых услуг и рынков, или финансовой стабильности.

Вопрос о возможности доступа третьих лиц к данным, составляющим тайну связи, был раскрыт выше. Администрирование согласий субъектов тайны связи на обработку сведений, составляющих тайну связи и/или их передачу третьим лицам (в т.ч. наличие права субъекта определять порядок использования таких сведений, делегирования права на выдачу согласий, отзыва согласий на их сбор, обработку и/или передачу и т.д.) подчиняется общим

правилам, установленным в GDPR.

Специальные нормы по идентификации субъектов тайн (в т.ч. их законных представителей) не выявлены.

В отношении форм и способов получения согласий, порядка фиксации и хранения подтверждения согласий следует отметить, что согласие на обработку сведений, составляющих тайну связи, аналогично согласиям на обработку иных персональных данных.

Соединенные Штаты Америки

Конституция США не закрепляет эксплицитно[65] право на частную жизнь, а также право на тайну связи, однако Верховный Суд США в многочисленных судебных решениях указывал, что Первая, Четвертая и Девятая поправка Конституции применимы к отношениям, затрагивающим тайну частной жизни (*Griswold v. Connecticut, Roe v. Wade, Lawrence v. Texas*). А право на тайну связи, благодаря правоприменительной практике, стало выводиться из Четвертой поправки,[66] и прослушивание телефонных разговоров без постановления суда стало трактоваться как нарушение Четвертой поправки (*Katz v. United States*).

Право на тайну связи регламентируется следующими федеральными законами США: Закон о свободе информации (the Freedom of Information Act of 1996); Закон о частной жизни (the Privacy Act of 1974); Закон о конфиденциальности электронных сообщений (the Electronic Communications Privacy Act, ECPA), Закон о защите личных данных водителя (the Driver's Privacy Protection Act of 1994); Закон Меган (Megan's Law of 1999), Закон о борьбе с компьютерными мошенничеством и противоправным поведением (the Computer Fraud and Abuse Act, CFAA) и различные разделы Закона о связи (the Communications Act).

ECPA и CFAA регулируют перехват электронных сообщений и несанкционированный доступ к компьютерам. Закон о содействии правоохранительным органам (CALEA), введенный в 1994 году, предусматривает то, что все телекоммуникационное оборудование должно быть спроектировано таким образом, чтобы государственные органы США, наделенные такими полномочиями, могли бы перехватить и прослушать телефонные

[65] Hao Wang. Protecting Privacy in China: A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China: Book. – Springer-Verlag Berlin Heidelberg, 2011. - P. 120

[66] The Social Science Research Networkhttp://ssrn.com/abstract=1348322

разговоры[67].

Федеральная комиссия по связи США (FCC) является основным регулятором за соблюдением положений о конфиденциальности информации, относимой к тайне связи, в некоторой части разделяя компетенцию с Федеральной торговой комиссией (FTC).

Кроме того, правовая система США предполагает регулирование рассматриваемого вопроса на уровне штатов. Для целей настоящего исследования штат Калифорния рассматривается как наиболее репрезентативный. В 1972 году в Конституцию штата Калифорния были внесены изменения[68], согласно которым на сегодняшний день тайна личной жизни (privacy) прямо закреплена в качестве неотъемлемого права человека. В разделе 1798.1 Гражданский Кодекс штата Калифорния указывает, что так как все более широкое использование информационных технологий значительно увеличивает потенциальный риск нарушения права на тайну личной жизни, в целях защиты частной жизни отдельных лиц необходимо, чтобы содержание и распространение личной информации подвергались строгим ограничениям. Таковые ограничения, выражающиеся в правилах оборота и обработки персональных данных, установлены в California Consumer Privacy Act of 2018[69] (CCPA), который вступает в силу в 2020 году. Кроме того, в 2015 году в Калифорнии был принят Закон о конфиденциальности электронных сообщений (CECPA), который не только устанавливает конкретизирующие нормы в отношении ECPA, но также и закрепляет термины и понятия, не содержащиеся в федеральном законодательстве, но релевантные для настоящего исследования.

В Законодательстве США принципы формирования сведений, составляющих тайну связи, не определены. Тем не менее, можно сформулировать следующие принципы на основании системного толкования применимых норм федерального законодательства и законодательства штатов.

ECPA не содержит дефиниции, позволяющей отграничить сведения, составляющие тайну связи, однако, Калифорнийский CECPA содержит следующее. «Информация об электронной связи» включает в себя любую информацию об электронной коммуникации или

[67] Virginia Horniak PRIVACY OF COMMUNICATION - ETHICS AND TECHNOLOGY [Electronic resource] // Mälardalen University Sweden [Site]. – URL: http://www.idt.mdh.se/utbildning/exjobb/files/TR0390.pdf

[68] J. Clark Kelso California's Constitutional Right to Privacy [Electronic resource] // Barkeley Law University of California [Site]. – URL: https://www.law.berkeley.edu/wp-content/uploads/2016/12/Kelso-Californias-Constitutional-Right-to-Privacy.pdf (accessed: 28.07.2018).

[69] California Consumer Privacy Act of 2018 (CCPA) [Electronic resource] // California Legislative Information [Site]. – URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (accessed: 28.07.2018).

использовании электронного коммуникационного сервиса, включая, но не ограничиваясь, сведениями о содержании, отправителе, получателе, местонахождении обоих в момент связи, IP-адресе и т.д[70] При этом закон разделяет информацию об электронной связи и «информацию об абоненте». Под последней понимается имя, адрес, телефонный номер, адрес электронной почты или иная контактная информация, доступная провайдеру, идентификатор или номер абонента, продолжительность оказания услуг, виды услуг, предоставляемых или предоставленных абоненту.

Таким образом, США оперирует открытым перечнем сведений, относящихся к тайне связи, основным критерием является прямое отнесение конкретной информации в предмет регулирования нормативно-правового акта (секторально), ввиду этого одни и те же данные, в зависимости от лица, их хранящего/обрабатывающего, могут обладать различным режимом оборота.

Здесь стоит отметить, что анонимизация или де-идентификация персональных данных в США занимает большое место в разрешении проблем, возникающих в связи с технологией больших данных. Используются для данных целей следующие методы: (1) маскирование данных, (2) добавление шумов, (3) скремблирование букв, (4) кодирование и т.д.[71]

Согласно § 1861 Закона о внешней разведке (FISA) детализация звонка – это информация, определяющая сессию звонка, включая номер телефона, международный идентификационный номер оборудования мобильной связи мобильного абонента или номер идентификатора оборудования мобильной связи), номер телефонной карты, время или продолжительность вызова, за исключением имени, адреса или финансовой информации абонента или клиента и данных о его местоположении. Термин «адрес» здесь включает в себя любой «[...] электронный адрес, например электронный адрес или временный сетевой адрес (включая адрес интернет-протокола)»[72].

Кроме того, согласно п. 3.2.2. к такой информации относятся не только сведения об электронной связи, но и информация, пересекающаяся с персональными данными. Согласно

---

[70] Electronic Communications Privacy Act (Section 1546) [Electronic resource] // California Legislative Information [Site]. – URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160SB178 (accessed: 27.07.2018).

[71] Dr. Khaled El Elmam Health Data De-Identification [Electronic resource] // The International Association of Privacy Professionals (IAPP) [Site]. – URL: https://iapp.org/media/pdf/knowledge_center/Perspectives_on_Health_Data_De-Identification_final.pdf (accessed: 27.07.2018).

[72] 50 U.S.C. §1861(k)(3) [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/uscode/text/15/6809 (accessed: 09.08.2018).

Закону о частной жизни (Privacy Act) идентификаторами, из-за которых та или иная информация начинает относиться к персональным данным, являются: имя, адрес, телефонные номера, адреса электронной почты, идентификаторы или серийные номера устройств, веб-адреса (URL-ссылки), IP-адреса.

Вместе с тем, стоит отметить, что вопрос о составе метаданных, относящихся к тайне связи, не является однозначным. Законодательство США не использует термин «метаданные», а также относимые к нему термины, которые использует Великобритания, Германия, ЕС. Вместо этого используется термин запись (record), относящийся сразу к самому содержанию и реквизитам документа.

Таким образом, имеется логичное разделение между «информацией об электронной связи» и «информацией об абоненте», однако исчерпывающего перечня законодательство и судебная практика не дает.

Сведения, составляющие тайну связи, могут одновременно охраняться как иные виды тайн и относиться к иным видам сведений ограниченного характера, в том числе: относиться к персональным данным и охраняться как тайна личной жизни.

Механизм правовой защиты субъектов включает в себя несколько видов правовой ответственности.

За нарушение тайны связи предусмотрены следующие виды ответственности:

(6) Уголовная ответственность – тюремное заключение на срок не более 5 лет и/или штрафом в размере не более 250.000 долларов США (если нарушить – физическое лицо), штрафа в размере не более 500.000 долларов США (если нарушить – юридическое лицо)[73].

(7) Гражданская ответственность – реальный ущерб, 100 долларов США за каждый день нарушения или до 10.000 долларов США за нарушение прав.

(8) Гражданская ответственность США перед субъектом, которому причинён вред – до 10.000 долларов США за каждый инцидент.

Как следует из информации, указанной выше, абонентские номера и иных идентификаторы абонентских устройств (в том числе серийный номер мобильного телефона (IMEI), номер IMSI, динамический или статический IP-адрес устройства в сети Интернет, уникальный идентификатор оборудования сетей передачи данных (MAC-адрес) относятся

[73] 18 U.S.C. 2511(4)(a) [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/uscode/text/15/6809 (accessed: 09.08.2018).

одновременно к тайне связи и к персональным данным.

Фактический состав сведений, относимых к тайне связи, приведен ранее и вычленен, в первую очередь, из толкования Закона о частной жизни (Privacy Act), Закона о внешней разведке (FISA), Закона о конфиденциальности электронных сообщений (ECPA) и Закона о конфиденциальности электронных сообщений штата Калифорния (CECPA).

Относительно порядка и условий передачи третьим лицам, сведений составляющих тайну связи, можно отметить следующее.

Передачу сведений, составляющих тайну связи, регламентируют в США три акта: Закон о частной жизни (Privacy Act), Закона о внешней разведке (FISA), Закон о конфиденциальности электронных сообщений (ECPA) и Закон о связи (Communications Act of 1934). Первый устанавливает ограничение на распространение, разглашение и допуск государственных органов до информации, относимой к персональным данным. Второй нормативно-правовой акт запрещает провайдеру услуг электронной связи раскрывать содержание сообщений, которые он хранит и/или передает, и ограничивает раскрытие таких данных государственным органам (но не частным лицам). Третий нормативно-правовой акт ограничивает использование и разглашение пользовательской сетевой информации (CPNI) поставщиками телекоммуникационных услуг и предоставляет право доступа к таковой для самих пользователей-физических лиц[74].

Предоставление сведений, составляющих тайну связи, допускается только в трех следующих случаях: (1) на основании решения суда, (2) с согласия одной из сторон-участников сеанса связи, (3) в отношении сеансов связи злоумышленника внутри электронной информационной системы.

Специальных правил и норм, определяющих порядок трансграничной передачи сведений, составляющих тайну связи, исследованным законодательством не предусмотрено.

Согласно ECPA поставщик услуг электронной связи или дистанционной обработки данных должен предоставить государственному органу (A) имя; (B) адрес; (C) записи локального и междугородного телефонного соединения или записи времени сеанса и продолжительности сеанса связи; (D) продолжительность оказания услуг абоненту (включая дату начала) и виды используемых услуг; (E) номер телефона или прибора или другой номер или идентификационный номер абонента, включая любой временный сетевой адрес; и (F)

[74] Gina Stevens Privacy Protections for Personal Information Online – April 6, 2011 [Electronic resource] // Federation of American Scientists [Site]. – URL: https://fas.org/sgp/crs/misc/R41756.pdf (accessed: 27.07.2018).

средства и источник платежа (включая номер кредитной карты или номер банковского счета) абонента, если государственный орган предъявляет (1) административный запрос, санкционированный федеральным законом или законом штата, федеральным или государственным большим жюри или (2) судебный запрос о предоставлении документов, или (3) иным способом, предусмотренным законом.[75]

Общие положения Закона о частной жизни 1974 года представляют право на представителя (representative), который может подписывать согласие, передавать персональные данные третьим лицам в интересах и от имени физического лица.

Специальных детализированных правил по форме согласия в отношении использования тайны связи законодательство США не содержит.

Законодательство США содержит исключения, позволяющие провайдерам услуг связи получать доступ, использовать сведения, подпадающие под тайну связи, (1) в рамках исполнения своих обязанностей как провайдеров, (2) для целей противодействия мошенничеству, (3) для целей содействия государственным органам и органам штата, если они действуют в рамках своих полномочий, (4) в рамках контрольных мероприятий, инициированных Федеральной комиссией по связи США.

К операторам связи предъявляются общие требования об информационной безопасности, и, в отличие от медицинской тайны, конкретный перечень мер не закреплен в специальном законодательстве. ECPA и CFAA не содержат положений об требованиях в сфере информационной безопасности.

ECPA позволяет работодателям перехватывать электронные сообщения, если сотрудник дает на это согласие, для этого работодатели должны ввести политику (IAUP), которая письменно уведомляет сотрудника о том, что любая деятельность в сети, даже не связанная с трудовой, может контролироваться работодателем, и что защита паролем не является гарантией личной конфиденциальности.

Сингапур

Конституция Сингапура не закрепляет эксплицитно право на частную жизнь, а также

[75] 18 U.S. Code § 2703 - Required disclosure of customer communications or records [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/uscode/text/18/2703 (accessed: 09.08.2018).

право на тайну связи[76]. Право на тайну связи регламентируется следующими федеральными законами: Закон о внутренней безопасности (Internal Security Act), Закон о телекоммуникациях (Telecommunications Act). Законодательства о запрете перехвата звонков и иных контртеррористических в Сингапуре нет[77].

Провайдеры услуг связи в Сингапуре являются государственными компаниями или аффилированными с государством компаниями[78], поэтому так или иначе передача информации, относимой к тайне связи, регулируется на уровне локальных нормативных актов, и не доступны для исследования.

Регламентация информации, относимой к персональным данным и к тайне связи одновременно, регулируется Законом о защите персональных данных (Personal Data Protection Act, PDPA), который устанавливает правила касательно состава данных, передачи данных и обязательных случаев раскрытия информации, относимой к персональным данным. Данный акт не регламентирует оборот данных для государственных органов.

В законодательстве Сингапура принципы формирования сведений, составляющих тайну связи, не определены. Тем не менее, можно сформулировать следующие принципы на основании системного толкования применимых норм законодательства и судебной практики.

Согласно PDPA персональные данные – это информация, достоверная или вымышленная, о физическом лице, который может быть идентифицирован (1) на основании этой информации или (2) на основании этой информации и иной другой информации, доступной для идентифицирующей организации. Согласно рекомендациям органа, являющегося надзорным в области защиты прав субъектов персональных данных в Сингапуре (PDPC)[79], идентифицирующей информацией являются, например, имя, адрес, номер телефона.

---

[76] Privacy and Human Rights [Electronic resource] // Global Internet Liberty Campaign [Site]. – URL: http://gilc.org/privacy/survey/surveylz.html (accessed: 27.07.2018).

[77] Kent Roach Comparative Counter-Terrorism Law [Electronic resource] // Google Books Library [Site]. – URL: https://books.google.ru/books?id=0UzzCQAAQBAJ&pg=PA627&lpg=PA627&dq=Wiretapping+Law+singapore&source=bl&ots=VAVeZfSrL-&sig=g4LhzsDGGzEqJa-_BtplMFAuz0s&hl=ru&sa=X&ved=2ahUKEwi6t9DSweDcAhWHBZoKHXoBDdM4ChDoATACegQICRAB#v=onepage&q=Wiretapping%20Law%20singapore&f=false (accessed: 27.07.2018).

[78] EPIC. Privacy and Human Rights Report 2006 [Electronic resource] // World Legal Information Institute [Site]. – URL: http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Republic-24.html (accessed: 27.07.2018).

[79] Personal Data Protection Commission, ADVISORY GUIDELINES FOR THE TELECOMMUNICATION SECTOR – May 16, 2014 [Electronic resource] // Personal Data Commission Singapore [Site]. – URL: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Sector-Specific-Advisory/finalised-advisory-guidelines-on-application-of-pdpa-to-telecom-sector.pdf (accessed: 27.07.2018).

В деле *Teo Wai Cheong v. Credit Industriel et Commercial* сказано, что записи телефонных разговоров с клиентами банка возможно передавать (раскрывать) третьим лицам, если вместо имен клиентов в информации о звонке будут обозначены обезличенные идентификаторы «A», «B», «C» и т.д. Поэтому информация, передаваемая в обезличенной форме, не регламентируется PDPA, а поэтому может быть свободно передаваема.

Таким образом, логичного разделения между персональными данными и информацией, относимой к тайне связи, законодательство и судебная практика не дает.

Сведения, составляющие тайну связи, могут одновременно охраняться как иные виды тайн и относиться к иным видам сведений ограниченного характера, в том числе: относиться к персональным данным и охраняться как тайна личной жизни.

Механизм правовой защиты субъектов включает в себя несколько видов правовой ответственности.

Если контролирующий орган обнаружит, что организация нарушает закон, регулирующий отношения в сфере персональных данных, он может наложить следующие обязанности на нарушителя:

a. прекратить сбор, использование или раскрытие личных данных, нарушающих закон;
b. уничтожить личные данные, собранные в нарушение закона;
c. обеспечить доступ к персональным данным или их исправление; ***и / или***

выплатить штраф в размере не более 1 миллиона долларов США[80].

Согласно рекомендациям PDPC, номер мобильного телефона человека, вероятно, будет классифицироваться как персональные данные, поскольку он может однозначно идентифицировать или быть связанным с этим лицом. Телефонный номер, которым владеют несколько лиц (например, стационарный телефон, совместно используемый несколькими жильцами в жилом помещении), также может считаться персональным данными, если в конкретных обстоятельствах сочетание с другой информацией приводит к идентификации личности.

Серийный номер мобильного телефона (IMEI) сам по себе не является персональными данными, однако, как только к IMEI начинает присоединяться, аккумулируясь, иная

[80] The Personal Data Protection Act 2012 (PDPA) [Electronic resource] // Personal Data Commission Singapore [Site]. – URL: https://www.pdpc.gov.sg/Legislation-and-Guidelines/Enforcement-of-the-Act (accessed: 27.07.2018).

информация о пользователе (не обязательно включающая в себя фамилию, имя и отчество лица), в этом случае данный объем информации будет определен как персональные данные. Такой же критерий относится и к IP-адресам.

Фактический состав сведений, относимых к тайне связи, отмечен в пунктах выше и вычленен, в первую очередь, из толкования Закона о защите персональных данных.

Относительно порядка и условий передачи третьим лицам, сведений составляющих тайну связи, можно отметить следующее.

Если специальный закон предусматривает раскрытие информации, которая может включать персональные данные, этот закон будет применяться в той мере, в какой он не согласуется с PDPA. Например, Закон о предотвращении коррупции налагает на лицо обязанность раскрывать любую информацию, запрашиваемую властями. В этих условиях данное обязательство раскрыть информацию будет иметь преимущественное значение над положениями о защите данных.

Принимая во внимание данную законодательную технику Сингапура, представляется, что изъятия из режима охраны в социальных, государственных, экономических целях могут носить не исчерпывающий характер в исследованном законодательстве и судебной практике.

Обобщая законодательство в части, контролирующий орган PDPA выделил некоторые исключения в отношении расследований и разбирательств. Организация может собирать данные об индивидууме без его или ее согласия, когда сбор необходим для любого расследования или разбирательства, с тем чтобы не поставить под угрозу доступность или точность персональных данных. Кроме того, организация может передавать личные данные физического лица без его согласия, если использование необходимо для вышеназванных целей.

Однако эти исключения не распространяются на внутренние проверки или расследования внутри коммерческих организаций. Тем не менее, некоторые авторы утверждают[81], что согласие со стороны сотрудников не требуется, поскольку такие проверки будут подпадать под действие трудового законодательства. Для соблюдения всех требований закона сотрудники должны быть уведомлены о таких потенциальных целях использования персональных данных в трудовом договоре или иным образом.

[81] The Privacy, Data Protection and Cybersecurity Law Review [Electronic resource] // The Law Reviews [Site]. – URL: https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151342/singapore (accessed: 27.07.2018).

Согласно PDPA юридическое лицо может передавать данные из Сингапура, однако такие данные должны быть надлежаще защищены согласно правилам PDPA. PDPA применяется к иностранным организациям в отношении деятельности, связанной с сбором, использованием и раскрытием персональных данных в Сингапуре, независимо от их физического присутствия в стране.

Поэтому в случае передачи персональных данных в Сингапур, положения о защите данных PDPA будут применяться в отношении деятельности, связанной с персональными данными в Сингапуре.

Случаи, условия и порядок использования и получения доступа к информации, составляющей тайну связи, без согласия субъекта тайны, главным образом, определяется специальным законодательством.

В 2011 году Сингапур запустил проект data.gov.sg: он содержит около 8600 наборов данных из 60 государственных министерств и ведомств. Он управляется Министерством финансов и Управлением развития инфокоммуникаций (IDA) Сингапура. Сингапурский земельный орган является одним из ключевых партнеров, поскольку он предоставляет OneMap, кадастровую карту, на которой основаны многие приложения.

В настоящее время только около 50 процентов наборов данных на data.gov.sg открыты (машиночитаемы), но IDA работает над наполнением базы открытых данных. Наиболее активным партнером по продвижению использования открытых данных является частная организация под названием «UP Singapore».

Чтобы получить доступ к данным, находящимся в базе данных gov.sg, пользователи должны пройти процедуру государственной регистрации, прежде чем использовать какой-либо из наборов данных, и согласиться с условиями использования сайта. Условия использования довольно строгие, например, в отношении положений об авторских правах и компенсациях за неправомерное использование.

Хотя данные предоставляются бесплатно, интеллектуальная собственность остается у государства. и сайт не предоставляет открытого лицензирования. Правительство Сингапура также может попросить пользователей прекратить использование наборов данных и удалить их из своих приложений или веб-сайтов по своей просьбе.

В настоящее время в Сингапуре нет главы фонда открытых данных и, как правило,

термин «открытые данные» не используется[82].

Особенностей доступа третьих лиц с согласия субъекта тайны и связанных с этим процессов не выявлено.

Специальным детализированных правил по форме согласия в отношении использования тайны связи законодательство не содержит.

Согласно Закону о телекоммуникациях использование и распространение информации в законных целях возможно без согласия субъекта персональных данных[83]. Данное право относится к так называемой информации об оказании услуг конечным пользователям (End User Service Information), в которую также входят сведения, относимые к персональным.

К операторам связи предъявляются общие требования информационной безопасности.

Хотя PDPA обязывает организации защищать личные данные, в настоящее время в законодательстве нет требования об уведомлении властей о произошедшей утечке данных. В отсутствие требований государственные регуляторы ввели специальные требования к таким сообщениям. Например, MAS выпустила ряд уведомлений для финансовых учреждений 1 июля 2014 года, чтобы указать, что все нарушения в сфере информационной безопасности должны сообщаться в MAS в течение одного часа после обнаружения.

В Сингапуре Закон о неправомерном использовании компьютеров и кибербезопасности (CMCA) является ключевым законодательством, регулирующим кибербезопасность, CMCA в первую очередь сосредоточен на определении понятий различных киберпреступлений, включая криминализацию несанкционированного доступа или модификацию компьютерных материалов, использование или перехват вычислительных центров, препятствование использованию компьютера и несанкционированное раскрытие кодов доступа и паролей. Поправки к 2017 году в CMCA предоставили возможность получения или предоставления государственным органам персональных данных, которые были получены в результате компьютерного преступления.

Несмотря на то, что CMCA в целом регулирует сферу уголовного права, поправки 2013 года ввели положения о мерах по кибербезопасности в случае обнаружения критических

[82] Waltraut Ritter Open Data in Asia. Knowledge Dialogues, August 2014 [Electronic resource] // Knowledge Dialogues [Site]. – URL: https://knowledgedialogues.files.wordpress.com/2014/07/open-data-asia-09-2014.pdf (accessed: 27.07.2018).

[83] Personal Data Protection Commission, ADVISORY GUIDELINES FOR THE TELECOMMUNICATION SECTOR – May 16, 2014 [Electronic resource] // Personal Data Protection Commission Singapore [Site]. – URL: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Sector-Specific-Advisory/finalised-advisory-guidelines-on-application-of-pdpa-to-telecom-sector.pdf (accessed: 27.07.2018).

угроз. В частности, министр внутренних дел имеет право поручить организациям принимать превентивные меры для предотвращения, обнаружения или противодействия любой угрозе кибербезопасности, если такая угроза может повредить интересам национальной безопасности[84].

Южная Корея

Право на тайну личной жизни базируется на Конституции Кореи и вытекает из следующих её положений: «Тайна личной жизни гражданина не может быть нарушена» (статья 17); «Тайна переписки гражданина не может быть нарушена» (статья 18). Также на основании данных положений было разработано такое понятие, как «право на самостоятельное определение личной информации». Право на тайну личной жизни было сформулировано как отдельное право в 2005 году в решении Конституционного Суда Коре, получившем название «Дело об отпечатках пальцев». В данном деле Конституционный Суд установил, что хотя право на тайну личной жизни, не сформулировано в качестве отдельного права в Конституции Кореи, оно вытекает из совокупности её положения.[85]

Законодательство Кореи не содержит определения понятия «тайна личной жизни», но содержит определение понятия «личная информация», которая, по сути, и охраняется с помощью тайны личной жизни.

Личная информация это информация, относящаяся к любому живому лицу, которая дает возможность идентифицировать такое лицо с помощью его имени, регистрационного номера резидента, изображения и так далее (в том числе, информация, которая сама по себе не дает возможности определить лицо, но позволяет сделать это в совокупности с иной информацией). Такое «широкое» определение понятия «личная информация» стало причиной возникновения многочисленных судебных споров о том, какая информация подпадает под определение «личной информации».

[84] Yuet Ming Tham The Privacy, Data Protection and Cybersecurity Law Review – Edition 4 [Electronic resource] // The Law Reviews [Site]. – URL: https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151342/singapore (accessed: 27.07.2018).

[85] The Constitution of the Republic of Korea [Electronic resource] // WIPO [Site]. – URL: http://www.wipo.int/edocs/lexdocs/laws/en/kr/kr061en.pdf (accessed: 27.07.2018).

International Mobile Equipment Identity (IMEI) case[86]

В деле IMEI разработчик приложения для смартфона собирал идентификационные данные пользователей международного мобильного оборудования и информацию об универсальном модуле идентификации абонента в процессе установки приложения на смартфон.

С помощью собранных данных разработчик приложения мог идентифицировать и запоминать пользователей смартфонов и предоставлять индивидуальные предложения по услугам пользователям приложения, на основании индивидуальной истории поиска каждого пользователя. Далее требовалась определённая информация не только для того чтобы определить девайс, но и установить непосредственно личность пользователя, поскольку идентификационные данные пользователей международного мобильного оборудования и информация об универсальном модуле идентификации позволяла определить конкретный девайс, но не позволяла определить личность пользователя. Таким образом, различные собранные данные о пользователе могли идентифицировать его личность. Собираемые о пользователе данные включали: имя пользователя, дату рождения, адрес, информацию о счете, информацию о девайсе. С другой стороны, у разработчика девайсов не было информации об имени пользователя конкретного девайса. Одним из ключевых вопросов в данном деле был вопрос о том может ли разработчик приложения законно получить доступ к данным пользователя, находящимся в распоряжении мобильного оператора. В данном деле суд признал данные, находящиеся в распоряжении разработчика мобильного приложения, личной информацией. Аргументация суда сводилась к тому, что для признания информации личной не обязательно устанавливать, мог ли разработчик приложения получить данные пользователя от мобильного оператора, а достаточно установить, что если такие данные каким-либо способом попадут в распоряжение разработчика приложения, разработчик приложения сможет без труда идентифицировать пользователя. Данные пользователей международного мобильного оборудования и информация об универсальном модуле идентификации абонента будут являться личной информацией, по мнению суда, поскольку при сопоставлении с данными мобильного оператора личность пользователя будет легко определить.

[86] Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung Structure and enforcement of data privacy in South Korea [Electronic resource] // The Social Science Research Network [Site]. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2904896 (accessed: 27.07.2018).

Mobile Phone Number case[87]

В деле Mobile Phone Number case перед судом был поставлен вопрос о том, являются ли 4 последние цифры в телефонном номере личной информацией.

В данном конкретном деле суд пришёл к выводу, что 4 последние цифры телефонного номера являются личной информацией. Суд аргументировал свою позицию тем, что, сопоставив четыре последние цифры мобильного номера с информацией о лице, которое использует такие последние четыре цифры для его или ее личного мобильного номера, с легкостью позволит идентифицировать конкретное лицо.

Ключевым актом, содержащим регулирование в отношении охраны любых видов тайн и тайны личной жизни в целом, является Закон «О защите личной жизни»: этот акт устанавливает общее регулирование. Данный акт имеет схожую структуру с системой охраны данных в ЕС. Регулирование по вопросам охраны тайн также содержится в специальных нормативных актах, однако, такие акты не посвящены конкретному виду тайны, а содержат специальное регулирование отношений в конкретном секторе либо какой-либо специфической информации (например, регулирование кредитной информации, регулирование данных о локации).

Перечень нормативных актов, регулирующих отношения, связанные с различными видами тайн, сводится к следующему.

- Конституция Республики Корея (*Constitution of the Republic Korea*)
- Закон «О защите личной информации» (*Personal Information Protection Act*)
- Закон «О Рекламной поддержке Информации и Коммуникационном Использовании Сети и Защите Информации (Закон о Коммуникационном Использовании Информации) (*Act on Promotion of Information and Communications Network Utilisation and Information Protection (Communications Network Act)*),
- Закон «Об Использовании и Защите Кредитной Информации» (Закон «О кредитной информации») (*Act on Use and Protection of Credit Information (Credit Information Act*)),
- Закон «О тайне коммуникаций» (*Communication Privacy Act*),
- Закон «О Финансовых Транзакциях под реальным именем и Гарантии Секретности (*Act on Real Name Financial Transactions and Guarantee of Secrecy (Real Name Financial*

[87] Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung Structure and enforcement of data privacy in South Korea [Electronic resource] // The Social Science Research Network [Site]. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2904896 (accessed: 27.07.2018).

Transactions Act),

- Законе «Об электронных финансовых транзакциях» (*Electronic Financial Transaction Act (EFTA)*)
- Закон «О Сообщении и Использовании Специальной Финансовой Информации о Транзакциях» (*Act on Report and Use of Specific Financial Transaction Information (Financial Transaction Information Act*),
- Закон «Об Использовании и Защите Информации о Местоположении (*Act on Use and Protection of Location Information (Location Information Act*)).

В законодательстве Кореи также различается такое понятие, как «информация с ограниченным доступом» («sensitive information»): это информация относительно идеологии, веры, информация об участии в политических партиях или профессиональных союзах, политические воззрения, здоровье, сексуальная жизнь.

В общем и целом, сравнив и обобщив процедуры доступа к информации, составляющей различные виды тайн, можно сделать вывод, что принципы осуществления такого доступа сводятся к следующему.

1. По общему правилу доступ к информации, охраняемой тайной личной жизни, медицинской тайной, тайной коммуникации, банковской тайной, осуществляется с разрешения субъекта такой информации.

2. В случаях, указанных в законе, доступ может осуществляться без согласия субъекта данных при наличии судебного решения (судебного приказа) о раскрытии таких данных.

3. В отдельных случаях, специально обозначенных в законе (которые в целом сводятся к обеспечению безопасности, предотвращении правонарушения, угрозе жизни и здоровью) информация может быть раскрыта без судебного решения.

При этом особыми правами в отдельных нормативно-правовых актах могут наделяться как органы государственной власти в целом, так и отдельные их представители (например, глава следственного органа).

Регулирование в отношении таких видов тайны, как медицинская тайна, тайна коммуникации, тайна личной жизни является схожим и базируется на Законе «О защите личной информации». В связи с этим в целях наиболее эффективного выполнения технического задания вопросы регулирования данных видов тайны будут рассмотрены совместно, при этом в случае наличия особенностей регулирования отдельных видов тайны они будут рассмотрены отдельно.

Порядок и условия передачи сведений, составляющих тайну, третьим лицам, а также аффилированным лицам и аудиторам

По общему правилу, в отношении любого вида тайны раскрытие информации может происходить только с согласия субъекта такой информации. В случае раскрытия информации, субъект информации должен быть поставлен в известность о таком раскрытии, а также о цели раскрытия, периоде раскрытия, о получателе такой информации.

В случае передачи информации о лице обработчиком информации третьему лицу, такая передача может происходить в следующих случаях.

1. Получено согласие субъекта данных

2. Получено решение (приказ) суда в связи с уголовным расследованием или по каким-то аналогичным причинам.

3. Информация передается без решения суда:

- когда такая передача предусмотрена специальным положением закона, прямо допускающим передачу информации, в случаях, когда такая передача неизбежна, и публичный институт осуществляет такую передачу в соответствии с законом;
- когда это необходимо для защиты от опасности, защиты жизни, здоровья или экономического благополучия субъекта данных или третьего лица, при этом субъект данных или его/ее представитель не намерен высказывать намерения либо предыдущее согласие не может быть расценено надлежащим, в силу неизвестности адресата.

4. Органы государственной власти, публичные органы могут запрашивать личную информацию для целей правоохранительной деятельности, административной деятельности: когда это необходимо для раскрытия преступлений, целей государственного обвинения и преследования, либо в рамках судебного производства с целью проведения производства по делу или для наказания и обеспечения исполнения судебного решения об ответственном хранении.

Защита, предусмотренная на законодательном уровне, распространяется лишь на информацию, которая отвечает определению понятия «личная информация». Если информация не отвечает данному определению, она может защищаться «частно-правовыми» методами: политикой конфиденциальности, отдельными договорами и соглашениями и так далее.

Наиболее актуальные вопросы судебной практики при раскрытии информации

третьим лицам

Предоставление информации без решения суда

Положение о предоставлении возможности запрашивать личную информацию без решения суда неоднократно становилось причиной судебных разбирательств. В качестве иллюстрации можно привести дело Lenz v. Universal Music Corp., рассмотренное Верховным Судом Кореи.[88] В данном деле интернет-провайдер предоставил государственному органу информацию в связи с производство по делу о правонарушении интеллектуальных прав. Верховный Суд признал, что в отсутствии четких критериев необходимости предоставления информации государственным органам, доказать виновность интернет-провайдера представляется крайне сложным.

(Статьи 15, 17 закона «О защите тайны личной жизни»)

Факт раскрытия информации третьим лицам

В некоторых случаях бывает сложно определить, действительно ли было совершено правонарушение и информация была раскрыта третьим лицам. В качестве примера может выступать дело **GS Caltex**.[89] Работник одной из дочерних компаний GS Caltex подготовил CD диски, содержащий личную информацию членов бонусной программы с целью извлечения личной финансовой прибыли, однако, не успел их распространить, поэтому информация, по сути, так и не была раскрыта или предана третьим лицам. Пользователи, чьи данные содержались на данных CD дисках, обратились в суд с иском против компании GS Catlex. Суд пришёл к выводу о том, что поскольку личная информация, в итоге, не была раскрыта, нарушение не было совершено, и права на взыскание убытков у пользователей не возникло.

Форма выражения согласия на передачу информации третьим лицам

Одним из наиболее актуальных вопросов является форма, в которой должно быть получено согласие на раскрытие информации третьим лицам. Примером может служить дело **Home Plus**.[90] В данном деле было получено согласие пользователей на раскрытие их личной информации для страховых компаний в маркетинговых целях. Было поставлено под

[88] Lenz v. Universal Music Corp [Electronic resource]: Seoul High Court 2010 na 35260 (S Korea, October 13, 2010) // Harvard Law Review [Site]. – URL: https://harvardlawreview.org/2016/06/lenz-v-universal-music-corp/ (accessed: 27.07.2018).

[89] Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung Structure and enforcement of data privacy in South Korea [Electronic resource] // The Social Science Research Network [Site]. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2904896 (accessed: 27.07.2018).

[90] Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung Structure and enforcement of data privacy in South Korea [Electronic resource] // The Social Science Research Network [Site]. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2904896 (accessed: 27.07.2018).

сомнение, правомерно ли получать согласие пользователей путём включения в стандартный договор пункта о получении согласия на раскрытие данных третьим лицам, при условии, что этот пункт написан таким мелким шрифтом, что текст практически не различим. Данное дело породило целый ряд судебных разбирательств по аналогичным вопросам.

Изъятия из режима охраны в социальных, государственных, экономических целях

На государстве лежит обязанность по разработке таких мер при раскрытии данных, чтобы максимально снизить негативный эффект от сбора личной информации. При этом в отдельных специальных нормативных актах содержится уточнение целей, для которых может собираться личная информация.

При этом в отношении данных публичного сектора, установлено, что государственные, публичные органы могут раскрывать личную информацию без специального решения суда для целей правоохранительной деятельности. При раскрытии данных, относящихся к данным частного сектора, доступ государственных органов к данным может осуществляться только с согласия субъекта данных, на основании закона или судебного решения.

Вопросы, связанные с тайной коммуникации, регулируются Законом « О тайне коммуникации» (в частности, статьи 5-8).

Ограничение в целях обеспечения национальной безопасности и предотвращении преступлений

Закон «О тайне коммуникаций» устанавливает возможность введения мер, ограничивающих коммуникации, для целей расследования преступлений в соответствии с предписаниями Уголовного Кодекса, Закона «О защите национальной безопасности», Закона «О защите военной тайны» либо для иных целей национальной безопасности, в соответствии с дозволением суда. При этом под «мерами, ограничивающими коммуникации», следует понимать проверку любого письма, прослушивание любой телекоммуникации, предоставление телекоммуникационных подтверждающих данных, запись или прослушивание разговоров, которые не были осуществлены публично». Меры, ограничивающие коммуникации, допускаются только в случае, если есть действительное основание полагать, что планируется совершение правонарушение либо преступление уже совершено и иным способом сложно предотвратить совершение преступления, арестовать преступника или получить доказательства. Главы определенных разведывательных и

следственных органов могут также предпринимать меры, ограничивающие коммуникации, когда они предполагают наличие угрозы национальной безопасности и такие меры необходимы для предотвращения опасности. Если меры, ограничивающие коммуникации, предпринимаются **против жителей Кореи**, разрешение необходимо получать у старшего председательствующего судьи Верховного Суда. Если меры, ограничивающие коммуникации, предпринимаются **против недружественных Корее стран, иностранных агентов, групп или лиц, подозреваемых в предприятии антинациональных действий или шпионаже для иностранных властей**, должно быть получено письменное разрешение Президента Республики Корея. Для расследования преступлений предпринимаемые меры не должны длится дольше двух месяцев, для противодействия угрозе национальной безопасности – 4 месяца.

В случае когда меры должны быть предприняты немедленно, поскольку вопрос касается преступления, совершаемого организованной группы против национальной безопасности, либо планируется совершение организованного тяжкого преступления, которое может повлечь смерть или тяжкий вред, государственный обвинитель, офицер полиции, глава разведывательного или следственного органа, может предпринять меры, ограничивающие свободу коммуникации без соответствующего разрешения суда, при условии что заявление в суд будет направлено сразу после такого как были предприняты такие меры. Если в течение 36 часов после того как были предприняты такие меры суд не вынесет решение о соответствующем разрешении, меры должны быть приостановлены.

Ограничение в рамках административных мер

Раскрытие частной информации может быть осуществлено государственными органами для административных или регуляторных целей. Регулирование по данным вопросам содержится в специальном законодательстве.

Ограничение в рамках анти-террористической деятельности

К изъятиям в государственных целях также относится раскрытие информации Национальному Разведывательному Управлению, когда такое управление осуществляет запрос в рамках деятельности по борьбе с терроризмом. Хотя по общему правилу для получения информации о содержании (контенте) коммуникаций, информации о въезде/выезде в страну, финансовой информации Национальное Разведывательное Управление должно соблюдать порядок получения информации, предусмотренный законом «Об тайне коммуникаций», закона «Об иммиграции», Закона « О раскрытии и использовании

Специальной Финансовой Информации о Транзакциях», для получения информации в рамках осуществления антитеррористической деятельности в соответствии с законом «Об антитеррористической деятельности» Национальное Разведывательное Управление может получать информацию без решения суда. Причем получить можно только определенный вид информации, а именно: контактная информация, информация о местоположении (локация), иная личная информация в случае, если она относится к террористической деятельности.

Данные о пассажирах

Государственные органы могут запросить у перевозчиков данные о пассажирах: национальность, имя, дата рождения, номер паспорта, номер брони, адрес, номер телефона, пункты следования, данные о туристической компании. Такими полномочиями обладают, например, руководитель Таможенного Органа, который может запросить у авиа- или судоходных компаний данные о бронировании пассажиров, если такие данные будут необходимы для целей обнаружения контрафактных товаров, наркотических средств, огнестрельного оружия, взрывчатых средств и иных запрещённых товаров. Аналогичными полномочиями обладают сотрудники иммиграционной службы, которые могут запросить данные о пассажирах в целях выявления пассажиров с недействительным паспортом или иным документом, удостоверяющим личность, либо приглашением, а также пассажиров, перевозящих огнестрельное оружие, взрывчатые вещества либо иные предметы, способные нанести вред здоровью.

Государственные органы также обладают полномочиями запросить информацию у физических и юридических лиц и любых частных организаций для осуществления сбора статистических данных.

Трансграничная передача сведений

В случае когда личная информация передается за рубеж третьему лицу, обработчик информации должен информировать субъекта данных о такой передаче, как и при раскрытии информации, и получить согласие субъекта на такую трансграничную передачу. В случае получения такого согласия, ограничений для трансграничной передачи информации нет. В отличие от регулирования, имеющегося в ЕС, в Корее нет регулирования, позволяющего без получения согласия субъекта данных осуществлять трансграничную передачу информации в страну, в которой, по мнению регулирующего органа, обеспечивается достаточный уровень

защиты персональных данных.[91] Осуществление передачи личной информации за рубеж в нарушение положений закона «О защите тайны» запрещено.

Механизмы правовой защиты прав субъектов тайн

(1) Права субъектов персональной информации на требования об уточнении, удалении, предоставление информации об обрабатываемых данных;

(2) Специальные требования в отношении обеспечения безопасности обрабатываемой личной информации;

(3) Механизм судебной защиты в порядке гражданского, уголовного, административного производства, а также возможность оспорить положения нормативно-правового акта на основании противоречия положениям Конституции;

(4) Возможность взыскания штрафных убытков в споре с обработчиком информации;

(5) Осуществление защиты личной информации многочисленными государственными органами;

(6) Деидентификация данных

Де-идентификация данных

В Южной Корее существуют правила (стандарты) о де-идентификации данных. Стандарты о де-идентифкации персональных данных были опубликованы под руководством Правительства Кореи, включая Отдел, отвечающий за Координацию Политики Правительства, Министерство Внутренних Дел, Комиссию по Коммуникациям Кореи, Комиссию по предоставлении Финансовых Услуг, Министерство Наук и другие отделы. Целью правил было установить стандарты по де-идентификации персональных данных и установить пределы использования персональных данных для безопасного использования больших данных, развития новых технологий, в том числе, технологии Интернета Вещей.

Процедура де-идентификации схематично может быть отображена следующим образом.

[91] Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung Structure and enforcement of data privacy in South Korea [Electronic resource] // The Social Science Research Network [Site]. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2904896 (accessed: 27.07.2018).

Рис. 1. Процедура де-идентификации данных.

Юридическая (в т.ч. уголовная, административная и гражданско-правовая) ответственность за разглашение и неправомерную обработку (в т.ч. специальными субъектами) сведений

Физическое лицо может защищать свои права в случае нарушении права на тайну личной жизни в порядке гражданского, уголовного, административного производства, а также осуществлять защиту в конституционном суда. Органы государственного обвинения могут также подать иск с целью осуществления тайны личной информации в случае совершения уголовного или административного нарушения. Механизм защиты юридических лиц ограничен и сводится, в основном, к защите нарушения прав на коммерческую тайну.

Гражданско-правовая ответственность

В случае если право на тайну личной жизни защищается в рамках гражданского судопроизводства, у стороны в соответствии с Гражданским Кодексом возникает право взыскивать убытки, моральный вред и право на обеспечительные меры. У лица, чьи права были нарушены, возникает право требовать штрафные убытки в размере, не превышающем тройной размер причинённых убытков. Также в пользу истца может быть взыскана компенсация в размере, не превышающем 3 миллиона вон без необходимости доказывать реальный ущерб. При этом если правонарушение совершено оператором персональных данных, то бремя доказывания лежит на ответчике: оператор должен доказать, что деяние было совершено не по его неосторожности или умышленно. При этом такая компенсация может быть выплачена в дополнение к компенсации убытков, если оператор данных не

сможет доказать отсутствие умысла или неосторожности.

На практике часто возникают споры относительно наличия умысла на совершение нарушения и небрежности в действиях. Примером спора по вопросу наличия небрежности в действиях ответчика является ***дело Auction***, рассмотренное Верховным Судом Кореи.[92] Auction является популярным сайтом, осуществляющим продажи через интернет. В 2008 году сайт был взломан и огромный массив личной информации о более 10 миллионах пользователях был похищен, включая имена пользователей, гражданские идентификационные номера, номера аккаунтов, адреса пользователей сайта. С исковыми заявлениями против сайта Auction обратилось около 146 000 пользователей. Верховный Суд указал, что в подобном деле необходимо оценить такие факторы, как уровень развития механизмов безопасности во время хакерской атаки, меры безопасности, которые предпринимались сайтом в момент атаки, технические способы взлома, используемые хакерами. Суд пришёл к выводу, что в данном случае Auction сделал все возможное для предотвращения хакерской атаки, поэтому действия Auction не могут быть расценены как неосторожные и во взыскании убытков должно быть отказано.

Уголовная ответственность

В случае если право на тайну личной жизни защищается в рамках уголовного судопроизводства, у стороны в соответствии с Уголовным Кодексом возникает право инициировать уголовное разбирательство против нарушившей стороны. Уголовно наказуемыми могут быть такие действия, как вскрытие каким-либо лицом письма, документа, рисунка, из вида или дизайна которых следует, что они являются секретными (в том числе, если на них содержится соответствующая пометка о секретности), а также получение доступа путём использования технических средств к содержимому (контенту) письма, документа, рисунка, или электронного документа. Уголовная ответственность может заключаться как в выплате штрафа, но также и в тюремном заключении. Уголовное разбирательство может идти независимо от гражданского и административного, при этом на практике часто после возбуждения уголовного дела за нарушение права на тайну личной жизни возникает

[92] Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung Structure and enforcement of data privacy in South Korea [Electronic resource] // The Social Science Research Network [Site]. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2904896 (accessed: 27.07.2018).

гражданское и уголовное разбирательство.[93] Министерство внутренних дел обладает полномочием на возбуждение уголовного дела в случае, если произошло серьезное нарушение Закона «О защите тайны личной жизни».

Административная ответственность

В соответствии с Законом «О защите личной информации», в случае нарушения данного закона у стороны есть право инициировать административное разбирательство, в результате которого на другую сторону будет возложено административное взыскание.[94]

Широким спектром административных полномочий обладает Комиссия по Охране Личной Информации (Personal Information Protection Commission ("PIPC")). Комиссия по Охране Личной информации обладает правом выносить резолюции по различным вопросам, связанным с охраной тайны личной жизни, которые, в том числе, включают резолюции относительно нормативных актов, политик, регулирования по вопросам защиты тайны личной жизни, интерпретации и применения указанных актов.[95] Комиссия готовит рекомендации государственным органам относительно охраны прав тайны личной жизни.

Правом налагать административный штраф за нарушение тайны личной жизни и налагать меры по устранению таких нарушений обладает **Министерство Внутренних Дел**. (ст. 34, 64 Закона «Об охране тайны личной жизни»). Министерство внутренних дел обладает правом делать выговор государственным служащим в случае допущения ими нарушений Закона «О защите тайны личной жизни».

Тайна связи

Записи интернет-журнала (дата, частота, длительность соединения) и записи телефонных разговоров (номера входящих и исходящих номеров, продолжительность разговоров, время звонков) относятся к личной информации и охраняются как личная информация только в случае, если поставщик услуг, собирающий информацию о записях интернет-журнала и записи телефонных разговоров также обладает базой данных, содержащей имена пользователей и/или их идентификационные номера и если у компании

[93] Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung Structure and enforcement of data privacy in South Korea [Electronic resource] // The Social Science Research Network [Site]. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2904896 (accessed: 27.07.2018).

[94] Privacy in South Korea: overview by Kwang Bae Park and Sunghee Chae, Lee & Ko [Electronic resource] // Thomson Reuters Practical Law [Site]. – URL: https://uk.practicallaw.thomsonreuters.com/6-579-7825?transitionType=Default&contextData=(sc.Default) (accessed: 09.08.2018).

[95] Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung Structure and enforcement of data privacy in South Korea [Electronic resource] // The Social Science Research Network [Site]. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2904896 (accessed: 27.07.2018).

есть техническая возможность совместить две эти базы данных.

Также в рамках вопроса о тайне связи, необходимо выделить Закон «Об информации о локации». Информация о локации это информация, которая может быть собрана с помощью оборудования для обеспечения связи и которое позволяет определить местоположения (локацию) пользователя. Информация о локации не является личной информацией, но тесно связана с такой информацией, поскольку при определенных обстоятельствах может позволить идентифицировать лицо. Для сбора информации о локации лица необходимо получить согласие такого лица на сбор этой информации и раскрытие её третьим лицам. (статья 36, Закона «Об информации о локации»).

Обязанности операторов связи по обеспечению соблюдения тайны связи, а также содержания этой обязанности

Данный вопрос регулируется Законом «О телекоммуникациях (Telecommunication Business Act). По общему правилу операторы связи должны получать согласие субъекта на раскрытие его данных третьим лицам, при этом третьи лица могут использовать такую информацию исключительно в соответствии с целями, для которых такая информация была ими получена. Однако Закон «О телекоммуникациях» предусматривает исключения: в случаях когда информация передается правоохранительным органам, которые обладают правом на получение такой информации по решению суда в соответствии с Уголовным Процессуальным Кодексом, получение согласия субъекта данных не является обязательным.

Однако в соответствии с Законом «О телекоммуникациях», телекоммуникационные операторы могут раскрывать данные и без решения суда, если такой запрос адресован судом, государственным обвинителем, главой органа расследования или службы разведки, когда такая информация необходима для целей судебного спора, расследования преступления, национальной безопасности или исполнения приговора. При этом в формулировке закона используется слово «может» , такой обязанности не установлено. К данным, которые могут быть раскрыты в таком порядке, относятся: имена пользователей, идентификационные коды, использующиеся для идентификации пользователей сети, даты, когда пользователи оформили подписки или отменили её.

Некоторые интернет-провайдеры в Корее начали на добровольной основе публиковать отчеты о доступности сервисов данных (transparency report)

Механизмы правовой защиты прав субъектов тайн;

Юридическая (в т.ч. уголовная, административная и гражданско-правовая)

ответственность за разглашение и неправомерную обработку (в т.ч. специальными субъектами) сведений

В соответствии с Законом «О защите тайны коммуникации», уголовно наказуемым деянием является получение доступа или запись содержимого (контента) при передаче или получении любых звуков, слов, символом или изображений путём передачи по проводам, беспроводным способом, по оптоволоконному кабелю или с помощью другой электромагнитной системы, включая телефон или электронную почту в отсутствие согласия субъекта указанной информации.[96]

Наиболее релевантная судебная практика

Положение о раскрытии информации без решения суда стало причиной судебного разбирательства, рассмотренного Судом Центрального Округа Сеула в 2010 году, а затем пересмотренное Верховным Судом Сеула в 2011 году и Верховным Судом Кореи в 2012 году.[97] В то время как в первой инстанции суд пришёл к выводу о том, что раскрытие информации в предусмотренном в Телекоммуникационном акте порядке без разрешения субъекта информации не может причинить такому субъекту психологический стресс, поскольку такое раскрытие считается правомерным с точки зрения закона. Однако Верховный Суд указал, что одного только запроса государственных органов недостаточно (даже если он осуществляется в указанном в законе «О Телекоммуникациях» порядке): раскрывающий данные субъект должен оценить тяжесть преступления, ради которого запрашивается информация, степень необходимости такой информации, публичные интересы, которые затрагивает данный вопрос, и соотнести указанные факторы с уровнем вреда, причиняемого субъекту информации в результате раскрытия такой информации. Только в таком случае будет обеспечено право пользователей на анонимность.

Такое решение было подтверждено и Верховным судом Кореи, однако, им также были даны дополнительные разъяснения по поводу того, каким образом должны быть интерпретированы положения о раскрытии информации без согласия субъекта информации. В частности, Верховный Суд указал на наличие различий между понятиями «контактная информация» и «телекоммуникационные подтверждающие данные». К контактной

[96] Kwang Bae Park, Hwan Kyoung Ko Data Protection 2018 [Electronic resource] // International Comparative Legal Guides [Site]. – URL: https://iclg.com/practice-areas/data-protection-laws-and-regulations/korea (accesssed: 27.07.2018).

[97] Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung Structure and enforcement of data privacy in South Korea [Electronic resource] // The Social Science Research Network [Site]. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2904896 (accessed: 27.07.2018).

информации относятся: имя, адрес, телефонный номер, номер регистрации резидента, идентификационный код пользователя. Именно контактные данные могут раскрываться без согласия пользователя и без решения суда. К телекоммуникационным подтверждающим данным относятся данные о том, когда пользователь осуществлял коммуникацию, каким способом он это делал, как долго длилась коммуникация, а также данные о местоположении пользователя в этот момент. При этом Верховный Суд Кореи отметил, что хотя у интернет-провайдеров нет обязанности раскрывать информацию органам государственной власти и они должны самостоятельно принимать решение о том, необходимо ли раскрывать данные в каждом конкретном случае, часто под давлением государственных органов власти они не имеют иного выбора, кроме как раскрыть информацию. В связи с этим в случае если орган государственной власти неправомерно запрашивает информацию и интернет-провайдер раскрывает такую информацию, ответственность за нарушение прав на тайну коммуникации будет возложена на государственные органы, осуществившие запрос. Аналогично интернет-провайдеры не будут нести ответственность за раскрытие данных Национальному Разведывательному Управлению Кореи, которое то осуществляет в рамках борьбы с террористической деятельностью.

В Кореи известны случаи анонимизации данных, охраняемых тайной связи, и использовании таких данных. Так, Korea Telecom предлагала доступ к анонимизированным данным, содержащим данные о тестах пользовательских сообщений и мест звонков с целью поддержки транспортного планирования – оптимизации работы ночного транспорта и решения проблем с перегруженным трафиком.

Израиль

В основе законодательства Израиля о тайне личной жизни лежит принцип охраны частной жизни, закреплённый в части 7 Основополагающих принципов ***(Basic Law: Human Dignity and Liberty 5752 – 1992)***. Основополагающие принципы содержат базовые правила:

- Все лица обладают правом на тайну личной жизни и личных связей;

- Вмешательство в частную жизнь лица без его согласия запрещено;

- Осуществление поиска на частной территории запрещён, за исключением случаев, включая личный досмотр и осмотр личных вещей;

- Не допускается нарушение конфиденциальности разговоров, переписки или записей лица.

При принятии решения о раскрытии сведений, охраняемых как тайна личной жизни, перед судом ставится вопрос о соблюдении баланса интересов, а именно, необходимо оценить, является ли раскрытие информации столь необходимым, что ставится под угрозу право лица на тайну личной жизни. Примером служит прецедентное дело **Association for Civil Rights in Israel v. Minister of Interior (2004)**, где Верховный Суд указал, что передача данных осуществлялась в неоправданно большом объеме и это приводило к нарушению баланса интересов, поскольку нарушались права на тайну личной жизни отдельно взятых лиц, данные которых передавались. Суд указал, что передача данных должна быть ограничена на законодательном уровне путем указания получателей данных, способов использования данных, мер охраны данных. При этом в деле **Rami Mor v. Barak ETC (2010)** Верховный Суд в принципе отказал в вынесении судебного приказа о раскрытии личности обвиняемого на основании права на анонимность. При этом судья Eliezer Rivlin указала, что анонимность в определенных пределах должна уважаться, так как это является частью интернет-культуры.

Специальным нормативным актом является закон «О защите тайны личной жизни» 5741 – 19811 (Protection of Privacy Law, 5741 – 19811), который содержит общее регулирование тайны личной жизни, а также ряд специальных актов для каждого из вида тайн.

Условно структура нормативных актов в Израиле, регулирующих вопросы тайны, строится следующим образом.

- Основополагающие принципы ***(Basic Law: Human Dignity and Liberty 5752 – 1992)***.
- Закон «О защите тайны личной жизни» 5741 – 19811 ***(Protection of Privacy Law, 5741 – 19811).***
- Закон «О коммуникациях», 2007 ***(Communications Data Act, 2007)***
- Телекоммуникационный Акт, 1982
- Закон «О прослушивании», 1979 ***(Wiretap Act, 1979)***
- Закон «О защите прав пациента» , 1996 год ***(Patient's rights act, 1996)***
- Закон «О медицинской помощи» ***(Medical Help Act)***,

- Закон «О генетической информации» , 5761-2000 ***(Genetic Information Law, 5761-2000)***
- Коммерческий Торговый закон ***(Commercial Trade Act)***
- Закон об инвестиционном консультировании, 5755–1995
- Закон «О запрете отмывания денежных средств» ***(Anti-money laundering Act)***
- Закон «О данных кредитных услуг», 5762–2002
- Закон «О передаче информации в базы данных, находящиеся за пределами государства», 5761-2001
- Закон «О международной юридической правовой помощи» 5758
- Закон «О клевете», 5725 – 1965, ***(Defamation (Protection) Law, 5725 – 1965)***
- Ответственность содержится как непосредственно в специальных нормативных актах, также и в актах общего характера.
- Гражданская ответственность: Закон о гражданских правонарушениях ***(Civil Wrongs Ordinance).***
- Уголовным Процессуальным Законом, 2007 ***(Criminal Procedure Act (Enforcement Powers – Communications Traffic Data).***

Законодательство Израиля содержит такое понятие, как «данные связи» («communication data»). К данным связи относятся: данные о локации, данные абонентах, информация о трафике. При этом данные о содержании (контенте) регулируются отдельным актом.

Ключевыми актами, содержащими регулирование, являются: Закон «О коммуникациях», Уголовный Процессуальный Закон, 2007 (Criminal Procedure Act (Enforcement Powers – Communications Traffic Data), 2007 (Communications Data Act)).

Данные, охраняемые тайной связи, могут также рассматриваться как данные, охраняемые тайной личной жизни, как ПД, большие пользовательские данные.

Обязанности операторов связи по обеспечению соблюдения тайны. Телекоммуникационные провайдеры должны соблюдать тайну связи. Однако в определенных случаях они могут раскрыть такие данные. Такие запросы могут следовать от суда, прокурора, главы следственного органа, главы спецслужбы, когда это требуется для расследования преступления, в рамках судебного разбирательства, вынесения наказания, национальной безопасности. Данные, которые могут быть раскрыты: имена пользователей,

резидентские номера пользователей, адреса пользователей, их телефонные номера, идентификационных коды, используемые для для идентификации пользователей в телекоммуникационной сети, даты, кода пользователи подтвердили или отменили свою подписку.[98]

Порядок и условия передачи сведений, составляющих тайну связи, третьим лицам, а также аффилированным лицам и аудиторам. Вопрос регулируется, в частности, статьями 3, 4 Закона «О коммуникациях» Передача сведений может осуществляться в следующем порядке.

1. Получение разрешения на доступ к сведениям осуществляется по решению суда (по общему правилу). Полиция, а также иные ведомства, относящиеся к силовым структурам, может запросить Мировой Суд предоставить коммуникационные данные в случае, если это необходимо для спасения или защиты жизни лица.; раскрыть, расследовать или предотвратить преступление, задержать или привлечь к ответственности лицо, совершившее преступление,; конфисковать по закону собственность.

2. Разрешение доступа к сведениям получается без решения суда (в определённых ситуациях). Старший офицер полиции может издать срочный приказ, вступающий в силу на 24 часа, если такой приказ необходим для предотвращения преступного деяния или остановить преступника, или спасти жизнь лица и недостаточно времени для получения разрешения через суд. О количестве таких приказов офицеру необходимо докладывать парламентскому комитету и генеральному прокурору.

Трансграничная передача сведений. Закон «О международной юридической правовой помощи» 5758-1998 содержит обязанность по трансграничной передаче данных в рамках осуществления кооперации между Израилем и иным государством. В соответствии с данным законом, иностранное государство может запросить у Израиля перечень информации, которая необходима такому государству в связи с вопросами, связанными с уголовным или гражданским судопроизводством. Такая передача осуществляется через Министерство Юстиции и с разрешения Министра Юстиции.

Регулирование по данному вопросу также содержится в Законе «О передаче информации в базы данных, находящиеся за пределами государства», 5761-2001. Данный

[98] Omer Tene Systematic Government Access to Private-Sector Data in Israel: Balancing Security Needs with Democratic Accountability [Electronic resource] // Oxford Academic. International Data Privacy Law [Site]. – URL: https://academic.oup.com/idpl/article/2/4/277/676924 (accessed: 27.07.2018).

закон был принят с целью предотвращения передачи данных в страны, где тайна личной жизни не получила необходимый и достаточный уровень охраны.

Случаи, условия и порядок передачи сведений, составляющих тайну связи, третьим лицам без согласия субъектов тайны. Информация, составляющая тайну личной жизни, может получаться специальным охранными службами, в том числе, полицией, военными службами(“Aman”), Израильской Службой Безопасности (“Shin Bet” или “Sahabak”), Разведывательной Службой (“Mossad”). В случае если право на тайну личной жизни будет нарушено лицом в связи с исполнением обязанностей, которые на него возложены законом, такое лицо не будет нести ответственности.[99]

Обязанности операторов связи по обеспечению соблюдения тайны связи, а также содержания этой обязанности. По общему правилу, телком операторы или их работники не могут разглашать коммуникационные данные. Однако в определенных случаях данные могут раскрываться. Такие запросы могут следовать от суда, прокурора, главы следственного органа, главы спецслужбы, когда это требуется для расследования преступления, в рамках судебного разбирательства, вынесения наказания, национальной безопасности. Данные, которые могут быть раскрыты в таком порядке: имена пользователей, резидентские номера пользователей, адреса пользователей, их телефонные номера, идентификационные коды, используемые для идентификации пользователей в телекоммуникационной сети, даты, кода пользователи подтвердили или отменили свою подписку.

В соответствии с Телекоммуникационным Актом 1982 года, государственные власти могут обратиться к операторам телекоммуникаций с инструкциями об изменении и модифицировании оборудования с целью «встраивания» специального оборудования для прослушивания.

В соответствии со статьёй 13 Телекоммуникационного Акта, премьер-министр, после консультаций с Министерством Обороны, Министерством Национальной Безопасности, Службой Безопасности Израиля или службой Моссад, может дать инструкции операторам телекоммуникаций об установке специального оборудования, а также о предоставлении доступа к этому оборудованию секретных служб.

В Израиле также существует специальный закон «О прослушивании», 1979 (Wiretap Act). Под «**прослушиванием**» понимается прослушивание беседы с использованием

[99] Ibid.

девайсов без разрешения какой-либо из сторон, участвующих в беседе. При этом под «беседой» понимается не только устный разговор, но также коммуникация между компьютерами. Такое прослушивание запрещено за исключением случаев, когда оно осуществляется на законных основаниях национальными службами безопасности и правоохранительными органами. Прослушивание полицией осуществляется по решению Президента Районного Суда.

Механизм правовой защиты субъектов состоит из следующих элементов:

(1) Раскрытие информации по общему правилу осуществляется только с согласия субъекта тайны;

(2) Круг субъектов, который может иметь доступ к тайне без согласия субъекта тайны, ограничен.

(3) Случаи, когда допускается разглашение сведений, составляющих тайну коммуникации, строго ограничены.

За неправомерное разглашение сведений, составляющих тайну, предусмотрена юридическая ответственность.

Нарушение тайны личной жизни в соответствии с частью 4 главы 1 Закона «О защите тайны личной жизни» является гражданским правонарушением. Такие нарушения регулируются положениями Закона «О гражданских правонарушениях».

В соответствии с положениями части 5 главы 1 Закона «О защите тайны личной жизни», лицо, которое намеренно нарушает тайну личной жизни способами, предусмотренными в законе, могут быть подвержены тюремному наказанию на срок до пяти лет.

В соответствии с частью 6 Закона «О защите тайны личной жизни» , право на судебное разбирательство в результате нарушения положений Закона «О защите тайны личной жизни» не возникает, если нарушение является незначительным (в отношении как гражданско правонарушения, так и уголовного).

Нарушение тайны личной жизни может повлечь за собой возмещение ущерба.

В случае если лицо привлечено к ответственности в соответствии со статьёй 5 Закона «О защите тайны личной жизни», суд может взыскать с такого лица компенсацию ущерба в сумме, не превышающей 50 000 шекелей.

Закон «О защите личной жизни» в статье 19 также указывает на основания освобождения от ответственности.

Лицо не должно нести ответственность за действия, которые такое лицо было уполномочено совершать по закону. Органы по охране безопасности или лицо, трудоустроенное такими органами или уполномоченное действовать от лица таких органов не должно нести ответственность за нарушение, обоснованно совершенное в рамках исполнения своей функции или для целей осуществления таких функций.

Под органами по охране безопасности понимаются: полиция Израиля, Служба Разведки Генерального Штаба, Военная Полиция Обороны Израиля; Всеобщая Служба Безопасности; Особая Служба Разведки (Моссад)

В любых уголовных или гражданско-правовых спорах о нарушении тайны личной жизни защищающаяся сторона будет добросовестной в случае, если:

(1) нарушение было осуществлено с помощью публикации, защищённой Законом «О защите чести и достоинства».

(2) ответчик или обвиняемый совершил нарушение при условии осуществления действий добросовестно и в одном из следующих случаев

(a) он не знал и не должен был знать о том, что может случить нарушение тайны личной жизни;

(b) нарушение было совершено в таких обстоятельствах, при которых лицо, осуществившее нарушение находилось в ситуации, когда нарушние было вызвано его юридическими, моральными социальными или профессиональными обязательствами;

(c) нарушение было совершено в рамках осуществления защиты законных личных интересов нарушителя;

(d) нарушение было совершено в рамках законного осуществления деятельности нарушителям=и в рамках обыкновенного течения работы, в случае если нарушение не было осуществлено путём публикации;

(e) нарушение было осуществлено путём создания фотографии или опубликования сделанной фотографии, если такая фотография была сделана в месте открытого доступа и сторона, чьи права были нарушены, была запечатлена на такой фотографии случайно;

(3) нарушение включало публичный интерес, что оправдывалось обстоятельствами дела, в случае, если нарушение было совершено путём публикации, при этом публикация не являлась ложной.

Объединенные Арабские Эмираты

Законодательство ОАЭ не содержит понятия тайны связи. Однако статьей 31 Конституции ОАЭ гарантирована свобода почтовой переписки, передачи телеграфных сообщений и прочих средств связи, а также их тайна. Кроме того, в ключевом для понимания тайны связи нормативном документе – Регламенте о защите потребителей (далее – Регламент)[100] содержатся положения, обязывающие обеспечивать защиту данных абонента (п.13.3 Регламента). Толкование положений п. 13.4 Регламента позволяет сказать, что данные абонента включаются в конфиденциальную информацию провайдера услуг связи.

Данные абонента - это любые персональные данные относящиеся к конкретному абоненту и включают, но не ограничиваясь, его имя, адрес, банковские реквизиты, реквизиты кредитной карты, детали для использования услуги, записи о вызовах и сообщениях, любая информация, возникающая вследствие использования абонентом телекоммуникационных услуг, статус абонента, история платежей и рейтинг кредитоспособности (п. 2.1.13 Регламента).

Законодательство ОАЭ не содержит принципов формирования сведений, составляющих тайну связи. Тем не менее, можно прийти к выводу о том, что перечень сведений является открытым, о чем свидетельствует указание в понятии данных абонента на «включает, но не ограничиваясь», а также «любые персональные данные».

Сведения ограниченного доступа в процессе анализа не выявлены.

Говоря о разграничении сведений, составляющих тайну связи, и сведений, составляющих иные категории охраняемой законом информации (ПД, большие пользовательские данные) необходимо отметить, что понятие данных абонента (п.2.1.13 Регламента) фактически свидетельствует о том, что все данные абонента, в том числе, «любая информация, возникающая вследствие использования абонентом телекоммуникационных услуг» являются персональными данными.

Механизмы правовой защиты заключаются в наличии обязанности по сохранению данных абонента, а также уголовной ответственности за ее нарушение. Помимо этого, абонент может подать жалобу провайдеру услуг связи (раздел 15 Регламента).

[100] Consumer Protection Regulations [Electronic resource]: Regulations by Telecommunications Regulatory Authority (TRA) of 10.01.2017 ver.1.3. // Telecommunications Regulatory Authority [Site]. – URL: https://www.tra.gov.ae/assets/8zJXhCkG.pdf.aspx (accessed: 10.08.2018).

Юридическая ответственность за нарушение тайны связи будет наступать по ст.378, 379 Уголовного кодекса ОАЭ[101]. При этом понятие «тайны» является вопросом факта. Применительно к вопросу о понятии «тайна» отсутствуют какие-либо рекомендации судебных органов[102].

Согласно п.2 ст.72 Федерального Постановления-Закона №3 от 2003 г. «Об организации телекоммуникационного сектора»[103] случаи копирования, раскрытия или распространения информации о любых коммуникациях или телефонных сообщений при помощи использования Публичной телекоммуникационной сети при отсутствии права на это любым лицом, будь то сотрудник лицензиата, или связанное с ним лицо, способом, который позволяет прочитать содержимое любой коммуникации, телефонного сообщения или любых других телекоммуникационных услуг, наказываются тюремным заключением на срок, не превышающий 1 год и (или) штрафом в размере от 50 000 до 1 000 000 дирхам.

Хотя Конституция ОАЭ содержит положения, обеспечивающие защиту тайны связи, выявить соотношение конституционных прав не представляется возможным в связи с отсутствием решений суда по данному вопросу.

Порядок и условия передачи сведений, составляющих тайну связи, определены в Регламенте. Согласно ст.13.2 провайдер услуг связи может раскрыть данные абонента, если такое раскрытие:

1) разрешено законом;
2) прямо разрешено абонентом;
3) прямо разрешено положениями Регламента или иными нормативными положениями;
4) осуществляется провайдером услуг связи в ходе проверки кредитоспособности в авторитетном агентстве кредитных историй;
5) осуществляется в целях ответа на законный запрос правоохранительных органов для помощи в расследовании преступных деяний; или
6) осуществляется в целях ответа на законной запрос от любого уполномоченного органа в

[101] Federal Law No. (3) of 1987 Promulgating the Penal Code [Electronic resource] // LEGAL ADVICE MIDDLE EAST [Site]. – URL: https://legaladviceme.com/legislation/117/uae-federal-law-3-of-1987-promulgating-penal-code (accessed: 09.08.2018).

[102] N. O'Connell. Privacy in a UAE Healthcare Context. February 2014 [Electronic resource] // AL TAMIMI & CO. [Site]. – URL: https://www.tamimi.com/law-update-articles/privacy-in-a-uae-healthcare-context/ (accessed: 09.08.2018).

[103] On Organizing The Telecommunications Sector [Electronic resource]: Federal Decree-Law No. 3 of 2003 // Legal Portal of the United Arab Emirates [Site]. – URL: https://elaws.moj.gov.ae/UAE-MOJ_LC-En/00_TELECOMMUNICATIONS/UAE-LC-En_2003-11-15_00003_Markait.html?val=EL1 (accessed: 10.08.2018).

отношении вопросов, связанных с публичными интересами и (или) вопросов государственной безопасности;

7) осуществляется для Регулирующего органа в сфере телекоммуникаций (TRA) в соответствии с настоящим Регламентом.

Например, согласно статье 13.10 Регламента TRA может запросить у любого провайдера услуг связи данные абонента, которые необходимы TRA для осуществления своих обязанностей. Любой такой запрос должен быть выполнен в письменном виде и провайдер, которому адресован такой запрос, обязуется предпринять все необходимые меры для предоставления запрошенных данных абонента.

Провайдер услуг связи обязан получить предварительное согласие абонента до передачи любых его данных своим аффилированным и (или) иным третьим лицам, которые прямо не вовлечены в оказание телекоммуникационных услуг, предоставляемых абоненту (п. 13.5. Регламента).

Если провайдеру услуг связи необходимо передать данные абонента своим аффилированным лицам или иным третьим лицам, которые прямо вовлечены в оказание телекоммуникационных услуг, предоставляемых абоненту, такие третьи лица обязаны предпринимать все необходимые и достаточные меры для защиты конфиденциальности данных абонента и использовать их только в целях предоставления телекоммуникационных услуг (п.13.8 Регламента).

В федеральном законодательстве отсутствуют прямые запреты для трансграничной передачи сведений, составляющих тайну связи[104].

Случаи, условия, порядок передачи сведений, составляющих тайну связи, без согласия субъектов описаны выше.

Изъятия из режима тайны связи в целях обеспечения возможности обработки накопленных данных для достижения социальных, государственных, экономических целей не установлены.

По вопросу о случаях и порядке раскрытия сведений, составляющих тайну связи, в том числе, в форме открытых данных, и принципа раскрытия данных по умолчанию в деятельности органов государственного управления см. Врачебная тайна в ОАЭ. Кроме того, дополним, что согласно п. 14.2.2 Регламента провайдер услуг связи не может

[104] C. Beckett. Big Data: Is the GCC ready? [Electronic resource] // Dentons [Site]. – URL: https://www.dentons.com/en/insights/alerts/2015/april/8/big-data-is-the-gcc-ready (accessed: 10.08.2018).

опубликовывать справочную информацию, относящуюся к физическому лицу без прямого предварительного согласия такого лица. После получения согласия провайдер обязуется обеспечить возможность для абонента отозвать согласие. К справочной информации о физическом лице относится как минимум: имя, город и телефонный номер.

Возможность доступа третьих лиц к тайне связи с согласия субъекта раскрыта выше.

Возможность администрирования согласий субъектов тайны связи на обработку сведений, составляющих тайну связи, и их передачу третьим лицам (в т.ч. наличие права субъекта определять порядок использования таких сведений, делегирования права на выдачу согласий, отзыва согласий на их сбор, обработку и/или передачу и т.д.), а также специальных норм (при их наличии) по идентификации субъектов тайны связи (в т.ч. их законных представителей) в целом не предусмотрена.

В отношении формы, способов получения согласий субъектов тайны связи на обработку сведений, составляющих тайну связи, и / или их передачу третьим лицам, порядка фиксации и хранения подтверждений получений согласий регулирование содержится только в п.13.5 Регламента. Согласно данному пункту провайдер услуг связи должен получить предварительное согласие абонента до распространения любых данных абонента с его аффилированными лицами и (или) иными третьими лицами, не принимающими непосредственного участия в оказании телекоммуникационных услуг, оказываемых абоненту. Согласие может быть предоставлено в момент, когда формируется договор с абонентом при условии, что всегда обеспечивается механизм, посредством которого абонент может отозвать свое согласие (механизм «opt-out») на более позднем этапе, если этого требует абонент.

Права и обязанности специальных категорий лиц в части доступа к сведениям, составляющих тайну связи, а также случаи такого доступа не установлены. Можно отметить лишь обязанность провайдера услуг связи обеспечить, чтобы в договоре между ним и любым аффилированным лицом или иным третьим лицом, которым будут переданы данные абонента, содержалась ответственность таких лиц за обеспечение безопасности и защиты данных абонента.

Согласно ст.13.3. Регламента провайдер услуг связи обязуется предпринять все разумные меры для защиты тайны данных абонента, которую он хранит в своих файлах, будь то электронная или бумажная форма. Провайдер услуг связи обязуется использовать надежные меры безопасности в отношении таких рисков как утрата, несанкционированный

доступ, уничтожение, утечка, использование не по назначению, модификация и (или) несанкционированное раскрытие. В том числе, персонал провайдера услуг связи также должен выполнять требования по защите данных абонента.

Согласно п.13.6. провайдеру услуг связи, который имеет доступ к данным абонента в результате их взаимосвязи с другим провайдером услуг связи, строго запрещено использовать данные абонента для любых иных целей, не относящихся к взаимосвязи. В частности, такие данные не могут быть использованы для маркетинговых целей или анти-конкурентных практик.

С 1 января 2012 года TRA запустило кампанию по информированию и противодействию использования поддельных мобильных телефонов в ОАЭ[105]. Было объявлено, что устройства, использующие фальсифицированные IMEI будут отключены от связи. Был запущен SMS-сервис, посредством которого пользователи могли проверить статус своих устройств. Операторы мобильной связи были обязаны также информировать своих потребителей о статусе мобильных устройств и о том, что при использовании фальсифицированных IMEI пользователи будут отключены от связи.

Законодательство ОАЭ не предусматривает специального права для работодателей по реализации контроля за сведения о соединениях и содержании переговоров и переписки работника по сети связи, осуществляемых при использовании телефонной связи, доступа в интернет для служебных целей. В данном случае применяются общие правила обеспечения тайны связи. Например, такие действия можно осуществлять с согласия. Отметим, что согласно ст.15 Закона о компьютерных преступлениях[106] перехват или вмешательства в любые сообщения, передаваемые через информационную сеть без разрешения и намеренно уголовно наказуемо. Также согласно ст.378 Уголовного кодекса наказание предусмотрено за перехват или разглашение корреспонденции или телефонных разговоров без получения предварительного согласия на это.

Регламент предусматривает обязанность провайдера услуг связи по выполнению мер по охране конфиденциальности данных абонента. Указывается, что должны предприниматься обоснованно необходимые меры (*reasonable*). Согласно ст. 13.11 Регламента TRA может при

[105] TRA Announcement [Electronic resource] // Telecommunications Regulatory Authority [Site]. – URL: http://www.tra.gov.ae/assets/3vyZ23hl.pdf.aspx (accessed: 10.08.2018).

[106] On Combating Cybercrimes [Electronic resource]: Federal Decree-Law No. 5 of 2012 // Legal Portal of the United Arab Emirates [Site]. – URL: https://elaws.moj.gov.ae/UAE-MOJ_LC-En/00_PENALTIES%20AND%20CRIMINAL%20MEASURES/UAE-LC-En_2012-08-13_00005_Markait.html?val=EL1 (accessed: 10.08.2018).

условии заблаговременного уведомления провайдера услуг связи посетить его помещения или его аффилированных лиц, где хранятся данные абонента, для того чтобы TRA мог ознакомиться с предпринимаемыми мерами безопасности. В случае, если TRA не будет удовлетворен уровнем обеспечиваемой безопасности в указанных помещениях, TRA оставляет за собой право проинструктировать провайдера услуг связи или поручить ему проинструктировать своих аффилированных лиц об усилении мер безопасности в конкретном помещении или предложить переместить хранимые данные абонента в более безопасные помещения, которые могут быть рассмотрены в качестве целесообразных и обоснованных.

1.2. Врачебная тайна

Российская Федерация

Понятие и фактический состав сведений, юридическая ответственность за нарушение. Российское законодательство содержит понятие «врачебной тайны», которое по своему характеру идентично медицинской тайне. Самое общее понятие определено в Законе об охране здоровья граждан. Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении (ст. 13 Закона об основах охраны здоровья граждан).

Можно выделить следующие принципы формирования сведений, составляющих медицинскую тайну: открытый перечень; сведения, раскрытие которых может нарушить тайну личной жизни пациента и причинить ему моральный вред и/или материальный ущерб.

Законодательство довольно широко определяет врачебную тайну и содержит те виды сведений, которые к ней относятся. Следующие сведения составляют врачебную тайну:

(1) Сведения о факте обращения за медицинской помощью;

(2) Информация о состоянии здоровья пациента и диагнозе;

(3) Иные сведения, полученные при медицинском обследовании и лечении (ст. 13 Закона об основах охраны здоровья граждан).

Стоит отметить, что указанные выше сведения охраняются и в отношении умерших лиц (см. Определение КС РФ от 9 июня 2015 г. N 1275-О).

Частные виды врачебной тайны приводятся и в иных законах. Например,

Федеральный закон от 22.12.1992 г. № 4180-1 «О трансплантации органов и (или) тканей человека» к врачебной тайне относит информацию о доноре и реципиенте при трансплантации органов и (или) тканей человека.

Вопрос о составе сведений, включающих медицинскую тайну, редко является предметом спора и судебного рассмотрения (в отличие, например, от тайны связи). Вместе с тем, можно упомянуть следующие примеры.

К врачебной тайне были отнесены: информация об уклонении водителей от профилактического наблюдения, а также о наличии у них симптомов заболевания, препятствующего управлению транспортными средствами (см. Определение Верховного Суда РФ от 27.11.2013 N 57-АПГ13-7), сведения, отраженные в журнале дежурств медицинского учреждения, напротив не были отнесены к врачебной тайне (Постановление Президиума суда Ханты-Мансийского автономного округа – Югры от 22.02.2013 №44Г-7/2013); Сведения о состоянии здоровья, одновременно составляют врачебную тайну и относятся к специальным категориям персональных данных (ст. 10 Закона о персональных данных). Отдельные сведения могут быть отнесены к биометрическим персональным данным (ст. 11 Закона о персональных данных). Таким образом, сведения, составляющие врачебную тайну (за исключением сведений о факте обращения), относятся к персональным данным специальных видов, для которых предусмотрены повышенные требования правовой защиты.

Сведения, составляющие врачебную тайну, одновременно являются частным случаем тайны личной жизни и могут относиться к служебной тайне.

Поскольку информация о состоянии здоровья прямо отнесена к персональным данным, то пациент имеет права субъекта персональных данных, включая право на доступ, право требования уточнения, блокирования и уничтожения персональных данных, право на обжалование действий/бездействий оператора (ст.ст.14, 17, 21 Закона о персональных данных). Возможность ограничения права на медицинскую тайну есть только на основании федерального закона (ст. 55 Конституции).

За нарушение врачебной тайны предусмотрены следующие виды ответственности:

(1) Уголовная ответственность в виде штрафа до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо принудительными работами на срок до четырех лет с лишением права занимать определенные

должности или заниматься определенной деятельностью на срок до пяти лет или без такового, либо арестом на срок до шести месяцев, либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет (ст. 137 УК РФ).

(2) Административная ответственность в соответствии со ст.13.11 КоАП (нарушение законодательства об обработке персональных данных), ст. 13.14 КоАП (за разглашение сведений конфиденциального характера лицом, получившим доступ к таким сведениям с использованием служебного положения). Отдельный состав именно за нарушение врачебной тайны КоАП не предусмотрен.

(3) Гражданско-правовая ответственность на основании исков о компенсации морального вреда, возмещения убытков, причинении вреда.

Отдельно отметим, что фактический состав сведений, которые составляют врачебную тайну, является довольно определенным. Судебная практика по указанному вопросу немногочисленна.

Предоставление третьим лицам. Основанием предоставления сведений, составляющих медицинскую тайну, третьим лицам является письменное согласие пациента. Никакие иные формы согласия Законодательством не предусмотрены (ст. 13 Закона об основах охраны здоровья). При этом разглашение сведений, составляющих медицинскую тайну, физическим лицам и должностным лицам допускается в любых целях, том числе в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе. Предоставление сведений аффилированным лицам, которые являются медицинскими организациями, допускается без согласия пациента, если такое предоставление осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг (следует из системного толкования ст. 13 Закона об основах охраны здоровья и ст. 10 Закона о персональных данных). Что касается предоставления сведений коммерческим организациям, деятельность которых не связана с оказанием медицинских услуг, такое предоставление возможно только для достижения той цели, ради которой осуществляется сбор и обработка персональных данных (ст. 10 Закона о персональных данных). Исчерпывающий перечь случаев предоставления сведений, составляющих врачебную тайну, без согласия пациента, определен федеральными законами (ст. 10 Закона о персональных данных, ст. 13 Закона об основах охраны здоровья).

Правила трансграничной передачи сведений, составляющих медицинскую тайну, регулируются Законом о персональных данных.

Перечень оснований, когда допускается предоставление третьим лицам сведений, составляющих врачебную тайну, без согласия субъекта тайны исчерпывающим образом определен в Законодательстве. Сведения, составляющие врачебную тайну, имеют двойственный статус: с одной стороны, охраняются как врачебная тайна, с другой, как – специальные категории персональных данных. В этой связи два закона предусматривают случаи и порядок предоставления третьим лицам соответствующих сведений без согласия субъекта тайны.

Из системного толкования положений Законодательства следует, что случаи предоставления третьим лицам без согласия, которые установлены Законом об основах охраны здоровья, распространяются исключительно на лиц, которые могут быть связаны врачебной тайной. К таким лицам, главным образом, относятся медицинские учреждения, в которых проходило лечение пациента, врачи, иной медицинский персонал и иные работники медицинских учреждений, студенты, обучающиеся по таким специальностям. Закон об основах охраны граждан предусматривает следующие случаи предоставления третьим лицам без согласия пациентов:

- В целях проведения медицинского обследования и лечения гражданина, который не способен выразить свою волю;
- При угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
- По запросу правоохранительных органов, перечисленных в законе;
- В случае оказания медицинской помощи несовершеннолетнему, не достигшему определенного возраста, предусмотренного в Законе;
- При обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;
- В целях осуществления учета и контроля в системе обязательного социального страхования;
- В целях осуществления контроля качества и безопасности медицинской деятельности;

- В некоторых иных специальных случаях, которые предусмотрены в Законе об основах охраны здоровья граждан.

Те случаи предоставления без согласия, которые предусмотрены Законом о персональных данных, имеют более широкое распространение. Они применяются к любым операторам, которые на законной основе обрабатывают сведения о состоянии здоровья. К таким случаям, в том числе, относятся: обработка общедоступных данных, обработка в соответствии с международными договорами и т.д. (ст. 10 Закона о персональных данных).

Если сведения, обрабатываемые государственными органами, отнесены к тому или иному охраняемому виду тайны, то доступ к таким сведениям ограничивается, как предусмотрено законами, регулирующими соответствующий вид тайны (ст. 5 Закона о доступе к информации государственных органов).

Закон об основах охраны здоровья граждан не предусматривает основания и порядок опубликования, сведений составляющих врачебную тайну, в качестве открытых данных. Соответственно, законодательство не позволяет публиковать такие сведения в форме открытых данных государственных органов.

Исходя из буквального толкования Закона об основах охраны здоровья, с согласия пациента сведения, составляющие его врачебную тайну, могут предоставляться другим гражданам и должностным лицам в любых целях. Как указано выше, положения и изъятия, предусмотренные Законом об основах охраны здоровья граждан, напрямую распространяются на тех лиц, для которых врачебная тайна является профессиональной тайной. Что касается иных субъектов, то применение к ним данных положений является спорным. Вместе с тем, с согласия субъектов тайны, их персональные данные могут быть предоставлены третьим лицам (ст.ст. 9, 10 Закона о персональных данных). При этом использование, в том числе предоставление персональных данных третьим лицам, всегда ограничено целями обработки. То есть предоставление специальных категорий всегда должно осуществляться в рамках заявленной цели сбора соответствующих персональных данных (ст.5 Закона о персональных данных).

Обзор требований информационной безопасности, предусмотренные для медицинских организаций. Поскольку сведения о состоянии здоровья относятся к категории специальных персональных данных, то требования к защите информационных систем, в которых обрабатываются такие данные, являются повышенными (см. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных

данных при их обработке в информационных системах персональных данных»). Дополнительно стоит отметить, что с введением в 2017 г. системы Единой государственной информационной системе в сфере здравоохранения («ЕГИСЗ») появились дополнительные требования в части обеспечения безопасности информации, которая содержится в ЕГИСЗ. Например, следующие НПА содержат соответствующие требования:

- Постановление Правительства РФ от 05.05.2018 № 555 «О единой государственной информационной системе в сфере здравоохранения».
- Приказ Минздравсоцразвития России от 25.01.2011 № 29н «Об утверждении Порядка ведения персонифицированного учета в сфере обязательного медицинского страхования».

Заслуживает внимания репрезентативная ***судебная практика Российской Федерации и ЕСПЧ*** по вопросам обработки и защиты информации, составляющей соответствующие виды тайн. В частности, можно отметить следующие судебные решения.

Постановление ЕСПЧ по делу «Авилкина и другие (avilkina and others) против Российской Федерации» от 6 июня 2013 г. Лечебные учреждения передали прокуратуре некоторые сведения о своих пациентах без их согласия. Те обратились в ЕСПЧ, ссылаясь на то, что запрошенные сведения составляли врачебную тайну и на них должны распространяться гарантии защиты, предусмотренные статьей 8 Европейской конвенции.

Заявители (пациенты) утверждали: интерес прокуратуры к данным сведениям был вызван их религиозной принадлежностью. Заявители являлись последователями учений, исповедуемых и распространяемых Свидетелями Иеговы, а те, как известно, в силу религиозных убеждений зачастую отказываются от переливания крови.

По мнению заявителей, религиозная принадлежность не должна быть основанием для ограничения прав. Кроме того, право на уважение частной жизни, гарантированное Европейской конвенцией, распространяется и на последователей религии[107].

ЕСПЧ нашел жалобу справедливой по следующим основаниям:

(1) Нет сомнений в том, что передача государственными больницами медицинских документов заявительниц прокуратуре представляла собой вмешательство в их право на уважение личной жизни, гарантированное пунктом 1 статьи 8 Конвенции.

[107] Султанов А.Р. Комментарий к Постановлению Европейского суда по правам человека по делу «Авилкина и другие против Российской Федерации» // Международное правосудие. – 2013. – № 3. – С. 25-30.

(2) Европейский Суд учитывает, что прокурор мог использовать другие возможности, помимо требования о раскрытии информации, составляющей врачебную тайну, при рассмотрении полученных жалоб. В частности, он мог попытаться получить согласие заявительниц на раскрытие и/или допросить их по данному вопросу (см. §§ 23 - 24 Постановления). Тем не менее, прокурор предпочел потребовать раскрытия информации, составляющей врачебную тайну, не уведомив заявительниц и не предоставив им возможности возражать или согласиться.

(3) По мнению Европейского Суда, возможность возражения против раскрытия информации, составляющей врачебную тайну, когда она уже находилась в распоряжении прокурора, не обеспечивала заявительницам достаточной защиты против несанкционированного раскрытия.

Определение КС РФ от 9 июня 2015 г. № 1275-О. Гражданин Зубков В.Н. обратился в КС РФ, считая неконституционными положения Закона об основах охраны здоровья, не позволяющие ему получить доступ к истории болезни его умершей жены.

КС РФ не согласился с позицией Зубкова В.Н., указав, что: «Медицинская информация, непосредственно касающаяся не самого гражданина, а его умерших близких (родственника, супруга и т.д.), как связанная с памятью о дорогих ему людях, может представлять для него не меньшую важность, чем сведения о нем самом. В то же время подобная информация является конфиденциальной и составляет медицинскую тайну не только при жизни лица, но и после его смерти. … введение законодателем ограничений на предоставление медицинских сведений в отношении умершего гражданина третьим лицам само по себе отвечает этим конституционным положениям».

Определение Верховного Суда РФ от 27.11.2013 № 57-АПГ13-7. ВС РФ признал недействующим Закон Белгородской области, устанавливающий дополнительные правила освидетельствования водителей, в том числе в связи с тем, что его положения расширяли круг изъятий, предусмотренных Законом об основах охраны здоровья. В частности, в соответствии с названным законом предполагалось установление обязанности медицинских учреждений направлять информацию об уклонении водителей от профилактического наблюдения, а также о наличии у них симптомов заболевания, препятствующего управлению транспортными средствами, в органы прокуратуры и иным должностным лицам, уполномоченным инициировать дела о прекращении действия права на управление транспортными средствами, а в отношении лиц, лишенных права на управление

транспортными средствами, - также в орган, исполняющий постановление о лишении права управления транспортными средствами.

Обзор судебной практики Верховного Суда РФ от 01.03.2006 «Обзор судебной практики Верховного Суда Российской Федерации за четвертый квартал 2005 года». В данном обзоре ВС РФ подтвердил позицию о том, что адвокат не имеет права на получение сведений составляющих врачебную тайну, т.к. ст. 13 Закона об основах охраны здоровья не предусматривает этого.

Постановление Президиума суда Ханты-Мансийского автономного округа - Югры от 22.02.2013 № 44Г-7/2013. Работница, уволенная за разглашение сведений, которые содержались в медицинском журнале, требовала восстановления на работе. Требование удовлетворено в части восстановления на работе, поскольку в трудовом договоре и должностной инструкции истицы не определен конкретный перечень сведений, которые могут быть отнесены к врачебной тайне, сведения, отраженные в журнале дежурств, не относятся к врачебной тайне, так как не позволяют идентифицировать пациента.

Европейский союз

Публичные источники определяют врачебную тайну как медицинское, правовое, социально-этическое понятие, представляющее собой запрет медицинскому работнику сообщать третьим лицам информацию о состоянии здоровья пациента, диагнозе, результатах обследования, самом факте обращения за медицинской помощью и сведений о личной жизни, полученных при обследовании и лечении[108]. Среди ключевых составляющих принципов врачебной тайны называют следующие:

1. «Индивиду принадлежит право на неприкосновенность личной жизни и конфиденциальность данных о его здоровье;

2. Индивиду принадлежит право контролировать доступ к данным о его здоровье и разрешать раскрытие таких данных только с его согласия;

3. В каждом случае раскрытия конфиденциальных данных о здоровье специалисты сферы здравоохранения должны оценивать необходимость и пропорциональность такого

[108] Врачебная тайна [Электронный ресурс] // Википедия — свободная энциклопедия [Сайт]. – URL: https://ru.wikipedia.org/wiki/%D0%92%D1%80%D0%B0%D1%87%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F_%D1%82%D0%B0%D0%B9%D0%BD%D0%B0 (дата обращения: 30.07.2018).

раскрытия, а также сопутствующие риски»[109].

Можно сказать, что термин врачебная тайна, по сути, охватывает собой право на неприкосновенность частной жизни (*privacy*), право на конфиденциальность медицинских данных (*medical confidentiality*) и защиту персональных данных (*personal data protection*)[110]. В правовом поле эти три составляющие чаще всего не существуют раздельно, а образуют некий единый набор правил разного уровня, призванный гарантировать права лица в отношении информации о его здоровье. Чаще всего право на неприкосновенность частной жизни и охрану сведений о здоровье представляют собой высокоуровневые принципы, закреплённые на уровне международных соглашений и конституций отдельных государств, тогда как практическая реализация этих принципов находит свое выражение в установлении специального режима обработки персональных данных, связанных со здоровьем. Далее обратимся к положениям международных документов.

Следует отметить, что врачебная тайна известна еще со времен появления клятвы Гиппократа[111]. Одним из первых документов о правах пациентов, закрепляющих право на конфиденциальность стал принятый в 1972 г. Билль Американской Ассоциацией Больниц[112]. Затем право на конфиденциальность информация относительно состояния здоровья пациента, диагноза, прогноза и лечения, а также любой иной информации личного характера даже после смерти пациента было закреплено в Лиссабонской декларация о правах пациента[113]. В документе также указано, что разглашение допускается, только если пациент даст прямое согласие, или если это прямо предусмотрено законом. Информация может сообщаться

---

[109] H. Helmchen, N. Sartorius. Ethics in Psychiatry: European Contributions. [Electronic resource] // Google books library [Site]. – URL: https://books.google.ru/books?id=70h31egRm40C&pg=PA162&lpg=PA162&dq=European+Standards+on+Confidentiality+and+Privacy+in+Healthcare&source=bl&ots=dIJEFObHan&sig=slG8SHy6Sl9lE8mxviEDVDaJhxA&hl=ru&sa=X&ved=2ahUKEwiC1NLi48PcAhWixKYKHbeVAsAQ6AEwDHoECAcQAQ#v=onepage&q=European%20Standards%20on%20Confidentiality%20and%20Privacy%20in%20Healthcare&f=false (accessed: 30.07.2018).

[110] B. M. Knoppers. Protecting Data Privacy in Health Services Research [Electronic resource]: Institute of Medicine (US) Committee on the Role of Institutional Review Boards in Health. Services Research Data Privacy Protection. Washington (DC): National Academies Press (US). – 2000 // The National Center for Biotechnology Information [Site]. – URL: https://www.ncbi.nlm.nih.gov/books/NBK222816/ (accessed: 30.07.2018).

[111] Кля́тва Гиппокра́та — врачебная клятва, выражающая основополагающие морально-этические принципы поведения врача [Электронный ресурс] // Википедия — свободная энциклопедия [Сайт]. – URL: https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8F%D1%82%D0%B2%D0%B0_%D0%93%D0%B8%D0%BF%D0%BF%D0%BE%D0%BA%D1%80%D0%B0%D1%82%D0%B0 (дата обращения: 30.07.2018).

[112] American Hospital Association. Statement on a patient's bill of rights [Electronic resource] // Illinois Institute of Technology [Site]. – URL: http://ethics.iit.edu/codes/AHA%201972.pdf (accessed: 30.07.2018).

[113] Лиссабонская декларация о правах пациента – принята 34-й Всемирной Медицинской Ассамблеей. Лиссабон, Португалия, сентябрь–октябрь 1981 года [Электронный ресурс] // Медицина и право [Сайт]. – URL: http://www.med-pravo.ru/Ethics/LisbonDecl.htm (дата обращения: 30.07.2018).

другим учреждениям здравоохранения исключительно по мере необходимости, если пациент не дал прямого согласия.

Обязательства по конфиденциальности содержатся в Международном кодексе медицинской этики 1983 г.[114]. Раздел 4 Декларации о политике в области обеспечения прав пациента в Европе 1994 г.[115] закрепляет, что вся информация, относящаяся к здоровью пациента, медицинскому состоянию, диагнозу, прогнозу и лечению, а также любая другая личная информация должна быть сохранена в тайне, даже после смерти лица. Конфиденциальная информация может быть раскрыта только с прямо выраженного согласия лица, такое согласие презюмируется в случае предоставления данных сотрудникам здравоохранения в ходе лечения. Любые данные, идентифицирующие пациента, должны охраняться. В соответствии с Конвенцией о правах человека и биомедицине 1997 г., каждый человек имеет право на уважение своей частной жизни, в том числе и тогда, когда это касается сведений о его здоровье[116]. Наконец, право на конфиденциальность обозначено в составе четырнадцати прав пациента в Европейской хартии прав пациентов 2002 г.[117]

Статья 6 Конвенции 108 относит данные, касающиеся здоровья, к специальной категории данных. В соответствии со специальными рекомендациями, выработанными Рабочей группой Совета Европы для регулирования обработки данных в медицинском секторе[118], медицинские данные (*medical data*) определяются как персональные данные лица, относящиеся к его здоровью или связанные с ним. Генетические данные (*genetic data*) включают в себя данные любого рода, касающиеся наследственных характеристик лица или порядком наследования таких характеристик в группе родственных индивидов. Требования, предъявляемые к охране медицинских данных, устанавливают, что при сборе и обработке

---

[114] Международный кодекс медицинской этики [Электронный ресурс] // Медицинский сайт MedLinks.ru [Сайт]. – URL: http://www.medlinks.ru/article.php?sid=1630 (дата обращения: 30.07.2018).

[115] Declaration on the promotion of patients' rights in Europe – European consultation on the rights of patients Amsterdam 28 – 30 march 1994 – [Electronic resource] // World Health Organization [Site]. – URL: http://www.who.int/genomics/public/eu_declaration1994.pdf (accessed: 30.07.2018).

[116] Конвенция о защите прав человека и человеческого достоинства в связи с применением достижений биологии и медицины: Конвенция о правах человека и биомедицине [Электронный ресурс]: заключена в г. Овьедо 04.04.1997 (с изм. от 27.11.2008) – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 30.07.2018).

[117] European charter of patients' rights – Rome, November 2002 – [Electronic resource] // European Commission [Site]. – URL: http://ec.europa.eu/health/ph_overview/co_operation/mobility/docs/health_services_co108_en.pdf (accessed: 30.07.2018).

[118] On the Protection of Medical Data [Electronic resource]: Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 adopted February 13, 1997 // University of Minnesota. Human Rights Library [Site]. – URL: http://hrlibrary.umn.edu/instree/coerecr97-5.html (accessed: 30.07.2018).

медицинских данных должно быть гарантировано основополагающее право на неприкосновенность частной жизни. Сбор и обработка таких данных должны осуществляться только при условии закрепления в местном законодательстве защитных мер. В частности, сбор и обработка допускаются только работниками сферы здравоохранения, связанными обязательством по сохранению конфиденциальности данных.

В целях установления правил для облегчения доступа к безопасному и высококачественному трансграничному медицинскому обслуживанию в рамках ЕС и обеспечения мобильности пациентов в 2011 году была принята директива ЕС «О правах пациентов в трансграничном медицинском обслуживании» (далее - «Директива 2011/24/ЕС»)[119]. Обеспечение непрерывности трансграничного медицинского обслуживания зависит от передачи персональных данных, содержащих информацию о здоровье пациента. Соответственно, возможность для передачи таких персональных данных из одного государства-члена ЕС в другое должна существовать одновременно с обеспечением соблюдения основных прав человека. «Трансграничное медицинское обслуживание должно осуществляться в соответствии с фундаментальным правом на неприкосновенность частной жизни в связи с обработкой персональных данных и должно быть защищено посредством национальных мер, GDPR и Директивой»[120]. Обмен медицинскими данными и информацией осуществляется с помощью Информационной системы внутреннего рынка ЕС (IMI).

Вопросы трансграничной передачи данных о здоровье лица, их доступность для пациента с территории любого из государств-участников ЕС при одновременном соблюдении высоких требований к конфиденциальности данных, учитывая их особый характер, имеют приоритетное значение на сегодняшний день. В своем Сообщении от 25 апреля 2018[121] Европейская Комиссия указывает на большую роль цифровых решений для здравоохранения, в том числе для обеспечения непрерывности лечения вне зависимости от места нахождения лица и для целей предотвращения заболеваемости. Также отмечается ключевое значение данных для развития цифровизации в данной сфере. Данные о здоровье могут существовать в

[119] О правах пациентов в трансграничном медицинском обслуживании [Электронный ресурс]: регламент Европейского парламента и Совета Европейского Союза. – № 2011/24/ЕС – 09.03.2011 – Доступ из справ.-правовой системы «Консультант Плюс». (дата обращения: 30.07.2018).

[120] О правах пациентов в трансграничном медицинском обслуживании / Там же.

[121] On enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society [Electronic resource]: Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – April 25, 2018. // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0233&from=EN (accessed: 30.07.2018).

различной форме, при этом управление данными в разных странах ЕС различается. Довольно часто данные могут быть недоступны, как для пациента, так и для органов власти, медицинского персонала и исследовательских центров, а используемые электронные системы являются несовместимыми. ЕС поддерживает использование высокопроизводительных вычислительных систем, информационной аналитики и искусственного интеллекта в целях разработки новых медицинских сервисов, позволяющих быстрее и точнее ставить диагноз и назначать лечение. Но использование таких технологий напрямую зависит от доступности значительного объема данных и соответствующего правового регулирования, которые позволят защитить права граждан и одновременно стимулировать инновации. На сегодняшний день использование технологий в здравоохранении все еще осуществляется довольно медленно, а потому Комиссия намерена ускорить данный процесс. Ранее уже были обозначены такие направления, как обеспечение доступа граждан к данным и их трансграничная передача, улучшения качества данных для целей исследований, предотвращении заболеваемости и персонализированного здравоохранения, обеспечение граждан техническими устройствами для реализации своих прав. Комиссия в дальнейшем намерена предпринять действия по:

1. стандартизации электронных медицинских систем в различных государствах ЕС с целью их функциональной совместимости;

2. развитию инфраструктуры eHealth Digital Service в целях расширения круга сервисов и услуг для граждан;

3. стимулированию финансирования в данной сфере;

4. установлению механизма для добровольного сотрудничества органов власти и иных участников в целях обмена данными для проведения исследований в сфере превентивной и персонализированной медицины;

5. развитию условий для безопасного обмена и трансграничной передачи геномной и иной информации на внутреннем рынке для целей исследований;

6. запуску пилотных проектов по указанным направлениям.

Приоритетным также является обмен инновационными практиками, развитием и укреплением потенциала и технической поддержка компетентных органов власти, а также распространение информации среди медицинских специалистов и пациентов.

В соответствии с GDPR под данными в отношении здоровья понимаются «персональные данные, касающиеся физического или психического здоровья физического

лица, в том числе предоставление медицинских услуг, которые раскрывают информацию о состоянии его/ее здоровья»[122]; под генетическими данными понимаются «персональные данные, касающиеся унаследованных или приобретенных генетических характеристик физического лица, которые предоставляют уникальную информацию о физиологии или здоровье указанного физического лица и которые являются результатом, в частности, анализа биологического образца соответствующего физического лица <…> Связанные со здоровьем персональные данные должны включать в себя все данные, которые относятся к состоянию здоровья субъекта данных и раскрывают информацию о прошлом, текущем и будущем физическом или психологическом состоянии здоровья субъекта данных. Сюда относится информация о физическом лице, собранная в ходе регистрации или предоставления медицинских услуг указанному физическому лицу; номер, символ или знак, присвоенные физическому лицу для однозначной идентификации лица; информация, полученная в результате исследования или обследования части тела или телесного материала, включая генетические данные и биологические образцы; а также любая информация, например, о заболевании, инвалидности, риске заболевания, медицинском анамнезе, клиническом лечении или о физиологическом или медико-биологическом состоянии субъекта данных, независимо от источника данных, например, они могут быть получены от врача или другого медицинского работника, больницы, медицинского оборудования или в результате диагностики в лабораторных условиях»[123].

GDPR закрепляет общий запрет на обработку генетических данных и данных касающихся здоровья. Обработка разрешается только в прямо предусмотренных случаях (ст. 9 GDPR), а именно:

1. с согласия лица на обработку;

2. в целях исполнения обязательств в сфере трудового законодательства и социального обеспечения;

3. обработка необходима для защиты жизненно важных интересов субъекта данных или другого физического лица;

4. обработка осуществляется фондом, объединением или некоммерческой

[122] 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) – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 30.07.2018).

[123] 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) / Там же.

организацией в рамках их законной деятельности в политических, философских, религиозных или профсоюзных целях;

5. обработка относится к персональным данным, которые субъект данных очевидным образом сделал общедоступными;

6. обработка необходима для предъявления, исполнения или защиты судебных исков;

7. обработка необходима по причинам особого общественного интереса на основании законодательства ЕС или государства-члена ЕС, которое должно быть пропорционально преследуемой цели, должно соответствовать сущности права на защиту данных и предусматривать приемлемые и конкретные меры для защиты основных прав и интересов субъекта данных;

8. обработка необходима в целях превентивной или профессиональной медицины, для оценки трудоспособности работника, для диагностики состояния здоровья, предоставления медицинской или социальной помощи, лечения или для обслуживания в сфере здравоохранения и социального обеспечения на основании законодательства или по договору с сотрудником сферы здравоохранения. Такая обработка должна осуществляться только лицом, которое обязано соблюдать профессиональную тайну;

9. обработка необходима в целях общественного интереса в области здравоохранения, например, защиты от серьезных трансграничных угроз здоровью или для обеспечения высоких стандартов качества и надежности медицинского обслуживания и лекарственных средств или медицинской техники;

10. обработка необходима для целей архивирования информации в государственных интересах.

В преамбуле GDPR дополнительно поясняется, что такие особые категории персональных данных, которые требуют более высокого уровня защиты, должны обрабатываться в целях, связанных со здоровьем, только если это необходимо для достижения целей в интересах физических лиц или общества в целом. В частности, использование данных, касающихся здоровья, не должно приводить к тому, что такие персональные данные станут доступны третьи лицам, например, страховым компаниям и банкам, и будут обрабатываться в других целях.

Передача данных третьим лицам является способом обработки, а потому допускается только в установленных выше случаях. Статья 20 GDPR также закрепляет право лица на переносимость данных, которое означает, что субъект данных вправе передать свои данные

другому лицу (контролеру) беспрепятственно со стороны контролера, которому первоначально были предоставлены персональные данные при условии, что обработка осуществляется на основании согласия лица и с использованием автоматизированных средств обработки.

GDPR устанавливает специальные правила в отношении трансграничной передачи данных. В частности, проводится разграничение между странами, которые обеспечивают адекватный уровень защиты персональных данных, и теми, которые не обеспечивают. Если страна или международная организация обеспечивает необходимый уровень защиты, тогда передача персональных данных в эти страны разрешена и не требует предварительного одобрения со стороны надзорного органа ЕС. Во все остальные страны передавать данные разрешается только в том случае, если организации, получающие эти данные, обеспечивают достаточные гарантии защиты данных, такие как: наличие юридически обязывающего и подлежащего исполнению документа между государственными органами соответствующих стран, обязательные корпоративные правила, утвержденные компетентным надзорным органом, положения о стандартной защите данных и т.д. Отступление от указанных правил допускается в случаях, когда:

1. субъект данных был проинформирован о возможных рисках и дал прямое согласие на соответствующую передачу;
2. передача необходима для выполнения договора или преддоговорных обязательств между субъектом данных и лицом, которому они передаются;
3. передача необходима для заключения договора или исполнения договора, заключенного в интересах субъекта данных между контролером и другим лицом;
4. передача необходима в целях общественного интереса;
5. передача необходима в целях подачи судебного иска или обеспечения производства по нему;
6. передача необходима для защиты жизненно важных интересов субъекта данных или других лиц, при этом субъект данных лишен возможности самостоятельно дать свое согласие;
7. передача осуществляется из реестра, целью которого является предоставление информации общественности и который открыт для ознакомления широкой общественности или любому лицу.

Под согласием субъекта данных понимается любое «свободно данное, конкретное,

содержательное и определенное указание о своей воле, посредством которого субъект персональных данных оповещает о своем согласии на обработку относящихся к нему персональных данных, например, посредством письменного заявления, в том числе поданного электронным способом, или устного заявления. Сюда может относиться простановка галочки/крестика при посещении интернет-сайта, выбор технических настроек для услуг информационного общества или иное заявление или способ поведения, который четко указывает на то, что субъект данных в указанном контексте согласен на запланированную обработку своих персональных данных. Молчание, уже проставленная галочка/крестик или бездействие лица не являются согласием. Согласие должно охватывать всю обработку, осуществляемую для той же самой цели или целей. Если обработка служит нескольким целям, согласие должно быть дано для каждой из них» .

Применительно к сфере медицины важно отметить особенности, предусмотренные в отношении обработки персональных данных в целях научных исследований или в статистических целях, допускаемой без получения согласия лица. В частности, например, последующая обработка данных, осуществляемая в интересах общества, в целях проведения научного исследования или осуществления статистического учета не должна рассматриваться в качестве несовместимой с первоначальными целями обработки, на которые было получено согласие субъекта. В этом случае также допускается хранить персональные данные в течение более длительного срока. Права субъекта данных также ограничиваются при обработке, осуществляемой в целях проведения научных исследований, например, субъект данных не может заявить возражение против такой обработки, когда это необходимо в интересах общества, и не может потребовать удалить свои данные, если это может сделать невозможным или негативно отразится на достижении целей обработки. Одновременно на такую обработку должны распространяться соответствующие гарантии, обеспечивающие наличие определенных технических и организационных мер, в частности, для соблюдения принципа минимизации данных, включая псевдонимизацию. При этом при определении того, что является научным исследованием для целей обработки необходимо исходить из наиболее широкой трактовки, включая сюда, например, развитие технологий, фундаментальные исследования, прикладные исследования и исследования, финансируемые за счет частных средств.

Допускается раскрытие данных контроллером в соответствии с решением государственного суда, третейского или административного органа третьей страны, в случае

если оно основано на действующем международном соглашении, например, на договоре о взаимной юридической помощи.

Применительно к обработке данных работников, GDPR предоставляет государствам-членам ЕС предусмотреть более специфичные правила для того, чтобы гарантировать защиту прав и свобод в отношении обработки персональных данных работников при выполнении должностных обязанностей, в частности, в целях приема на работу, выполнения трудового договора, управления, планирования и организации работы, равноправия и многообразия на рабочем месте, охраны труда и производственной безопасности и т.д.

В части субъектов обработки GDPR оперирует терминами «контролер» и «обрабатывающее данные лицо», под которым понимается лицо, обрабатывающее персональные данные от имени контролера. На контроллера возлагается обязанность работать только с теми обрабатывающими данные лицами, которые гарантируют наличие технических и организационных мер и соответствие обработки требованиям GDPR. В свою очередь лицо, обрабатывающее данные, не вправе без предварительного письменного разрешения контролера привлекать к работе другое лицо, обрабатывающее данные.

Лицо, обрабатывающее данные, должно действовать на основании договора, в котором будут определены тип персональных данных и категории субъектов данных, предмет, продолжительность, характер и цель обработки, а также обязанности и права контролера. Указанный договор должен в частности предусматривать, что обрабатывающее данные лицо:

1. осуществляет обработку персональных данных только на основании документально подтвержденного поручения контролера, за исключением случаеев, установленных законодательством ЕС;
2. гарантирует, что лица, уполномоченные на обработку персональных данных, приняли обязательства по соблюдению конфиденциальности;
3. принимает необходимые технические и организационные меры;
4. соблюдает условия, установленные для привлечения к работе иного лица, обрабатывающего данные;
5. помогает контролеру в исполнении его обязательств по реагированию на требования субъектов данных;
6. удаляет или восстанавливает персональные данные по выбору контролера, и удаляет существующие копии, кроме случаев, когда законодательством установлено

требование по обязательному хранению данных;

7. направляет контролеру всю информацию, подтверждающую соблюдение установленных требований и обязанностей.

Если лицо, обрабатывающее данные, привлекает к работе другое лицо, в таком случае на такое привлеченное лицо возлагаются такие же обязанности по защите данных при обработке. Если такое привлеченное лицо не выполняет указанные обязательства по защите данных, в таком случае первое лицо, привлекшее второе для обработки данных, несет ответственность перед контролером за выполнение обязанностей привлеченного им лица.

«Контролер и обрабатывающее данные лицо должны имплементировать соответствующие технические и организационные меры, чтобы гарантировать соразмерный риску уровень безопасности, включая inter alia следующее:

- псевдонимизацию и криптографическую защиту персональных данных;
- способность гарантировать постоянную конфиденциальность, целостность, доступность и устойчивость систем и услуг, связанных с обработкой;
- способность своевременно восстанавливать доступность и доступ к персональным данным в случае возникновения инцидента физического или технического свойства;
- процедуру регулярной проверки и оценки эффективности технических и организационных мер для обеспечения безопасности обработки» .

Каждому пользователю предоставляются меры защиты, предусмотренные в ст. 77 (право на подачу жалобы в надзорный орган), 78 (право подать жалобу на надзорный орган) и 79 (право на эффективное средство судебной защиты) GDPR. Ответственность за нарушение требований конфиденциальности данных включает в себя административные штрафы в размере не более 20 000 000 Евро или в случае компании, в размере не более 4% от общего годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше.

Отдельное внимание следует уделить ***судебной практике***, а в качестве репрезентативных дел допустимо привести следующие.

Дело Бодил Линдквист (Bodil Lindqvist) от 6 ноября 2003 г., N C-101/01 (2003)[124]. В

[124] Directive 95/46/EC - Scope - Publication of personal data on the internet - Place of publication - Definition of transfer of personal data to third countries - Freedom of expression - Compatibility with Directive 95/46 of greater protection for personal data under the national legislation of a Member State [Electronic resource]: Judgment of the court dated November 03, 2003 (Cases C-101/01) // The Court of Justice of The European Union [Site]. – URL:

решении по делу Суд ЕС указал, что в понятие данных, которые относятся к состоянию здоровья субъекта, должен включается максимально широкий перечень сведений, включающих данные о физическом и психическом состоянии лица. Соответственно, к таким данным также относится и информация о том, что лицо травмировало ногу и находится на больничном. В этом деле Суд также указал, что распространение физическим лицом персональных данных третьих лиц в сети Интернет не подпадает под действие исключения об обработке данных для личных нужд, поскольку такие данные становятся доступными неопределенному кругу лиц.

Дело Икс против Комиссии европейских сообществ (X v Commission of the European Communities) от 5 октября 1994 N Case C-404/92 P[125]

В данном деле Суд ЕС пришел к следующим выводам. Право на уважение личной и семейной жизни человека, закрепленное в статье 8 Европейской конвенции о защите прав человека и основных свобод, является одним из основополагающих прав, охраняемых в ЕС. Данное право включает в себя право на сохранение конфиденциальности сведений о состоянии здоровья. Ограничения могут быть установлены только в целях защиты общественно интереса и должны быть пропорциональными. Медицинское освидетельствование, осуществляемое до заключения трудового договора с кандидатом на должность служащего, установлено в целях определения факта, соответствует ли состояние здоровья кандидата установленным требованиям. Однако, несмотря на наличие законной цели, это не может оправдать проведение медицинского обследования лица против его воли. Тем не менее, если лицо было проинформировано и все равно отказалось от прохождения обязательного освидетельствования, соответствующее учреждение не обязано принимать его на работу и принимать на себя связанные с таким трудоустройством риски.

В данном конкретном деле лицо отказалось от прохождения тестирования на СПИД, что означает, что проведение учреждением иных тестов на наличие косвенных признаков СПИДа явилось нарушением права на неприкосновенность частной жизни такого лица.

---

http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=741431 (accessed: 30.07.2018).

[125] X v Commission of the European Communities. - Appeal - Member of the temporary staff - Pre-recruitment medical examination - Repercussions of a refusal to undergo an Aids test - Breach of the right of secrecy as regards state of health. [Electronic resource]: Judgment of the Court of 5 October 1994. Case C-404/92 P. // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1533053077430&uri=CELEX:61992CJ0404 (accessed: 30.07.2018).

Бирюк против Литвы (Biriuk v. Lithuania) N 23373/03.[126] В 2001 году крупнейшая литовская газета опубликовала на первой полосе статью об угрозе распространения СПИДа в отдаленном районе Литвы. В частности, в ней содержались ссылки на медицинский персонал местной больницы, подтверждавший, что г-н Армонас и г-жа Бирюк заражены вирусом ВИЧ. О г-же Бирюк, охарактеризованной как «печально известная неразборчивостью в связях», также сообщалось, что она имеет двоих незаконных детей с г-ном Армонасом. В связи с этим г-н Армонас и г-жа Бирюк предъявили иски к газете, ссылаясь на нарушение их права на неприкосновенность частной жизни. Суды удовлетворили иски, признав, что статья носила порочащий характер, и что газета опубликовала информацию о личной жизни согласия указанных лиц или законного общественного интереса. Однако в обоих делах суды указали, что не установлен факт преднамеренного распространения информации, поэтому они применили норму Закона об информировании общественности, который ограничивал сумму компенсации при отсутствии такого намерения 10 000 литов (приблизительно 2 900 евро).

Заявители жаловались, что, несмотря на признание судами страны серьезного нарушения их права на личную жизнь, им были присуждены незначительные компенсации ущерба. В обоих делах Европейский Суд не видит оснований для оспаривания выводов национальных судов. Тот факт, что г-жа Бирюк и г-н Армонас жили в деревне, тем более увеличивал вероятность того, что соседи и ближайшие родственники будут осведомлены об их болезни. Аналогично Европейский Суд согласился с мнением судов страны о том, что статья не содержала дискуссии, представляющей общественный интерес. Особенную озабоченность вызывает тот факт, что согласно публикации медицинский персонал подтвердил сведения о болезни г-жи Бирюк и г-на Армонаса. Существенное значение имеют гарантии медицинской конфиденциальности и запрет на раскрытие персональных данных, содержащиеся в национальном законодательстве, особенно с учетом негативного влияния такого раскрытия на готовность других лиц проходить добровольные тесты на ВИЧ и соответствующее лечение. В подобных делах законодательные ограничения судейского усмотрения в возмещении ущерба, который претерпели жертвы, лишили заявителей защиты их личной жизни, на которую они обоснованно могли рассчитывать. По делу допущены нарушения требований статьи 8 Конвенции о защите прав человека и основных свобод.

[126] Армонас против Литвы (Armonas v. Lithuania) (36919/02) Бирюк против Литвы (Biriuk v. Lithuania) [Электронный ресурс]: Постановление Европейского суда по правам человека от 25.11.2008 (23373/03) // Европейская конвенция о защите прав человека: право и практика [Сайт]. – URL: http://www.echr.ru/documents/doc/2468230/2468230-003.htm (дата обращения: 30.07.2018).

Европейский Суд присудил выплатить каждому заявителю 6 500 евро в счет компенсации причиненного морального вреда.

Раду против Молдовы (Radu v. the Republic of Moldova) N50073/07.[127] Заявительница, г-жа Раду занималась преподавательской деятельность в Полицейской академии. В ходе беременности двойней она была госпитализирована из-за угрозы выкидыша, при этом работодателю она сообщила, что не сможет выйти на работу по причине болезни. Работодатель запросил дополнительную информацию в больнице, где она находилась, о причинах ее отсутствия, в ответ ему предоставили сведения о ее состоянии здоровья и лечении. Г-жа Раду обратилась в суд на том основании, что раскрытие информации о ее здоровье ее работодателю причинило ей стресс, в результате чего у нее случился выкидыш. По ее мнению, раскрытие этих сведений сотрудниками больницы ее работодателю являлось нарушением ее на уважение частной жизни.

ЕСПЧ установил, что раскрытие информации о состоянии здоровья заявительницы и примененных процедурах ее работодателю не соответствовало национальному закону, а потому ее право на уважение частной жизни было нарушено. Суд подчеркнул, что раскрытие подобной информации было допустимо только с согласия пациента и никакие исключения из данного правила в данном случае не могут быть применены. Суд установил нарушение ст. 8 Конвенции о защите прав человека и основных свобод, на основании которого государство выплатило заявительнице г-же Раду 4500 евро в качестве возмещения за моральный ущерб и судебные издержки в размере 1440 евро.

Германия

Понятие врачебной тайны отсутствует в законодательстве Германии. При этом обязанность сохранять сведения, относящиеся к пациенту, выводится из положений ст.203 Уголовного кодекса Германии ФРГ[128]. Согласно данной статье каждый, кто незаконно разглашает секрет, относящийся, в том числе, к сфере частной жизни, и который стал известен лицу в качестве медицинского работника, несет ответственность в виде штрафа или

[127] Radu v. the Republic of Moldova [Electronic resource]: Judgement of the European Court of Human Rights dated July 15, 2014 // European Court of Human Rights [Site]. – URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-142398%22]} (accessed: 30.07.2018).

[128] German Criminal Code of 13.11.1998 [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/englisch_stgb/ (accessed: 07.08.2018).

тюремного заключения на срок не более одного года.

В отсутствие самого понятия врачебной тайны факт отнесения той или иной информации к врачебной тайне подлежит исследованию в каждом конкретном деле. В связи с этим, можно сказать, что принцип формирования является открытым. Помимо этого законодательно не закреплен и состав сведений, составляющих врачебную тайну. Однако необходимо отметить, что к таким сведениям относятся, в том числе, персональные данные и специальные категории персональных данных.

В части вопроса о разграничении сведений, составляющих врачебную тайну, и сведений ограниченного доступа между собой следует отметить, что институт сведений ограниченного доступа в законодательстве и судебных решениях не выявлен.

Сведения, составляющие врачебную тайну, одновременно могут относиться к частной жизни, а также персональным данным, в том числе, специальным категориям персональных данных.

В той части, в которой врачебную тайну составляют персональные данные, субъект персональных данных может подать жалобу в надзорный орган по месту проживания, работы или места предполагаемого нарушения в соответствии со ст.77 GDPR. При этом при нарушении установленных требований к обработке персональных данных ответственность может наступать в соответствии с Федеральным законом о Защите персональных данных ФРГ от 30 июня 2017 г. (Закон о ПД)[129]. Кроме того, как указывалось выше за нарушение врачебной тайны предусмотрена уголовная ответственность в ст. 203 Уголовного кодекса ФРГ. Состав разглашения врачебной тайны по конструкции является формальным. Таким образом, наступление общественно опасных последствий не выступает обязательным признаком объективной стороны.

По вопросу о соотношении существующих подходов к врачебной тайне и защите конституционных прав можно отметить, что судебные решения, иллюстрирующие данное соотношение не обнаружены. Однако можно предположить, что в данном случае используется общий подход, основанный на оценке пропорциональности ограничения

[129] Federal Data Protection Act (BDSG) of 30.06.2017 [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf (accessed: 07.08.2018).

прав[130].

Порядок передачи и условия передачи сведений, составляющих врачебную тайну, третьим лицам, а также аффилированным лицам и аудиторам, в том числе, трансграничная передача, аналогичны правилам GDPR.

В отношении случаев, условий и порядка передачи сведений, составляющих врачебную тайну, третьим лицам без согласия субъектов необходимо отметить, что с точки зрения Закона о ПД и GDPR согласие – это лишь одно из нескольких оснований обработки персональных данных. Таким образом, по умолчанию, допустима обработка медицинских данных при наличии иных, помимо согласия, оснований для обработки. В то же время в Законе о ПД содержатся уточнения в части такой обработки специальных категорий персональных данных по сравнению с регулированием GDPR.

Например, в пп. b п.1 ст.22 Закона о ПД, принятого в развитие GDPR, указывается, что обработка специальных категорий персональных данных без согласия субъекта персональных данных может осуществляться не только медицинским работником, но также и любым другим лицом, имеющим аналогичные обязанности по сохранению конфиденциальности, для следующих целей:

1) превентивной медицины
2) постановки диагноза
3) оказания медицинской или социальной помощи или лечения
4) для управления системами здравоохранения или социального обеспечения
5) оценки работоспособности работника
6) иная обработка в соответствии с договором субъекта персональных данных с медицинским работником.

Кроме того специальные категории персональные данные могут быть обработаны без согласия субъекта персональных данных для обеспечения высоких стандартов качества в сфере здравоохранения, а также в целях обеспечения надежности медицинского обслуживания и лекарственных средств или медицинской техники.

Для обработки специальных категорий персональных данных без согласия, контроллеры должны внедрять законодательно определенные меры информационной

[130] A. Barak. Proportionality. Constitutional Rights and their Limitations. [Electronic resource]: International Journal of Constitutional Law, Volume 13, Issue 2, 1 April 2015 // Oxford Academic. The International Journal of Constitutional Law [Site]. – URL: https://doi.org/10.1093/icon/mov028 (accessed: 07.08.2018).

безопасности (ст.22 Закона о ПД). В частности, к таким мерам относится:

(1) принятие внутренних политик, регулирующих повторное использование данных;

(2) обучение сотрудников;

(3) назначение сотрудника по защите данных;

(4) контроль доступа;

(5) ведение журнала событий и мониторинг;

(6) шифрование и / или псевдонимизация;

(7) создание резервных копий и процедур быстрого восстановления; и

(8) периодический аудит безопасности.

Здесь необходимо упомянуть инициативу Германии по созданию электронного здравоохранения. Так, с 1995 года в Германии существует медицинская страховая карточка, которая изначально создавалась исключительно для целей страхования. С 2014 года карта представлена в электронном формате, аналогичном формату кредитной карты с чипом и фотографией. На ней хранятся персональные данные, которые являются конфиденциальными. Во-первых, на карте хранятся данные, которые хранились и в прошлой версии карты[131], а именно: наименование схемы страхования, ФИО застрахованного, дата рождения, пол, адрес, страховой номер, дата начала страхового покрытия и т.д. Для считывания информации с карты используются специальные устройства (card reader).

В 2015 году был принят закон, регулирующий использование электронной медицинской карточки[132]. Законом предусмотрено, что помимо указанных выше данных карта также будет хранить медицинские назначения (электронные рецепты), медицинские данные, необходимые на случай экстренных ситуаций, электронные врачебные заключения, сведения о непереносимости определенных лекарственных средств, электронную медицинскую карту, данные о пособиях и затратах на страхование. Технически на самой карте могут храниться до 8 электронных рецептов и медицинские данные, необходимые на случай экстренных ситуаций. Остальные данные хранятся на сервере специальной информационной системы

[131] Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung - (Artikel 1 des Gesetzes v. 20. Dezember 1988, BGBl. I S. 2477) [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/sgb_5/__291a.html (accessed: 08.08.2018).

[132] Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze vom 21.12.2015 [Electronic resource] // Bundesgesetzblatt [Site]. – URL: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s2408.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s2408.pdf%27%5D__1533657145850 (accessed: 08.08.2018).

(функционирование системы обеспечивает специальная уполномоченная организация[133]). Отметим, что сбор, обработка и использование данных посредством электронной карты допустимы только с согласия, за исключением электронных рецептов, которые могут храниться без согласия пациента, однако должны быть удалены при наличии такого требования.

Доступ к данным карты может получить только врач, обладающий вторым ключом – персональной картой медицинского работника. Доступ осуществляется только в медицинских целях и только с согласия пациента, однако к данным, необходимым на случай экстренной помощи (в случае, если такие данные внесены на карту), врач может получить доступ в такой ситуации и без согласия пациента. Страховые компании не имеют доступа к данным карты[134].

Ключевая критика данной инициативы была направлена в сторону недостаточной защиты персональных данных[135]. В то же время, Министром здравоохранения Германии было отмечено, что из-за чувствительности содержащихся на карте данных, уровень ее защиты превышает уровень защиты банковских карт[136]. Передача данных осуществляется не через сеть Интернет, а через специально созданную безопасную сеть. Все медицинские данные зашифровываются.

В дополнение отметим еще несколько законодательно установленных случаев раскрытия сведений, составляющих врачебную тайну, без согласия субъекта:

- угроза распространения инфекционных заболеваний (Закон о защите населения от инфекционных заболеваний)[137]
- отдельные запросы, предусмотренные Кодексом социального права, часть V (§ 275

[133] Gematik. Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH [Electronic resource] // Gematik [Site]. – URL: https://www.gematik.de/telematikinfrastruktur/ (accessed: 08.08.2018).

[134] Die elektronische Gesundheitskarte [Electronic resource] // Bundesministerium für Gesundheit [Site]. – URL: https://www.bundesgesundheitsministerium.de/themen/krankenversicherung/egk.html#c1058 (accessed: 08.08.2018).

[135] E-Health-Gesetzentwurf ist für ULD enttäuschend 16.01.2015 [Electronic resource] // Das Unabhängige Landeszentrum für Datenschutz [Site]. – URL: https://www.datenschutzzentrum.de/artikel/861-E-Health-Gesetzentwurf-ist-fuer-ULD-enttaeuschend.html (accessed: 08.08.2018).

[136] E-Health Law in Germany. March 2016. Taylor Wedding [Electronic resource] // Taylor Wessing [Site]. – URL: https://united-kingdom.taylorwessing.com/synapse/ti-ehealth-law-germany.html (accessed: 08.08.2018).

[137] Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen 20.07.200 [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: http://www.gesetze-im-internet.de/ifsg/index.html (accessed: 07.08.2018).

SGB V[138])

Законодательство Германии не содержит прямого регулирования в отношении изъятия из режима охраны сведений, составляющих врачебную тайну, в целях обеспечения возможности обработки накопленных данных для достижения социальных (вкл. повышения уровня здоровья населения), государственных, экономических целей. Однако согласно ст.27 Закона о ПД специальные категории персональных данных могут обрабатываться в целях исследований и статистики без согласия субъекта персональных данных, если такая обработка необходима для указанных целей и если интересы контролера значительным образом превалируют над интересами субъекта персональных данных. При этом специальные категории персональных данных должны быть представлены в анонимизированном виде, насколько это позволяют цели проведения исследования или статистики, если это не противоречит законным интересам субъекта персональных данных.

Права субъекта персональных данных на доступ, исправление, ограничение и отказ ограничены в той части, в которой такие права могут сделать невозможным или значительно ухудшить достижение целей исследований или статистики. Такие ограничения необходимо для выполнения целей исследования или статистики.

Открытые сведения о здравоохранении публикуются Федеральным статистическим управлением Германии[139].

Big data

Использование big data технологий сегодня активно обсуждается в Германии. Так, крупные игроки на этом рынке отмечают, что действующее регулирование в сфере персональных данных может сдерживать процессы использования этих технологий в сфере здравоохранения[140]. Как было точно замечено сооснователем компании SAP, которая занимается также и технологиями big data, крупные проекты с использованием данных технологий в сфере медицины осуществляются в других странах, а не в Германии, потому что в Германии «прежде всем сделать первый шаг, мы начинаем спрашивать о защите персональных данных».

---

[138] Sozialgesetzbuch (SGB V) Fünftes Buch Gesetzliche Krankenversicherung [Electronic resource] // Sozialgesetzbuch [Site]. – URL: https://www.sozialgesetzbuch-sgb.de/sgbv/1.html (accessed: 07.08.2018).

[139] The Federal Statistical Office [Electronic resource] // Destatis [Site]. – URL: https://www.destatis.de/EN/Homepage.html (accessed: 07.08.2018).

[140] M. Telgheder, G. Brower-Rabinowitsch. Big-Data Fear Plagues German Healthcare. 24.04.2016 [Electronic resource] // Handelsblatt Global [Site]. – URL: https://global.handelsblatt.com/companies/big-data-phobia-plagues-german-healthcare-479373 (accessed: 07.08.2018).

Вопрос возможности доступа третьих лиц к данным, составляющим врачебную тайну с согласия субъекта был раскрыт выше.

Администрирование согласий субъектов врачебной тайны на обработку сведений, составляющих врачебную тайну и/или их передачу третьим лицам (в т.ч. наличие права субъекта определять порядок использования таких сведений, делегирования права на выдачу согласий, отзыва согласий на их сбор, обработку и/или передачу и т.д.) подчиняется общим правилам, установленным в GDPR.

Специальные нормы по идентификации субъектов тайн (в т.ч. их законных представителей) не выявлены.

Согласие на обработку сведений, составляющих врачебную тайну, аналогичны согласиям на обработку иных персональных данных. Способ получения, передачи и хранения также аналогичен общим требованиям, установленным GDPR.

В части информационной безопасности требования к информационным системам, содержащим сведения, относящиеся к врачебной тайне, закреплены в Законе об информационной безопасности[141].

Испания

Ст. 3 Закона Испании о медицинской информации 2002 года (Закон № 41/2002 от 14 ноября, регулирующий свободу пациента, права и обязанности клиник в отношении информации и документации) определяет документы медицинской организации как носители информации любого вида, которые содержат данные медицинского характера. Медицинская («клиническая») информация при этом представляет собой любые данные, независимо от формы, класса или типа, которые позволяют получить или вывести сведения о физическом состоянии и здоровье физического лица либо о способах, необходимых для его поддержания, ухода, улучшения или восстановления.

Закон Испании о медицинской информации 2002 года в ч. 1 ст. 2 устанавливает, что достоинство человеческой личности и уважение к автономии воли человека, а также к неприкосновенности его частной жизни, определяют всю деятельность, направленную на

[141] BSI Act of 14 August 2009 (Federal Law Gazette I p. 2821) [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html (accessed: 08.08.2018).

получение, использование, хранение, обеспечение безопасности и передачу информации и документов медицинской организации. Согласно ч. 7 ст. 2, лицо, которое получает доступ к информации и документам медицинской организации обязано обеспечивать необходимый уровень защиты информации.

В дополнение к указанному выше, ч. 1 ст. 7 Закона Испании о медицинской информации отдельно закрепляет право на неприкосновенность частной жизни и указывает, что каждый имеет право на конфиденциальность своих данных, относящихся к здоровью, и что никто не может получать к таким данным доступ без предварительного разрешения (допуска) на основании закона. Ч. 2 ст. 7 указывает, что медицинские организации должны обеспечивать гарантии указанных прав и принимать необходимые меры и документируемые процедуры в целях обеспечения правомерного доступа к данным пациентов.

Как показывает анализ испанского законодательства, к медицинской тайне применим тот же подход, согласно которому медицинскую тайну также можно рассматривать как один из квалифицирующих признаков информации. Ст. 16 Закона Испании о медицинской информации определяет возможности использования истории болезни (медицинской карты) пациента. В частности, ч. 3 ст. 16 указывает на то, что доступ к истории болезни со стороны судебной власти, органов в области эпидемиологии, общественного здоровья, следственных органов, образовательных организаций в каждом конкретном случае определяется исходя из законодательства о персональных данных и об охране здоровья граждан.

Помимо общих положений о принципах формирования врачебной тайны, ч. 2 ст. 15 Закона Испании о медицинской информации определяет содержание истории болезни (медицинской карты) пациента, которая включает в себя документацию, относящуюся к процессу госпитализации, подтверждение приема, информацию о срочности оказания медицинской помощи, анамнез и физическое состояние, развитие болезни, медицинские показания, время медицинского направления, информацию о дополнительных результатах исследования, информированное согласие и ряд иных данных, относящихся к сведениям о состоянии пациента, данных им согласиях и заключениях относительно его состояния и дальнейшего лечения.

Основные положения, определяющие порядок доступа третьих лиц к медицинской тайне, определены в ст. 16 Закона Испании о медицинской информации, нацеленной на регулирование использования истории болезни (медицинской карты) пациента.

Согласно ч. 1 ст. 16, история болезни (медицинская карта) представляет собой

инструмент, основным предназначением которого является предоставление адекватной медицинской помощи пациенту. Доступ к включенным в нее данным со стороны профессиональных медицинских работников, осуществляющих диагностику или лечение пациента именно в этих целях. При этом, в соответствии с ч. 2 ст. 16 каждая медицинская организация должна предоставить постоянный доступ к такой информации для профессиональных медицинских работников, оказывающих медицинскую помощь пациентам.

Ч. 3 ст. 16 предусматривает доступ к сведениям, включенным в историю болезни, в целях осуществления судебной власти, полномочий органов в области эпидемиологии, общественного здоровья, следствия, а также образовательных организаций. Такой доступ регулируется в каждом конкретном случае в соответствии с законодательством о персональных данных. При такого рода доступе требуется разделять данные, позволяющие идентифицировать пациента, и данные, которые связаны непосредственно с оказанием медицинской помощи таким образом, чтобы, по общему правилу обеспечивалась анонимность при обработке. Объединение идентифицирующих и анонимных (связанных с медицинской помощью) данных допускается в качестве исключения при реализации правосудия в установленных уголовно-процессуальным законодательством случаях, и такие ситуации разрешаются в зависимости от конкретных обстоятельств. Кроме того, в особых случаях, связанных с угрозой общественному здоровью, к идентифицирующим медицинским данным могут получать доступ органы в области санитарно-эпидемиологического благополучия, но в таких ситуациях информация может быть доступна только профессиональным работникам, связанным служебной тайной или эквивалентными обязательствами о неразглашении получаемой информации.

Трансграничная передача сведений, составляющих медицинскую тайну, не урегулирована специально, и подчиняется общим правилам, предусмотренным GDPR и Законом о персональных данных Испании.

Из проанализированных источников следует, что основным принципом раскрытия таких данных является анонимность и пропорциональность целям раскрытия.

В последнем опыте Испании особое внимание в литературе получила программа регионального правительства Каталонии по развитию системы открытых данных о здоровье, генерируемых в данном регионе (“PADRIS”). Согласно данной программе, значительный массив данных о здоровье пациентов обобщается способом, предполагающим анонимизацию

и обеспечение безопасности данных. Целью программы является развитие исследований и инновации в медицинских науках. Цель программы увязывается с конституционным правом граждан на защиту здоровья, предусмотренным ст. 43.1 Конституции Испании, социальную защиту согласно ст. 50 Конституции Испании и защиту право потребителей, подразумевающую, в том числе, защиту из здоровья, что вытекает из ст. 51.1 Конституции Испании.[142]

Основной принцип программы заключается в том, чтобы медицинская информация, касающаяся отдельных пациентов, которая ранее хранилась в отдельных медицинских организациях, была объединена в единую базу данных, допускающую анализ посредством **технологий больших данных**. В декларативных документах программы предусматривается «полная анонимизация» данных.[143]

Отдельного внимания заслуживает критика данной программы с консервативной точки зрения. Основной предмет критики – потенциальная возможность органов здравоохранения «продавать» данные, полученные от пользователей для включения в систему информации о здоровье бизнесу, с учетом того обстоятельства, что во многих случаях пациенты могут быть недостаточно проинформированы о целях использования их данных о здоровье на этапе получения таких данных, в том числе, в сравнении с подходами, реализованными в Великобритании.[144] В основе критики лежат достаточно широкие соображения, которые связаны с тем, что использование данных с учетом все же существующего риска их деанонимизации и того факта, что эти данные связаны со здоровьем субъектов, могут повлечь неправомерную дискриминацию со стороны работодателей, страховщиков, банков и иных подобных организаций, что может повлечь убытки заинтересованных физических лиц. В качестве основных и общих рисков использования больших данных при этом указывается возможность повторной идентификации в условиях, когда невозможно предугадать заранее способы последующего использования данных посредством технологий больших данных – именно на это указывал А.И. Савельев в статье «Проблема применения законодательства о персональных данных в эпоху “Больших данных”» применительно к России, но проблема эта носит общемировой уровень и

[142] См.: Ruda-Gonzalez A. Who’s Afraid of the Big Bad Data? Some Critical Reflections on the Programme to Open Access to Health Data (The Catalan Approach) // Asia Pacific Journal of Health Law & Ethics. – 2017. – Vol. 11. – No. 1. – pp. 61-82.

[143] Ibid. P. 62.

[144] Ibid. P. 71.

указанный теоретический анализ в полной мере соотносится с рассматриваемым контекстом.

Эстония

В соответствии со статьей 26 Конституции Эстонии, каждый имеет право на неприкосновенность семейной и частной жизни. Государственные учреждения, местные самоуправления и их должностные лица не вправе вмешиваться в чью-либо семейную и частную жизнь иначе, как в случаях и в порядке, установленных законом, в целях защиты здоровья, нравственности, общественного порядка или прав и свобод других людей, в целях пресечения преступления или поимки преступника[145].

Защита данных, связанных со здоровьем лица, относится к основополагающим правам пациента и имеет большое значение в контексте оказания медицинских услуг с использованием систем электронного здравоохранения, трансграничного лечения и проведения клинических и иных исследований. Система электронного здравоохранения eHealth Эстонии является одной из самых развитых в Европе. Ее основой является система Electronic Health Record (*e-Health Record* или *EHR*), построенная с использованием технологии блокчейн (*blockchain*) и интегрирующая данные различных медицинских организаций с целью создания единых учетных записей, доступ к которым может быть предоставлен каждому пациенту онлайн. Доступ к системе для пациентов осуществляется через e-Patient portal[146].

EHR представляет собой базу данных сведений о состоянии здоровья, наполнение которой обеспечивается за счет законодательно закрепленной обязанности всех поставщиков медицинских услуг вносить медицинские данные всех пациентов в систему. Доступ к системе имеют пациенты, поставщики медицинских услуг, судебные эксперты-криминалисты (внесении данных о смерти лица) и другие лица, обрабатывающие данные (государственные органы, органы статистики, научные организации). Последние вправе использовать данные из EHR в целях проведения исследований, анализа и подготовки статистических данных, необходимых для разработки политики в сфере здравоохранения и исполнения

[145] The Constitution of the Republic of Estonia [Electronic resource]: passed by referendum of June 28, 1992 (as revised May 05, 2015) // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/rhvv/act/521052015001/consolide (accessed: 30.07.2018).

[146] e-Patient portal [Electronic resource] // Patient Portal [Site]. – URL: https://www.digilugu.ee/login?locale=en (accessed: 30.07.2018).

международных обязательств, при условии, что все данные закодированы (обезличены). Для использования обезличенных данных получение согласия лица не требуется. Доступ может быть предоставлен и иным лицам, если это предусмотрено законом.

Пациенты осуществляют полный контроль над своими данными и вправе в любой момент ограничить доступ к данным, содержащимся в системе. В этом случае лицу будет направлено уведомление, что предоставление медицинских услуг на базе неполной информации о его состоянии может быть опасным для здоровья.

Кроме того, данные лица, касающиеся его здоровья, относятся к категории специальных персональных данных. Поскольку Эстония является государством-членом ЕС, на нее распространяются соответствующие положения европейского права. В частности, вопросы обработки персональных данных регулируются GDPR, имеющим прямое действие на территории всего Европейского союза. Следует отметить, что в соответствии с п. 8 преамбулы GDPR, в случае, если GDPR предусматривает возможность уточнения или ограничения его положений в национальном законодательстве, государства-члены ЕС могут по мере необходимости инкорпорировать элементы GDPR в национальное законодательство. GDPR содержит несколько случаев, когда у национальных законодателей появляется право на изменение положений регламента в своем законодательстве. В тринадцати странах-членах ЕС уже принято национальное законодательство, учитывающее новые положения GDPR. В остальных странах такое законодательство еще не принято, но уже опубликованы и рассматриваются (на разных этапах) законопроекты, разработанные в соответствии с новыми принципами и правилами GDPR. Эстония относится к последним, соответствующий законопроект еще находится в разработке[147].

Таким образом, на дату составления настоящего отчета в целях определения правового режима сведений, относящихся к здоровью человека, необходимо руководствоваться положениями GDPR, описанными в разделе, посвященном регулированию ЕС.

Дополнительное применимое регулирование можно обнаружить в специализированном законодательстве. Вопросы обеспечения безопасности данных

[147] Personal Data Protection Act 616 SE Draft [Electronic resource] // Riigikogu [Site]. – URL: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/e14c5e2f-b684-4aa4-a7dd-ffb76f63f395/Isikuandmete%20kaitse%20seadus (accessed: 30.07.2018).

зафиксированы в Законе об услугах в сфере здравоохранения[148] (*Health Services Organisation Act.)* В статье 41 указывается, что организации в сфере здравоохранения, обязанные обеспечивать конфиденциальность информации в соответствии с законом, вправе обрабатывать персональные данные пациентов для целей предоставления медицинских услуг, включая специальные категории персональных данных, без согласия субъекта данных. Данные о состоянии здоровья пациента, находящегося в больнице, могут быть предоставлены близким лицам, за исключением случаев, когда (1) субъект данных запретил предоставление таких данных указанным лицам, (2) следственный орган запретил такое представление в целях предотвращения совершения преступления или для целей проводимого расследования.

В соответствии со статьей 5 Закона о психическом здоровье[149] (*Mental Health Act*) конфиденциальной является информация о психиатрическом диагнозе и лечении лица. Раскрытие такой информации допускается только с письменного согласия лица или его/ее представителя, либо по запросу органов следствия, полиции, прокуратуры, служб надзора за осужденными при судах в случаях, определенных законом. Раскрытие таких данных разрешается органам муниципальной и государственной власти или близким лица в той степени, в какой это необходимо для получения их мнения или согласия относительно помещения субъекта данных для лечения в закрытые учреждения.

В 2000 году был принят Закон об исследовании генов человека[150] (*Human Genes Research Act*). В соответствии с данным законом был создан Генный фонд (*Gene bank*), представляющий собой базу данных (биобанк) образцов тканей, ДНК, сведения о состоянии здоровья, генеалогии, генетических данных и данных, позволяющих идентифицировать генных доноров. Управление Генным фондом осуществляется Тартуским университетом, который осуществляет деятельность по развитию генетических исследований, собирает информацию о здоровье и генетическую информацию эстонского населения и использует результаты генетических исследований для целей укрепления здоровья населения. Для достижения указанных целей университету предоставляется право организовывать сбор

[148] Health Services Organization Act of May 09, 2001 (as revised May 02, 2018) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523052018005/consolide (accessed: 30.07.2018).

[149] Mental Health Act of February 12, 1997 (as revised December 09, 2015) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/501022016017/consolide (accessed: 30.07.2018).

[150] Human Genes Research Act of December 13, 2000 (as revised February 19, 2014) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/518062014005/consolide (accessed: 30.07.2018).

образцов тканей, составлять, кодировать, декодировать, хранить, уничтожать сведения о состоянии здоровье и генеалогические данные, проводить генетические исследования, собирать, хранить и уничтожать генетические данные. При этом университет вправе поручить право на обработку данных, за исключением кодирования и декодирования, третьему лицу на основании договора и на условиях, предусмотренных законом.

В соответствии с данными, опубликованными на сайте Тартуского университета, в Генном фонде содержатся данные от 51 535 человек (генных доноров) в возрасте от 18 лет и старше. Половой и возрастной состав базы данных достаточно точно отражает состав населения Эстонии. Сбор данных проводился во всех уездах Эстонии. Из представленных в биобанке Эстонии национальностей 83% – эстонцы, 14% – русские и 3% – другие национальности. Все данные генных доноров, находящиеся в биобанке, были собраны профессиональными медиками (в большинстве случаев семейными врачами, а также стационарными врачами и медсёстрами)[151].

Сбор материалов и данных для целей формирования Генного банка осуществляется ан добровольной основе с согласия донора. Согласие составляется по установленной письменной форме, должно содержать сведения, предусмотренные законом, и подписывается донором. Частичное или согласие под условием не допускаются. До момента поучения согласия донор должен быть проинформирован о своих правах. Донорам гарантируется конфиденциальность сведений об их личности и о факте предоставления материалов в биобанк. В отношении обработки таких данных законом устанавливаются самые высокие стандарты защиты данных. С целью обеспечения конфиденциальности личные данные генного донора отделяются от генетических данных, и каждый анализ крови и свод сведений о здоровье получает уникальный 16-значный код. Запрещено подключение базы данных Генного фонда к Интернету.

Законом установлено, что полученные образцы тканей, сведения о здоровье, иные персональные и генеалогические данные принадлежат на праве собственности оператору данных (университету) с момента их предоставления/создания, а потому доноры не вправе требовать выплаты им каких-либо денежных средств за обработку таких данных. Передача права собственности не допускается, а потому в случае прекращения деятельности оператора данные переходят в управление государством. Использование данных, образующих Генный

[151] Эстонский Генный фонд Тартуского Университета [Electronic resource] // Universitas Tartuenis [Site]. – URL: https://www.geenivaramu.ee/ru/estonskiy-gennyy-fond-tartuskogo-universiteta (accessed: 30.07.2018).

фонд допускается только для целей научных исследований, исследований заболеваний и лечения доноров, исследований в целях общественного здравоохранения и статистических целей. Использование в иных целях, в частности в рамках уголовного расследования, запрещается. Данные генеалогии могут быть использованы для структурирования образцов тканей, ДНК и сведений о состоянии здоровья на основе кровного родства.

Если донор не желает более участвовать в проекте Генного фонда, он имеет право требовать уничтожения данных, позволяющих идентифицировать личность, или, в определенных случаях, всей хранящейся в Генном фонде информации о нем. Закон предусматривает уголовную ответственность за принуждение к участию в генном донорстве, за проведение незаконных исследований на людях, за разглашение хранящейся в тайне информации и за дискриминацию.

Помимо установления специального режима обработки персональных данных, относящихся к здоровью лица, сохранение врачебной тайны обеспечивается за счет возложения соответствующих обязанностей по конфиденциальности на сотрудников медицинских учреждений и организаций. В соответствии со ст. 768 Закона об обязательствах (*Law of Obligations Act*)[152] организации в сфере здравоохранения и их сотрудники, оказывающие медицинские услуги, обязаны сохранять конфиденциальность данных пациентов, в том числе данных о состоянии их здоровья, которые стали им известны в ходе оказания медицинских услуг или при выполнении иных профессиональных обязанностей. Также они обязаны обеспечивать, чтобы информация, содержащаяся в соответствующих медицинских документах, не стала известна третьим лицам, за исключением случаев, когда это требуется по закону или по соглашению с пациентом. Отступления от данного правила допускается в случаях, если нераскрытые такой информации создает угрозу того, что пациент причинит существенный вред себе или окружающим.

Обязанность по сохранению конфиденциальности информации о состоянии здоровья и частной жизни застрахованных лиц, ставшей известной при исполнении профессиональных и договорных обязанностей возлагается на работников и представителей фонда медицинского

[152] Law of Obligations Act of September 26, 2001 (as revised December 13, 2017) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/507022018004/consolide (accessed: 30.07.2018).

страхования, если иное не предусмотрено законом[153]. Специальные обязанности возлагаются и на лиц, ответственных за безопасность и охрану труда. В соответствии со ст. 192 Закона об Обеспечении безопасности и охраны труда (*Occupational Health and Safety Act*)[154] специалист по профессиональному здравоохранению (*occupational health specialist*) должен следовать следующим принципам профессиональной этики:

- сохранение конфиденциальности сведений, который он/она получил в ходе выполнения своих обязанностей за исключением случаев, когда отклонение от таких принципов требуется для защиты здоровья и обеспечения безопасности работников;
- обеспечение конфиденциальности сведений о здоровье и частной жизни работников;
- раскрытие сведений о результатах медицинских обследований руководящего состава только в случае наложения ограничений на выполнение профессиональных обязанностей.

За разглашение персональных данных, относящихся к специальной категории, предусмотрена уголовная ответственность:

1. за незаконное раскрытие данных для физического лица – штраф в размере до 300 единиц штрафа (примерно 1200 Евро) [155], для юридического лица - штраф в размере до 32000 Евро;

за незаконное раскрытие данных с целью получения персональной выгоды или в случае если такое раскрытие причинило существенный вред другому лицу для физического лица – аналог исправительных работ (*pecuniary punishment;* далее условно – «исправительные работы») или лишение свободы на срок до одного года, для юридического лица – исправительные работы.

Соединенные Штаты Америки

Понятие ***медицинской тайны*** прямо не закреплено в системе права США, оно является

[153] Estonian Health Insurance Fund Act of June 14, 2000 (as revised December 06, 2017) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/505012018001/consolide (accessed: 30.07.2018).

[154] Occupational Health and Safety Act of June 16, 1999 (as revised June 13, 2018) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/526062018002/consolide (accessed: 30.07.2018).

[155] В соответствии со ст. 47 Уголовного кодекса Эстонии, 1 единица штрафа ровняется 4 Евро.

составным и многоаспектным: чаще всего медицинская информация подпадает под регулирование сразу нескольких законодательных актов. Ниже приведены основные законы федерального уровня, связанные с медицинской тайной и оборотом медицинской информации.

Закон об ответственности и переносе данных о страховании здоровья граждан (HIPAA)156, принятый в 1996 году, является федеральным законом США, который определяет основные правила конфиденциальности медицинской информации и безопасного обмена такой информацией для защиты от несанкционированного использования, а также вводит понятие «охраняемой медицинской информации».

В целях укрепления и совершенствования закона HIPAA в феврале 2009 года был принят Закон о медицинской информации в области здравоохранения и медицинского здоровья («HITECH»). В то время как HIPAA касается вопросов безопасности и конфиденциальности информации в области здравоохранения, HITECH расширяет правила безопасности и конфиденциальности HIPAA для лиц, не подотчетных HIPAA напрямую, тем самым расширяет круг лиц, обязанных предпринимать разумные меры защиты медицинской информации. Таким образом, HIPAA и HITECH являются основными в части регламентации оборота медицинской информации.

Закон о недискриминации генетической информации (The Genetic Information Nondiscrimination Act) был принят в 2008 году для защиты генетической информации человека от использования дискриминационным образом.

США также приняли законы, регулирующие конфиденциальность информации, хранящейся в органах исполнительной власти, и право доступа к информации, содержащейся в федеральных архивных записях. Закон США о свободе информации (The Freedom of Information Act) регулирует право любого лица на доступ к информации, содержащейся в федеральных архивных записях государственных органов исполнительной власти. Закон о конфиденциальности 1974 года (The Privacy Act of 1974) регулирует защиту персональных данных физических лиц (пациентов и практикующих врачей), а также случаи раскрытия и распространения такой информации. Федеральный закон об информационной безопасности и управлении («FISMA») является федеральным законом, который устанавливает меры информационной безопасности для информации, собираемой или поддерживаемой

[156] HIPAA [Electronic resource] // U.S. Department of Health & Human Services [Site]. – URL: https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf (accessed: 30.07.2018).

государственными органами исполнительной власти или для них.

Самый последний крупный закон о здравоохранении, Закон о защите пациентов и доступной медицинской помощи («ACA»), принят в марте 2010 года, он включает в себя широкий спектр реформ системы здравоохранения, в том числе требование о том, чтобы все американцы получали медицинскую страховку, расширенные права на участие в программе Medicaid. Закон поощряет обмен информацией о здоровье в целях содействия и координации помощи, а также улучшения качества оказания медицинской помощи.

Так или иначе вышеназванные законы раскрывают понятие медицинской тайны, а также связанное с ним понятие медицинской информации.

Та или иная информация понимается в качестве относящейся к медицинской тайне, исходя из конкретного рассматриваемого случая[157]. Критерием формирования является отнесение признаков информации под конкретное нормативно-правовое регулирование. По мнению американских ученых исчерпывающее определение всей медицинской информации, входящей в понятие медицинской тайны, не нужно закреплять в законе, однако стоит решить данную проблему через призму руководящих принципов, стандартов, кодексов поведения, передовой практики и других типов «мягких» стандартов. Но данный принцип формирования и отнесения информации к медицинской тайне является не до конца сформированным в системе права США[158].

Состав сведений, составляющих медицинскую тайну, ограничивается индивидуально идентифицируемой медицинской информацией. Согласно § 160.103 Главы 45 Свода федеральных нормативных актов[159] индивидуально идентифицируемая медицинская информация – это информация, которая является видом медицинской информации, включая демографическую информацию, собранную от лица, и которая: (1) создается или хранится поставщиком медицинских услуг, медицинским планом, работодателем и т.д., а также (2) относится к прошлому, настоящему или будущему физическому или психическому здоровью человека; к оказанию медицинской помощи физическому лицу; к прошлой, настоящей или будущей оплате медицинской услуги лицом; и при этом это то (i) что идентифицирует человека; или (ii) имеются основания полагать, что информация может использоваться для

[157] Health information beyond HIPPA [Electronic resource] // U.S. Department of Health & Human Services [Site]. – URL: https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf (accessed: 30.07.2018).

[158] Health information beyond HIPPA [Electronic resource] // U.S. Department of Health & Human Services [Site]. – URL: https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf (accessed: 30.07.2018).

[159] 45 CFR 160.103 - Definitions [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/cfr/text/45/160.103 (accessed: 09.08.2018).

идентификации личности такого физического лица. Согласно закону HIPAA охраняемая медицинская информация означает индивидуально идентифицируемую медицинскую информацию, (i) передающуюся с помощью электронных средств; (ii) хранящуюся на электронных носителях; или (iii) передающуюся или хранящуюся в любой другой форме или среде. Охраняемая медицинская информация исключает индивидуально идентифицируемую медицинскую информацию в (i) отчетах о образовании и записях, охватываемых исключениями закона Family Educational Rights and Privacy Act; (ii) в записях о занятости, хранимых работодателями; (iii) касательно лица, умершего более 50 лет назад.

Закон HITECH указывает, что им медицинская информация понимается также как и законом HIPPA.

Сведения, составляющие медицинскую тайну, могут одновременно охраняться как иные виды тайн или иметь статус информации ограниченного доступа по иным основаниям. Как указано в п. 3.5. фактический состав сведений, составляющих медицинскую тайну, часто пересекается с иными видами тайн, например, с тайной связи (идентификаторы или серийные номера устройств, URL-адреса, IP-адреса). При этом разграничение происходит (1) по субъекту, хранящему информацию (страховая организация, медицинская организация) и подпадающему по HIPAA или HITECH; (2) по составу через установленные критерии, закрепленные в Своде федеральных нормативных актов и законе HIPPA.

Как указано выше, некоторые сведения составляющие медицинскую тайну могут одновременно охраняться как иные виды тайн.

Защита прав субъектов медицинской тайны обеспечивается наличием разветвленной юридической ответственности за нарушение медицинской тайны.

Гражданско-правовая ответственность определяется исходя из многоуровневой структуры. Здесь имеется четыре категории, используемые для расчета штрафа: (1) нарушение, которое лицо не осознавало и не могло избежать, лицо приложило разумные усилия для соблюдения правил HIPAA; (2) лицо должно было знать, что нарушает, но оно не могло избежать такого нарушения даже с разумной осторожностью (но не «умышленное пренебрежение» правилами HIPAA); (3) нарушение, понесенное в результате «умышленного пренебрежения» правилами HIPAA (в случаях, когда была предпринята попытка исправить нарушение); (4) нарушение правил HIPAA в следствии умышленного пренебрежения при отсутствии попыток исправить нарушение. Штрафы за вышеназванные виды нарушений следующие. категория 1: штраф в размере от 100 долларов США до 50 000 долларов США за

нарушение; категория 2: штраф в размере от 1000 долларов США до 50 000 долларов США за нарушение; категория 3: штраф в размере от 10 000 долларов США до 50 000 долларов США за нарушение; категория 4: штраф в размере от 50 000 долларов США за нарушение.

Уголовно-правовая ответственность лиц, ответственных за нарушение медицинской тайны, в частности за утечку медицинских персональных данных. Уголовные санкции за нарушения HIPAA подразделяются на три отдельных уровня, при этом срок и сопровождающий его штраф определяются судьей на основании фактов каждого конкретного дела. Как и в случае с гражданской ответственностью, рассматривается ряд общих факторов, которые повлияют на выданный штраф: уровень 1: разумная причина или незнание о нарушении - до 1 года тюремного заключения; уровень 2: получение персональных данных вследствие обмана - до 5 лет тюремного заключения; уровень 3: получение персональных данных для личной выгоды - до 10 лет тюремного заключения.

В деле *Emily Byrne v. Avery Center for Obstetrics and Gynecology, P.C.*[160] Верховный суд США указал, что пациент имеет право подать в суд как на врача, так и на юридическое лицо, оказавшее медицинские услуги в порядке частного иска, что не противоречит HIPAA, хотя и такое право им прямо не предусмотрено.

На сегодняшний день в США идут обсуждения по поводу необходимости изменения настоящего законодательства (HIPAA, HITECH) **в связи с использованием технологий «больших данных», интернета вещей и «искусственного интеллекта»**. На данном этапе встречаются мнения как поддерживающие, так и критикующие максимальную либерализацию законодательства, так как по их мнению она будет нарушать конституционные права граждан на защиту частной жизни (privacy).

Данные становятся индивидуально идентифицируемыми, если они включают в себя какой-либо из так называемых идентификаторов для физического лица или для работодателя или члена семьи, или если поставщик или исследователь осведомлен о том, что эта информация может использоваться как самостоятельно, так и в сочетании с другой информацией, чтобы идентифицировать человека. Этими идентификаторами являются: имя, адрес (все географические единицы меньше штата, включая адрес улицы, город, округ или почтовый индекс), все элементы (за исключением лет) дат, связанных с физическим лицом (включая дату рождения, дату приема, дату выписки, дату смерти и точный возраст),

[160] Emily Byrne v. Avery Center for Obstetrics and Gynecology, P.C [Electronic resource] // Caselaw [Site]. – https://caselaw.findlaw.com/ct-supreme-court/1885827.html (accessed: 30.07.2018).

телефонные номера, номера факса, адреса электронной почты, номер социального страхования, номер медицинской карты, номер получателя медицинского плана, номер банковского счета, номер сертификата/лицензии, идентификаторы транспортных средств и серийные номера, включая регистрационные номера автомобилей, идентификаторы или серийные номера устройств, веб-адреса (URL-ссылки), IP-адреса, биометрические идентификаторы, включая отпечатки пальцев или голос, полноценные фотографические изображения и любые сопоставимые изображения, любой другой уникальный идентификационный номер, характеристика или код.

Стоит отметить, что информация о здоровье сама по себе, без перечисленных выше идентификаторов, не считается персональными данными (индивидуально идентифицируемой медицинской информацией). Например, набор данных жизненно важных показателей сам по себе не является защищаемой медицинской информацией (без идентификатора).

В отношении регулирования передачи сведений, подход США отличается от подхода ЕС, и многие ученые описывают его как секторальный. Правила конфиденциальности применяются к некоторым типам персонально идентифицируемой информации, большая часть личной информации не подлежит никакому законодательству о конфиденциальности (privacy в широком смысле)161. Поскольку регулируемые данные переходят от одного хранителя к другому, правила конфиденциальности редко следуют за материальными носителями. Например, если объект, охваченный HIPAA, отправляет медицинскую карточку в школу, запись в руках школы подчиняется Закону о правах на семью и конфиденциальности (FERPA), а не HIPAA. Если записи передаются третьей стороне, которая не подпадает под регулирование HIPAA (например, агентство общественного здравоохранения, исследователь, правоохранительный орган или агентство национальной безопасности), HIPAA не применяется к таким записям в руках получателя.

По общему правилу согласно HIPAA пациент должен дать разрешение (authorization)[162] для раскрытия и передачи защищаемой медицинской информации. Разрешение должно быть в письменной форме, включать в себя специфические структурные элементы, включая информирование пациента о его правах, а также быть оформлено в виде отдельного документа и подписано пациентом или его законным представителем. Дополнительные

[161] U.S. Department of Health & Human Services [Site]. – https://ncvhs.hhs.gov/wp-content/uploads/2018/05/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf (accessed: 30.07.2018).

[162] 45 CFR 160.103 - Definitions [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/cfr/text/45/160.103 (accessed: 09.08.2018).

требования к вышеназванным применяются в случаях, если осуществляется продажа такой информации, использование её в маркетинговых целях и т.д.

Кроме разрешения законодательство США оперирует понятием согласие (consent). Например, согласно ст. 23 Закона о недискриминации генетической информации[163] хранитель образцов ДНК и генетической информации, намеревающийся передать образцы, должен уведомить пациента о том, что последний имеет право на (1) дачу согласия на такую передачу, на (2) возврат образцов пациенту, а также на (3) уничтожение образцов. В случае если пациент не дал знать о своем намерении в течение 3 месяцев, хранителем может быть осуществлена передача генетического материала или информации.

Передача чувствительных данных, к которым относятся данные о здоровье, осуществляется только с разрешения пациента или его законного представителя. Дополнительных требований к трансграничной передаче таких данных в законодательстве США не имеется. Было несколько законодательных инициатив по введению требований о локализации персональных данных в США перед трансграничной передачей, однако до сих пор они не были поддержаны[164].

В следующих случаях согласие субъектов на передачу данных не требуется:

(1) оказание медицинской услуги и ее оплата, а также закрытый перечень иных операций в сфере здравоохранения (например, сертификация и лицензирование специалистов и учреждений здравоохранения)[165];

(2) в случае передачи информации бизнес-партнеру (лицу, на которое распространяется действие HIPPA, не требуется получать согласие, когда он делится медицинской информацией с деловым партнером, предоставляющим юридические, финансовые и иные услуги. Контракт под названием «партнерское соглашение» создает правовые отношения между обязанным лицом и деловым партнером. Бизнес-партнер не имеет права использовать или раскрывать данные в противоречие с партнерским соглашением или HIPAA);

(3) в иных случаях, прямо предусмотренных законом, например, использование и

[163]Genetic Privacy and Non-discrimination Bill 1998 [2002] First Reading [Electronic resource] // Australian Government. The Federal Register of Legislation [Site]. – URL: https://www.legislation.gov.au/Details/C2004B01325 (accessed: 30.07.2018).

[164]Nigel Cory Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? – May 1, 2017 [Electronic resource] // The Information Technology and Innovation Foundation (ITIF) [Site]. – URL: https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost (accessed: 30.07.2018).

[165] 45 CFR 160.103 - Definitions [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/cfr/text/45/160.103 (accessed: 09.08.2018).

раскрытие информации для отчетности в области общественного здравоохранения; раскрытие информации о жертвах жестокого обращения или насилия в семье; раскрытие информации для проведения инициации судебных и административных процедур; раскрытие информации для правоохранительных органов; использование и раскрытие информации для исследовательских целей; использование и раскрытие информации для предотвращения серьезной угрозы здоровью.

Кроме того, лица, на которые распространяется действие HIPPA, могут использовать или раскрывать ограниченный набор данных (*медицинская информация без идентификаторов*) для целей проведения исследования, поддержания общественного здравоохранения без получения согласия. Однако такое лицо должно заключить соглашение об использовании данных (data use agreement) с получателем данных, которое соответствует определенным стандартам[166].

HIPAA допускает определенные исключения для использования информации в публичных целях: данные пациента могут быть раскрыты государственным органам здравоохранения без разрешения пациента. В соответствии с HIPAA, поставщики могут раскрывать идентифицируемые данные пациента (защищенная медицинская информация), если это требуется по закону, позволяя государствам передавать законные исключения для ограничений HIPAA.

Разрешение для раскрытия информации не требуется для определенных государственных программ, связанных с социальным обеспечением или необходимых для получения государственного пособия, программ, когда обмен информацией предусмотрен или разрешен законодательством или постановлением.

В некоторых случаях предусмотрен отказ от права на медицинскую тайну пациентом, например, когда истец-пациент разрешает раскрытие конфиденциальной информации в той мере, в какой это необходимо для того, чтобы ответчик-врач разумно защищался от иска (*Jones v. Asheville Radiological Group*).

Законодательство США предусматривает, что с письменного разрешения физического лица возможна передача медицинской информации. HIPAA предусматривает, что разрешение должно быть дано самим субъектом или его представителем (personal representative) с указанием законного основания такого представительства. Однако исходя из

[166] 45 CFR § 164.514 (e) [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/cfr/text/45/164.514 (accessed: 09.08.2018).

систематического толкования термина «personal representative»[167] в HIPAA можно сделать вывод, что по умолчанию (1) им должно быть физическое лицо, (2) им должен быть родственник/законный представитель/представитель по медицинской помощи (health care agent). Важно подчеркнуть, что представитель по медицинской помощи в некоторых ситуациях, связанных с конкретным лечением, может быть назначен в качестве представителя, однако он должен быть ограничен в распоряжении только той информацией, которая ему стала доступна в рамках лечения: Департамент здравоохранения США подчеркивает, что лицо, подпадающее под действие HIPAA, не должно брать согласие у такого врача на распространение медицинской информации пациента в маркетинговых целях[168]. Специальных норм об идентификации субъектов, а также их представителей HIPAA и HITECH не содержат.

Широко известно, что в США используется подход, при котором возможно получение подразумеваемого согласия с возможностью последующего отказа от обработки персональных данных (opt-out), однако данный вид согласия не предусмотрен при обработке специальных видов персональных данных, к которым относятся сведения, составляющие медицинскую тайну. Как было указано в п. 3.2.9, законодательство США оперирует понятиями «согласие» (consent) и «разрешение» (authorization), которые являются формами получения согласий субъектов тайны на обработку сведений.

В отличие от иных законов США, затрагивающих проблемы информационной безопасности, HIPAA достаточно регламентирована, устанавливает конкретные административные, технические и физические гарантии обеспечения конфиденциальности, целостности и доступности защищаемых данных, которые они собирают, получают, хранят и/или передают[169]. В общем все меры можно перечлись следующим образом: лицо должно (1) обеспечить конфиденциальность, целостность и доступность информации; (2) защищать от любых разумно ожидаемых угроз или угроз безопасности или целостности информации; (3) защищать от любых разумно ожидаемых видов несанкционированного использования или раскрытия информации; а также (4) обеспечить соблюдение правил информационной

[167] 45 CFR 164.502(g) [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/cfr/text/45/164.502 (accessed: 09.08.2018).

[168] Personal Representatives [Electronic resource] // U.S. Department of Health & Human Services [Site]. – URL: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/personal-representatives/index.html (accessed: 30.07.2018).

[169] Cybersecurity in healthcare: A narrative review of trends, threats and ways forward [Electronic resource] // Northumbria Research Link (NRL) [Site]. – URL: http://nrl.northumbria.ac.uk/34336/ (accessed: 30.07.2018).

безопасности работниками такого юридического лица[170].

Сингапур

В Сингапуре понятие медицинской тайны прямо не закреплено в системе права, оно является составным и многоаспектным: медицинская информация подпадает под регулирование сразу нескольких законодательных актов, при этом ни один из них не имеет кодифицирующего характера.

Закон Medishield Life Scheme 2015 года[171], вводящий новую систему страхования здоровья граждан, - единственный закон, имеющий словосочетание «*медицинская информация*» в своем составе, при этом он не содержит нормы-дефиниции, но вводит этот термин как раздел внутри главы закона. Из систематического толкования можно сделать вывод, что медицинская информация – это вид конфиденциальной информации, хранящейся в медицинском учреждении или у конкретного врача после посещения пациентом.

К отношениям, связанным с медицинской тайной, применимо, в первую очередь, Законом о защите персональных данных (PDPA), который устанавливает основные правила обработки информации, относимой к персональным данным.

Специальное законодательство, регламентирующее медицинские правоотношения, не содержит общих норм и положений касательно информации, содержащей медицинские данные, кроме Закон о биомедицинских исследованиях (Human Biomedical Research Act 2015), о котором будет сказано далее.

При этом стоит отметить, что обезличенная медицинская информация, как указано в рекомендациях Министерства здравоохранения Сингапура,[172] не подлежит регламентации и свободна для распространения. Кроме того, в определённых ситуациях, например, в рамках проведения научного исследования, должны быть соблюдены все необходимые меры защиты информации: Министерство здравоохранения Сингапура указывает, что при работе ученого с

---

[170] U.S. Department of Health & Human Services [Site]. – https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf?language=es (accessed: 30.07.2018).

[171] Medishield Life Scheme Act 2015 [Electronic resource] // Singapore Statutes Online [Site]. – URL: https://sso.agc.gov.sg/Act/MLSA2015#pr27- (accessed: 30.07.2018).

[172] Ministry of Health Singapore Reflection on Transition [Electronic resource] // Ministry of Health Singapore [Site]. – URL: https://www.moh.gov.sg/content/dam/moh_web/Legislations/Legislation%20And%20Guidelines/HBRA/Reflection%20on%20Transition.pdf (accessed: 30.07.2018).

обезличенной информацией, ключ для расшифровки должен находится (1) у третьего лица *либо* (2) внутри самой медицинской организации, где происходит исследование, однако с ограничением доступа такого ученого к ключу, позволяющему идентифицировать лиц – субъектов персональных медицинских данных.

Однако информация, подпадающая под охрану медицинской тайны, понимается законодательством Сингапура шире, нежели медицинская информация, понимаемая в ключе законодательства о персональных данных. Исходя из логического толкования законодательства, к медицинской тайне относится любая информация, связанная с лечением, обследованием и профилактикой пациента. Этот вывод можно сделать, исходя из Закона о медицинской регистрации (Medical Registration Act), согласно которому вводятся ограничения на оборот конфиденциальной информации.

Некоторые должностные лица, к которым применяется упомянутый акт, не должны раскрывать какую-либо информацию, содержащуюся в каком-либо документе, которая, возможно, дошла до их сведения в ходе лечения и диагностики, если только раскрытие не будет сделано (а) в целях осуществления и обеспечения соблюдения вышеназванного закона или Закона о инфекционных заболеваниях; или (б) для любых других целей с согласия лица, к которому относится данная информация.

Та или иная информация понимается в качестве относящейся к медицинской тайне, исходя из конкретного рассматриваемого случая. Критерием формирования является отнесение признаков информации под критерий Medishield Life Scheme, хотя в доктрине нет единого мнения на этот счет.

Состав сведений, составляющих медицинскую тайну, ограничивается индивидуально идентифицируемой медицинской информацией. Важно учесть, что законодательство Сингапура, в отличие от ЕС и США, не учитывает разницы между «чувствительностью» данных[173], поэтому также методы и формы получения согласия субъекта персональных данных не зависят от вида данных[174].

Сведения, составляющие медицинскую тайну, могут одновременно охраняться как иные виды тайн или иметь статус информации ограниченного доступа по иным основаниям.

---

[173] Lee Soo Chye and Alvin Cheng Data protection in Singapore: overview [Electronic resource] // Thomson Reuters Practical Law [Site]. – URL: https://uk.practicallaw.thomsonreuters.com/6-579-6345?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1 (accessed: 30.07.2018).

[174] DLA Piper [Site]. – https://www.dlapiperdataprotection.com/index.html#handbook/world-map-section (accessed: 30.07.2018).

Закон о биомедицинских исследованиях (Human Biomedical Research Act 2015) вводит термин «индивидуально-идентифицированной» информации касательно биологического материала и медицинской информации, что включает в себя информацию, позволяющую идентифицировать лицо на основании (1) биологического материала или медицинской информации, или (2) биологического материала или медицинской информации и иной информации, из которой следует принадлежность к конкретному лицу, которая является доступной для исследовательского института, банка тканей или иной медицинской организации.

Министерство здравоохранения указывает, что этот термин полностью соотносится с общим законодательством о защите прав субъектов персональных данных[175].

Законодательство Сингапура оперирует понятием согласие (consent). Трансграничная передача медицинских данных не регламентирована специальными правилами. Законодательство Сингапура допускает определенные исключения для использования информации в публичных целях: данные пациента могут быть раскрыты государственным органам здравоохранения без разрешения пациента, согласно Infectious Diseases Act, Factories (Medical Examinations) Regulations, Immigration Act, Termination of Pregnancy Regulations, Private Hospitals and Medical Clinics Act, Enlistment Act, Prisons Regulations, Mental Disorders and Treatment Act, Misuse of Drugs Act.

К организациям, обрабатывающим сведения, относимые к медицинской тайне, предъявляются общие требования информационной безопасности.

Южная Корея

Специальных требований непосредственно к медицинской тайне в Корее не выявлено: в целом, регулирование совпадает с регулированием личной информации. Однако существует нормативный закон, регулирующий генетическую информацию: Закон «О биоэтике и безопасности» (Bioethics and safety Act). К генетической информации в соответствии с данным законом относится информация, полученная в результате анализа генетических особенностей человеческого материала лица.

[175] Ministry of Health Singapore Summary of Responses to Feedback Received During Public Consultation on Human Biomedical Research Bill [Electronic resource] // Ministry of Health Singapore [Site]. – URL: https://www.moh.gov.sg/content/moh_web/home/Publications/Reports/2015/summary-of-responses-to-feedback-received-during-public-consult.html (accessed: 30.07.2018).

Применительно к медицинской тайне остро стоит вопрос о возможности передачи такой информации при условии использования метода шифрования.

Делом, иллюстрирующим вопросы, связанные с шифрованием, является дело **Korean Pharmaceutical Association**, **the Korean Pharmaceutical Information Center, IMS Health Korea** рассмотренное в 2014 году.[176] Перед судом был поставлен вопрос о том, можно ли раскрывать личную информацию в случае, если такая информация зашифрована. Компании Korean Pharmaceutical Association, the Korean Pharmaceutical Information Center, без разрешения пациентов осуществляли сбор личной информации о здоровье пациентов, которые посещали их клиники. После сбора такая информация передавалась компании IMS Health Korea в зашифрованном виде. Суд принял решение против ответчика, поскольку пришёл к выводу, что уровень шифрования был недостаточно высоким, поэтому пользователей все ещё можно было идентифицировать. Таким образом, суд пришёл к выводу, что ответчик действительно нарушил право на медицинскую тайну пользователей, тем не менее, поскольку такая информация не вышла за пределы IMS Health Korea и не была использована для целей совершения преступления, суд пришёл к выводу об отсутствии оснований для взыскания убытков.[177]

Израиль

Врачебная тайна

Базовые положения о врачебной тайне содержатся в законе «О защите прав пациента», 1996 (Patient's rights act, 1996). Так, там установлен запрет на опубликование любых материалов, относящихся к личной жизни лица, включая его сексуальную жизнь, состояние здоровья или поведение на частной территории.

В статье 10 устанавливается, что врач, все лица, работающие под его началом, а также все иные сотрудники медицинского учреждения, должны соблюдать тайну личной жизни на всех стадиях осуществления лечения. При этом директор медицинского учреждения должен обеспечить соблюдение тайны на всех стадиях осуществления лечения.

В соответствии со статьёй 19 ФЗ «О медицинской помощи», лечащий врач или иной

[176] Seoul Central District Court, 2014godan5110. [Electronic resource] // Supreme Court of Korea [Site]. – URL: https://eng.scourt.go.kr/eng/judiciary/organization/courts3.jsp (accessed: 30.07.2018).

[177] Court takes side with druggists despite leakage of personal info [Electronic resource] // Korea Biomedical Review [Site]. – URL: http://www.koreabiomed.com/news/articleView.html?idxno=1345 (accessed: 30.07.2018).

сотрудник медицинского учреждения не должен раскрывать любую информацию, относящуюся к пациенту, которая попала в его распоряжение в связи с исполнением обязанностей или трудовой функции. Лечащий врач и, если речь идет о медицинском учреждении, директор медицинского учреждения должен сделать все необходимые приготовления, чтобы убедиться, что работники, находящиеся под его управлением, не раскрывали подобных сведений.

Генетическая информация

В Израиле существует отдельный закон, регулирующий вопросы, связанные с генетической информацией: Закон «О генетической информации», 5761-2000 (Genetic Information Law, 5761-2000).

Цель этого закона, в том числе, закрепить регулирование, обеспечить соблюдение прав на тайну личной жизни лица в связи с использованием генетической информации.

Генетическая информация это - любая информация, которая относится к генетической. Такая информация должна передаваться, раскрываться, храниться, использоваться в соответствии с положениями Закона «О генетической информации» (перечень сформулирован как открытый).

Порядок и условия передачи сведений, составляющих врачебную тайну, третьим лицам, а также аффилированным лицам и аудиторам

Врачебная тайна

Данный вопрос урегулирован в статьях 13, 20 закона «О медицинской помощи».

Обладатель базы данных может отказать в предоставлении информации лицу, если такой запрос относится к его физическому или психологическому здоровью и если такой запрос может нанести существенный вред здоровью такого лица либо поставить его жизнь под угрозу, владелец информации должен предоставить такую информацию врачу либо психологу лица.

По общему правилу, лечащий врач или сотрудник медицинского учреждения может передать медицинскую информацию о пациенте при наличии согласия пациента на передачу таких данных.

Генетическая информация

Лицо, которое получает генетическую информацию в отношении иного лица в рамках осуществления своих профессиональных обязанностей или в процессе устройства такого лица на работу, должно сохранять такую информацию в секрете и не использовать никаким

образом за исключением случаев, когда им было прямо получено согласие субъекта генетической информации при условии, что такое использование будет ограничено таким согласием.

Лицензиат, лицо, ответственное за проведение исследования, лечащий врач или лицо, предоставляющее генетическую консультацию, директор лаборатории для проведения генетических тестов, директор генетического института, лицо, принимающее участие в исследовании, должны предпринимать обоснованные меры для гарантирования того, что сотрудники, находящиеся под их руководством, соблюдают конфиденциальность в отношении вопросов, ставшим им известным в связи с исполнением их профессиональных обязанностей или в течение их трудоустройства.

Случаи, условия и порядок передачи сведений, составляющих тайну связи, третьим лицам без согласия субъектов тайны

Регулирование в отношении данного вопроса содержится в Законе «О защите парв пациента». Лечащий врач или сотрудник медицинского учреждения может передать медицинскую информацию без согласия пациента только в одном из следующих случаев: лечащий врач или сотрудник медицинского учреждения юридически обязан передать информацию; раскрытие информации производится в целях осуществления лечения другим врачом; в случае если информация не может быть раскрыта пациенту, поскольку может нанести ущерб его здоровью, и Этический Комитет одобрил раскрытие такой информации третьим лицам; Этический Комитет, после того как выслушал мнению пациента, пришел к выводу о необходимости раскрыть медицинскую информацию, поскольку такое раскрытие является необходимым для защиты здоровья иных лиц или общества, и такое раскрытие будет признано более приоритетным интересом по сравнению с нераскрытием; медицинская информация раскрывается медицинскому учреждению, осуществляющему лечение, либо кому-то из работников такого учреждения, и целью раскрытия информации является направление информации или внесение информации либо с целью направления уведомления, предусмотренного законом; раскрытие осуществляется с целью публикации в медицинском журнале либо для целей исследования в целях обучения в соответствии с распоряжением Министерства по данному вопросу, но при условии, что все детали, каким-либо образом идентифицирующие пациента, будут ликвидированы.

Информация будет раскрываться только в объеме, необходимом в данном конкретном случае, при этом должно быть сделано все возможное, чтобы скрыть личность пациента.

Также в законе предусмотрена возможность передачи информации о здоровье лица, находящегося под стражей, солдату, офицеру полиции, тюремному служащему, когда такая информация требуется для сохранения здоровья такого лица.

Генетическая информация

Лицензиат, лицо, ответственное за проведение исследования, лечащий врач или лицо, осуществляющее генетическое консультирование, директор генетического института и директор лаборатории для проведения генетического тестирования может передавать генетическую информацию другому лицу в соответствии с положениями статьи 20 Акта «О правах лиц» («The Subjects Rights Law») либо в соответствии со статьёй (a) (5) Акта с учётом соответствующих различий.

Лицо, обладающее генетической информацией или базой данных, содержащей генетическую информацию, может передавать такую информацию для целей легально одобренных исследований, обучения или публикации в научном журнале, при наличии одного из следующих условий:

(1) генетическая информация передается без раскрытия каких-либо идентифицирующих подробностей;

(2) субъект генетической информации дал согласие на в письменной форме на передачу генетической информации. В случае осуществлении публикации, никаких идентифицирующих признаков субъекта не допускается за исключением случаев, когда субъект прямо дал письменное предварительное согласие на такую публикацию.

Изъятия из режима охраны в социальных, государственных, экономических целях

Пациент имеет право отказаться от сохранения конфиденциальности медицинских данных о нем. Такой отказ осуществляется в письменной форме (“*Written Medical Confidentiality Waiver (Vasar)*”).

Лицо, в отношении которого пациент производит отказ, получает законный доступ к любым записям о здоровье пациента вне зависимости от того, относятся ли они к лечению в данный момент или нет.

Такой отказ может быть дан на любой срок, однако, пациент может указать и конкретный срок, на который дается отказ. При отказе в пользу организации, пациент также может сузить круг лиц, получающих доступ к информации.

Отказ от медицинской конфиденциальности в отношении медицинских записей или

медицинской информации не должен быть расценен как согласие на раскрытие генетической информации (Статья 22 закона о генетической информации).

Права и обязанности специальных категорий лиц (агентов, посредников, подрядчиков, в т.ч. юридических лиц, обслуживающих программно-аппаратные комплексы) в части доступа к сведениям, составляющим тайну связи, а также случаев такого доступа

В соответствии со статьей 20 закона «О генетической информации», лечащий врач и лицо предоставляющее генетическое консультирование могут предоставить генетическую информацию иному лечащему врачу или иному лицу, осуществляющему генетическое консультирование для целей лечения субъекта, за исключением случаев, когда субъект выразил свое несогласие с такой передачей. Однако даже при наличии возражений со стороны субъекта информация может быть передана иному лечащему врачу, если Этический Комитет после общения с субъектом генетической информации, придет к выводу о следующем:

(1) передача генетической информации в отношении субъекта необходима для подержания здоровья родственников или для поддержания здоровья самого субъекта, либо для предотвращения смерти, болезни или серьезному расстройству такого родственника, включая ещё не родившихся родственников.

(2) передача генетической информации является единственным способом для достижения целей, необходимых в соответствии пунктом (1);

(3) выгода, которую может получить родственник, в результе передачи генетической информации лечащему врачу является более значительной, чем вред, который будет нанесён субъекту в результате раскрытия такой информации либо причины, на основании которых субъект генетической информации выступает против раскрытия такой информации, являются незначительными.

Механизм правовой защиты субъектов состоит из следующих элементов:

(1) Раскрытие информации по общему правилу осуществляется только с согласия субъекта тайны;

(2) Круг субъектов, который может иметь доступ к тайне без согласия субъекта тайны, ограничен.

(3) Случаи, когда допускается разглашение сведений, составляющих тайну коммуникации, ограничены;

(4) Предусмотрена ответственность за неправомерное разглашение сведений, составляющих тайну.

Объединенные Арабские Эмираты

Законодательство ОАЭ не содержит понятия врачебной тайны. В то же время, в целом ряде законов предусмотрен запрет на раскрытие информации, относящейся к пациенту. При этом под законами в данном случае понимается все нормативное правовое регулирование за исключением законов шариата. Однако отметим, что законы шариата также требуют сохранение конфиденциальности и врачебной тайны[178].

В статье 13 Федерального закона №7 от 1975 года «О медицинской деятельности» (*On The Practice of Human Medicine Profession*)[179] указывается, что врач не вправе раскрывать личные секреты, связанные с его профессией, когда такие секреты стали известны ему от пациента, либо если он самостоятельно узнал их.

Аналогичное положение содержится и в ст. 5 Федерального закона о Медицинской ответственности №4 от 2016 года[180], согласно которой врачу запрещается разглашать любую конфиденциальную информацию, относящуюся к пациенту, которая становится известной в ходе лечения или вследствие осуществления лечения, независимо от того, сообщил ли такую информацию врачу сам пациент, либо же врач обнаружил такую информацию самостоятельно.

Законодательство ОАЭ не содержит принципов формирования сведений, составляющих врачебную тайну. Тем не менее, можно сформулировать следующие принципы на основании системного толкования применимых НПА:

---

[178] Islamic Medical Education Resources-03 0106-Medical Confidentiality. Lecture for Year 3 medical students on 25th June 2001 by Professor Omar Hasan Kasule [Electronic resource] // Islamic Medical Education Resources-03 [Site]. – URL: http://omarkasule-03.tripod.com/id695.html (accessed: 09.08.2018), G. Alahmad, K. Dierickx. What do Islamic institutional fatwas say about medical and research confidentiality and breach of confidentiality? [Electronic Resource] // Wiley Online Library [Site]. – URL: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1471-8847.2012.00329.x (accessed: 09.08.2018).

[179] Federal Law Concerning the Practice of human medicine profession [Electronic resource]: Federal Law No. 7 of 1975. // Dubai Health Authority [Site]. – URL: https://www.dha.gov.ae/Documents/Regulations/Federal%20laws/Federal%20Law%20No.%207-1975%20concerning%20the%20Practice%20of%20Human%20Medicine%20Profession.pdf (accessed: 09.08.2018).

[180] Federal Decree Law On Medical Liability [Electronic resource]: Federal Decree Law No.4 of 2016. // Dubai Health Authority [Site]. – URL: https://www.dha.gov.ae/Asset%20Library/MarketingAssets/20180611/(E)%20Federal%20Decree%20no.%204%20of%202016.pdf (accessed: 09.08.2018).

(1) Отнесение к врачебной тайне любых сведений, относящихся к пациенту;

(2) Открытый перечень сведений, относящихся к врачебной тайне;

Конкретный состав сведений не определен в законодательстве. К сведениям, не подлежащим раскрытию, относится любая информация, относящаяся к пациенту, независимо от того, узнал ли врач такую информацию от самого пациента, либо же самостоятельно обнаружил ее.

Сведения ограниченного доступа в процессе анализа не выявлены.

Поскольку в ОАЭ отсутствует законодательство о персональных данных, разграничить сведения, составляющие соответствующий вид тайны и сведения, составляющие персональные данные, не представляется возможным. Однако в ОАЭ есть несколько свободных экономических зон, на территории которых действуют свое законодательство.

Прежде всего, Закон о персональных данных №1 от 2007 г. (далее – Закон о ПД)[181] действует только на территории и в рамках деятельности свободной экономической зоны – Международного финансового центра Дубай (DIFC). Согласно положениям данного Закона персональные данные – это любые данные относящиеся к идентифицируемому физическому лицу. Таким образом, сведения, составляющие врачебную тайну, могут подпадать под общий запрет раскрытия информации, относящейся к врачебной тайне, а в части информации, которая относится к идентифицируемому физическому лицу, такие сведения будут являться персональными данными.

На территории свободной экономической зоны - Медицинский город Дубай также принято Постановление о защите медицинских данных №7 от 2013 г. (Постановление №7)[182]. Согласно ст.8 Постановления №7 оно применяется к следующей медицинской информации:

- информация о здоровье пациента, включая его историю болезни;

- информация о любых ограничениях физических возможностей, которые пациент имеет или имел;

- информация о медицинских услугах, которые предоставляются или предоставлялись пациенту;

- информация, предоставленная пациентом в отношении донорства, проведения

[181] Data Protection Law [Electronic resource] //: DIFC Law No. 2 of 2007. // Dubai International Financial Centre [Site]. – URL: https://www.difc.ae/files/3615/1739/8803/Data_Protection_Law_DIFC_Law_No._1_of_2007.pdf (accessed: 09.08.2018).

[182] Health Data Protection Regulation [Electronic resource]: DHCA Regulation No. 7 of 2013. // Dubai Healthcare City Authority [Site]. – URL: https://dhcr.gov.ae/AboutDHCRDocuments/10-Health%20Data%20Protection%20Regulation.pdf (accessed: 09.08.2018).

исследований;

- информация о пациенте, полученная ранее в связи с оказанием ему медицинских услуг.

В Постановлении №7 выделены две категории данных – медицинская информация пациента (любая информация, имеющая отношение к физическому и психическому здоровью пациента независимо от ее формы) и информация, идентифицирующая пациента (данные, относящиеся к пациенту, включая его полное имя, возраст, адрес и иную контактную информацию).

Механизм правовой защиты субъектов врачебной тайны заключается в наличии общего запрета раскрывать врачебную тайну и санкции за нарушение такого запрета.

Для территории DIFC дополнительно к этому механизм защиты содержится в Законе о ПД, согласно которому Комиссар по персональным данным в случае обнаружения нарушений в деятельности контролера персональных данных может выдать ему предписание:

(1) выполнить сформулированные в предписании действия, и (или)

(2) воздержаться от обработки любых персональных данных, указанных в предписании, либо воздержаться от обработки определенным способом или в определенных целях.

В случае, если контролер не выполнит требования предписания Комиссар может обратиться в Суд за получением одного или нескольких следующих приказов:

(1) приказ с требованием к контролеру персональных данных или его представителю соблюдать положения Закона или Постановления о персональных данных[183], либо иных нормативных актов, имеющих отношение к предписанию;

(2) приказ с требованием к контролеру персональных данных или его представителю оплатить любые расходы, понесенные Комиссаром или иным лицом в связи выдачей предписания или нарушения Закона, Постановления или иного нормативного правового акта, имеющего отношение к предписанию;

(3) любой иное приказ, который Суд сочтет необходимым.

Под Судом в данном случае понимается Суд DIFC, специально созданный в

[183] Data Protection Regulation (DPR) [Electronic resource]: DIFC Consolidated Version No. 3 (in force on 31.01.2018) // Dubai International Financial Centre [Site]. – URL: https://www.difc.ae/files/4515/1745/7405/Data_Protection_Regulations.pdf (accessed: 09.08.2018).

соответствии с Законом Дубай[184].

Кроме того, субъект персональных данных в соответствии с п.1 ст.34 Закона может подать жалобу Комиссару на нарушение его прав, связанных с обработкой персональных данных. Если субъект персональных данных понес ущерб в связи с нарушением, допущенным в отношении него контролером персональных данных, субъект может обратиться в суд с требованием о выплате компенсации такого ущерба (ст.38 Закона).

На территории Медицинского города Дубай также закреплены механизмы защиты прав. Так, пациент или его представитель могут подать жалобу Комиссару с жалобой на нарушение закона, вмешательство в информацию, идентифицирующую пациента.

Юридическая ответственность наступает на основании ст. 379 Уголовного кодекса ОАЭ, согласно которой любое лицо, которому в силу профессии, навыков, обстоятельств или умений была доверена тайна и которое раскрывает ее в случаях, не разрешенных законом, или который использует тайну для своей выгоды или выгоды другого лица, наказывается, если лицо, к которому относится эта тайна, не было согласно на раскрытие или использование тайны[185].

При этом понятие «тайны» является вопросом факта. Применительно к вопросу о понятии «тайна» отсутствуют какие-либо рекомендации судебных органов[186].

В случае нарушения требований Закона о ПД DIFC ответственность может наступать в виде штрафа. Перечень оснований привлечения к ответственности и размеры штрафов содержатся в Приложении №2 к Закону о ПД. Например, за обработку специальных категорий персональных данных без получения разрешения Комиссара штраф составляет 10, 000 долларов.

В Конституции ОАЭ отсутствуют положения, связанные с защитой тайны личной жизни (за исключением ст.31 о свободе почтовой переписки, передачи телеграфных сообщений и прочих средств связи). В связи с этим выявить соотношение конституционных прав не представляется возможным.

---

[184] DIFC Court Law [Electronic resource] //:DIFC Law No. 10 of 2004. // Dubai International Financial Centre [Site]. – URL: https://www.difc.ae/files/1914/5448/9176/Court_Law_DIFC_Law_No.10_of_2004.pdf (accessed: 09.08.2018).

[185] Federal Law No. (3) of 1987 Promulgating the Penal Code [Electronic resource] // LEGAL ADVICE MIDDLE EAST [Site]. – URL: https://legaladviceme.com/legislation/117/uae-federal-law-3-of-1987-promulgating-penal-code (accessed: 09.08.2018).

[186] N. O'Connell. Privacy in a UAE Healthcare Context. February 2014 [Electronic resource] // AL TAMIMI & CO. [Site]. – URL: https://www.tamimi.com/law-update-articles/privacy-in-a-uae-healthcare-context/ (accessed: 09.08.2018).

Не федеральном уровне порядок и условия передачи сведений, составляющих врачебную тайну, отсутствуют. В то же время соответствующее регулирование содержится в Законе о ПД DIFC и Постановлении №7 DHCC.

В ст.37 Постановления №7 DHCC указываются, в том числе, следующие случаи раскрытия медицинской информации пациента:

- это разрешено пациентом, или его представителем (если пациент умер или не может выразить волю);

- если это прямо необходимо для достижения целей, для которых такая информация была получена;

- это необходимо для предотвращения или уменьшения угрозы для общественного здоровья или безопасности общества, или жизни и здоровья пациента или другого лица;

- для целей оказания помощи в экстренных ситуациях, перемещения пациента, планирования выписки пациента и обеспечения координации при оказании пациенту медицинских услуг. При этом такая информация может быть раскрыта Лицензированному медицинскому работнику или представителю нетрадиционной медицины, который предоставляет медицинские услуги пациенту;

- представителю, близкому родственнику, супругу, детям и т.д. предоставляется общая информация о нахождении пациента на территории DHCC, либо сведения о факте смерти;

- для целей статистики. При этом не допускается публикация данных в такой форме, которая может идентифицировать пациента;

- для целей проведения исследований (также может быть необходимо получить разрешение этического комитета). Кроме того, не допускается публикация данных в такой форме, которая может идентифицировать пациента;

- для целей профессиональной аккредитации медицинских услуг. При этом не допускается публикация данных в такой форме, которая может идентифицировать пациента, а также раскрытие данных третьим лицам, за исключением случаев, прямо предусмотренных законом.

Раскрытие указанной выше информации допускается только в тех пределах, в которых это необходимо для достижения определенной цели. Помимо этого, когда раскрытие осуществляется в указанных выше случаях лицензиат (физическое лицо, оказывающее медицинские услуги и имеющее лицензию) обязано, как только это практически осуществимо, уведомить пациента или его представителя о раскрытии информации. В случае

если раскрываемая информация относится к жалобе пациента на лицензиата – уведомить Центр качества DHCC о раскрытии медицинской информации пациента. Лицензиат освобождается от соблюдения требований, если человек мертв более 15 лет, а кроме того, если источник медицинской информации о пациенте является общедоступным.

Отдельные положения касаются раскрытия информации, идентифицирующей пациента (то есть, персональных данных) (ст.38 Постановления №7), а именно: это разрешено пациентом или его представителем, когда пациент не в состоянии дать согласие; если это прямо связано с целью, с которой такая информация была получена; необходимо для предотвращения или уменьшения угрозы для общественного здоровья или безопасности общества, или жизни и здоровья пациента или другого лица.

В федеральном законодательстве отсутствуют прямые запреты для трансграничной передачи сведений, составляющих медицинскую тайну.

В Постановлении №7 DHCC речь идет только о передаче медицинской информации пациента третьему лицу, находящемуся вне юрисдикции DHCC. Такая передача допустима, только если к такому третьему лицу применяются регулирование, требующее обеспечивать адекватный уровень защиты медицинской информации пациента, и если такая передача разрешена пациентом или это необходимо для непрерывного предоставления пациенту медицинских услуг.

В ст.68 Постановления делается указание, что юрисдикция будет считаться обеспечивающей адекватный уровень защиты информации, если она будет указана в качестве таковой в Законе о ПД DIFC или если есть письменное одобрение Центрального органа управления. Перечень допустимых юрисдикций содержится в Постановлении о персональных данных DIFC. На сегодня туда включены: страны ЕС, а также Уругвай, Канада, Аргентина, Андорра, Гернси, о. Мэн, Фарерские острова. Россия не включена в перечень.

Некоторые упоминаемые выше случаи раскрытия данных, относящихся к врачебной тайне, осуществляются без согласия пациента. При этом говоря о дополнительных таких случаях раскрытия, необходимо указать следующее. Федеральный закон №7 от 1975 года «О медицинской деятельности» предусматривает несколько случаев, когда допускается раскрывать личные тайны пациента без его согласия. В частности:

(а) разглашение тайны было запрошено заинтересованным лицом;

(б) разглашение тайны служит интересам как мужа, так и жены, и разглашается им

индивидуально;

(в) цель разглашения тайны заключается в том, чтобы избежать совершения преступления. В этом случае тайна может быть разглашена только заинтересованным органам;

(г) врач относится к одной из страховых компаний и участвовал в осмотре пациента (то есть одного из клиентов компании). В этом случае секрет может быть раскрыт только соответствующей страховой компании.

В пункте 6 статье 5 Закона № 4 от 2016 года «О медицинской ответственности» в дополнение к указанным выше случаям раскрытия личных тайн пациента (подпункт «б», «в»), также предусматриваются несколько дополнительных случаев, когда допускается раскрывать личные тайны пациента. В частности:

(а) когда врач был назначен судебным органом или публичным следственным органом ОАЭ в качестве эксперта или если такой врач был уведомлен об участии его в качестве свидетеля в расследовании или уголовном судопроизводстве; и

(б) если врач был нанят на проведение экспертизы страховой компанией или их работодателями.

(в) когда раскрытие осуществляется по запросу органов здравоохранения с целью защиты общественного здоровья в соответствии с условиями и средствами контроля, изложенными в исполнительных положениях Закона №4 от 2016 г.;

(г) если цель раскрытия связана с защитой врача перед следственными органами или иным судебным органом, когда такая защита может потребоваться.

Изъятия из режима врачебной тайны в целях обеспечения возможности обработки накопленных данных для достижения социальных (вкл. повышения уровня здоровья населения), государственных, экономически целей не установлены.

Говоря о случаях и порядке раскрытия сведений, составляющих врачебную тайну, в том числе, в форме открытых данных, и принципа раскрытия данных по умолчанию в деятельности органов государственного управления, необходимо отметить следующее. Статистические сведения (открытые данные) публикуются на сайте Министерства здравоохранения ОАЭ[187], а также в специальной базе данных, портале официальных данных

[187] UAE Ministry of Health & Prevention [Electronic resource] // Ministry of Health & Prevention. United Arab Emirates [Site]. – URL: http://www.mohap.gov.ae/en/OpenData/Pages/default.aspx (accessed: 09.08.2018).

Правительства ОАЭ - Bayanat.ae[188]. Как утверждается на портале, он создан в целях продвижения подхода к цифровой экономике, основанной на знаниях. Управлением и поддержкой базы занимается Федеральное управление по конкуренции и статистики (FCSA).

Кроме того, Законом Дубай №26 от 2015 года[189]? на уровне эмирата Дубай создана специальная система данных - Dubai Open and Shared Data[190]. Закон является одним из элементов глобальной стратегии Дубай – Smart Dubai[191].

Open Data – это данные, которые предоставляются государственными органами, а также юридическими лицами и могут распространяться без ограничений, либо с минимальными ограничениями, установленными компетентным органом. Shared Data (совместно используемые данные) – это любые данные, не являющиеся открытыми данными. Такие данные, принадлежащие государственным органам, должны быть доступны для совместного использования или повторного использования (с определенным уровнем контроля в зависимости от того, квалифицируются ли такие данные как конфиденциальные, специальные или секретные как это указывается в Подходе к классификации данных Дубай[192]). В частности, используется следующая схема:

[188] Bayanat.ae [Electronic resource] // Bayanat [Site]. – URL: http://data.bayanat.ae/en_GB/dataset?tags=health (accessed: 09.08.2018).

[189] Regulating Data Dissemination and Exchange in the Emirate of Dubai [Electronic resource]: Dubai Law No. 26 of 2015 // The Supreme Legislation Committee [Site]. – URL: http://ogp.dubai.gov.ae/documants/pdf/ltiwndiymjezmdk.pdf (accessed: 09.08.2018).

[190] Open & Shared Data Framework [Electronic resource] // Dubai Data Manual [Site]. – URL: http://dubaidata.ae/open-and-shared-data-framework.html (accessed: 09.08.2018).

[191] Smart Dubai [Electronic resource] // Smart Dubai [Site]. – URL: https://smartdubai.ae/en/Pages/default.aspx (accessed: 09.08.2018).

[192] Dubai Data Classification Framework [Electronic resource] // Dubai Data [Site]. – URL: http://www.dubaidata.ae/pdf/Classification-Framework.pdf (accessed: 09.08.2018).

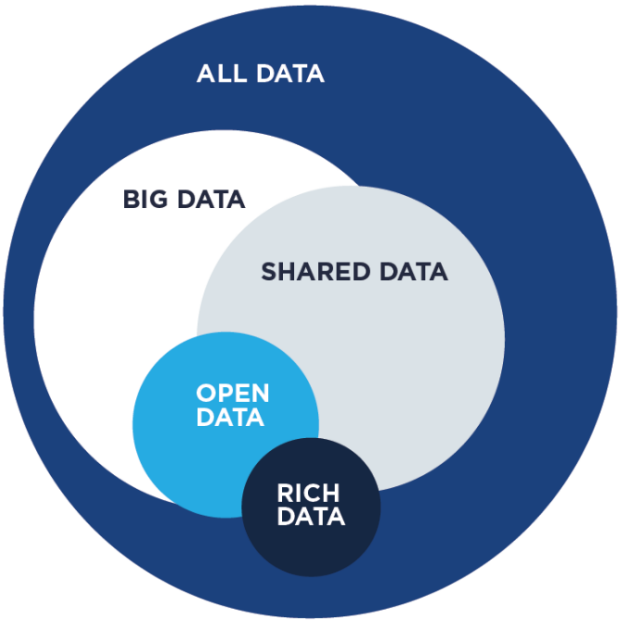

Рис. 2. Соотношение различных видов данных.

Data - любой организованный или неорганизованный набор параметров, фактов, понятий, инструкций, наблюдений или измерений, которые могут быть интерпретированы, могут быть раскрыты, обработаны.

Rich Data – данные, в которые превращаются Big Data после более глубокого, качественного анализа, извлечения информации. Как правило, отвечает на вопросы - «Почему?».

Open Data - данные, публикуемые государственными органами или организациями частного сектора, которые будут открыто использоваться физическими лицами или третьими лицами.

Shared Data - данные, предоставляемые для совместного использования и повторного использования среди организаций, с соблюдением определенных условий.

Big Data - чрезвычайно большие объемы данных, которые могут быть проанализированы для выявления моделей, тенденций и ассоциаций. Как правило, отвечает на вопрос - «Что?».

В Подходе к классификации данных Дубай сформулирована классификация данных по уровню «открытости» данных. То есть, на каком уровне, каким лицам и с какими ограничениями такие данные могут быть доступны. Помимо этого, на примере схемы описан поток таких данных. Для определения того, каким образом классифицировать данные создан

специальный инструмент, в котором сформулированы критерии, по которым производится оценка уровня влияния - от незначительного до высокого. Например, это критерий негативного влияния на частную жизнь физических лиц, конкуренцию, общественное здоровье или безопасность и т.д.

Для реализации данной инициативы разработан подробный план действий[193].

В Законе Дубай №26 от 2015 года указаны обязанности государственных органов, среди которых, есть следующее: разработка плана распространения данных, обеспечение качества данных и их периодическое обновление, изменение инфраструктуры (программного обеспечения, оборудования для электронного распространения и обмена данными). Помимо этого, предусматриваются разнообразные функции уполномоченного органа (то есть уполномоченного на реализацию положений данного Закона). В частности, это функции по подтверждению политик, стандартов, правил, форм, рекомендаций, инструкций распространения и обмена информацией. Кроме того, именно данный орган определяет провайдеров данных среди государственных органов и иных лиц.

Важно отметить, что провайдеры данных при раскрытии и распространении данных должны предпринимать все необходимые меры для защиты конфиденциальности и частной жизни, защищаемых на основании закона данных потребителей (ст.13 Закона Дубай №26 от 2015 года). В качестве одного из ключевых принципов работы данной системы предусмотрено, что конфиденциальность частной жизни физических лиц должна соблюдаться и по общему правилу должна иметь приоритет перед желанием классифицировать какой-либо набор данных в качестве Открытых данных. Однако, могут быть и случаи, когда права на конфиденциальность частной жизни будут ограничены общественными интересами в классификации какого-либо набора данных в качестве Открытых данных[194].

Возможность доступа третьих лиц к врачебной тайне с согласия субъекта раскрыта выше.

Возможность администрирования согласий субъектов врачебной тайны на обработку сведений, составляющих врачебную тайну, и их передачу третьим лицам (в т.ч. наличие права субъекта определять порядок использования таких сведений, делегирования права на

[193] Dubai Open and Shared Data Framework [Electronic resource] // Dubai Data [Site]. – URL: http://dubaidata.ae/pdf/Dubai-Open-Shared-Data-Framework-20170427.pdf (accessed: 09.08.2018).

[194] Dubai Data Strategy. Strategic Objectives [Electronic resource] // Dubai Data [Site]. – URL: http://dubaidata.ae/dubai-data-strategy.html (accessed: 09.08.2018).

выдачу согласий, отзыва согласий на их сбор, обработку и/или передачу и т.д.), а также специальных норм (при их наличии) по идентификации субъектов тайн (в т.ч. их законных представителей) в целом не предусмотрена.

Исключение составляет возможность изъявления согласия (разрешения) на раскрытие медицинских данных пациента или информации, идентифицирующей пациента его представителем на основании ст. 37, 38 Постановления №7 DHCC в случае, когда пациент умер или не может самостоятельно выразить такое согласие.

Форма, способ получения согласия субъекта врачебной тайны на обработку сведений, составляющих врачебную тайну, и/или их передачу третьим лицам (в т.ч. письменно, посредством электронной подписи, совершения конклюдентных действий и проч.), порядок фиксации и хранения подтверждений получения согласий (в т.ч. числе сроков их хранения) не законодательно определены.

В отношении требований к информационной безопасности при сборе, обработке, передаче, хранении сведений, составляющих врачебную тайну, включая требования к надежности систем обработки и хранения данных можно отметить следующее.

Согласно ст.31 Постановления №7 DHCC лицензиат несет ответственность за безопасность информационных систем и сетей и обязан:

(1) действовать своевременно для предотвращения, обнаружения и реагирования на инциденты, связанные с безопасностью;
(2) осуществлять обзор и оценку безопасности информационных систем и сетей и вносить соответствующие изменения в политику, практику, меры и процедуры безопасности на регулярной основе; а также
(3) периодически сообщать об инцидентах нарушения безопасности Подразделению по защите информации DHCC.

1.3. Банковская тайна

Российская Федерация

Понятие, принципы формирования и юридическая ответственность за нарушение. Банковская тайна включает сведения об операциях, о счетах и вкладах клиентов

кредитных организаций[195] и корреспондентов клиентов, а также иные сведения, устанавливаемые кредитной организацией, если это не противоречит федеральному закону (ст. 26 Закона о банках и банковской деятельности).

Принципы формирования сведений, составляющих банковскую тайну, в Законодательстве прямо не определены. Тем не менее, на основании релевантной судебной практики можно сформулировать следующие принципы:

(1) Гарантия тайны личной жизни. Отнесение сведений, раскрытие которых может привести к раскрытию тайны личной жизни в части финансового положения лица и иных деталей, касающихся его личной жизни;

(2) Обеспечение условий для эффективного функционирования банковской системы;

Перечень сведений, составляющих банковскую тайну, открытый.

Следующие сведения составляют банковскую тайну:

(1) Информация о клиентах кредитной организации и о корреспондентах клиентов;

(2) Информация об операциях, счетах и вкладах клиентов и корреспондентов (ст. 26 Закона о банковской тайне);

(3) Иные сведения, которые отнесены к банковской тайне внутренними документами кредитной организации.

Сведения, составляющие банковскую тайну, могут одновременно охраняться как иные виды тайн или иметь статус информации ограниченного доступа по иным основаниям, в том числе:

(1) Сведения о денежных переводах одновременно охраняются как тайна связи;

(2) Сведения о клиенте и его корреспонденте - как персональные данные;

(3) Сведения о вкладах, счетах, операциях по счету и иная подобная информация – как тайна личной жизни;

(4) Одни и те же сведения могут оставлять налоговую и банковскую тайну ;

(5) Сведения, предоставленные аудиторским компаниям, приобретают статус аудиторской тайны и Законом об аудиторской деятельности (ст. 9 Закона об аудиторской деятельности).

Как предусмотрено выше, некоторые сведения, составляющие банковскую тайну, могут одновременно охраняться как тайна связи или как тайна личной жизни. Сведения,

[195] Здесь и далее под кредитной организацией понимаются все субъекты, на которых возложена обязанность по сохранению банковской тайны, включая Банк России и организацию по страхованию вкладов.

составляющие банковскую тайну, переданные органам власти для исполнения ими возложенных на них обязанностей, могут переходить в правовой режим другого вида тайны (служебную, аудиторскую, государственную тайны). Защита прав субъектов банковской тайны обеспечивается наличием юридической ответственности разных видов за нарушение банковской тайны.

За нарушение тайны связи предусмотрены следующие виды ответственности:

(1) Уголовная ответственность в виде штрафа в размере до одного миллиона пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, обязательных работ на срок до четырехсот восьмидесяти часов, либо принудительных работ на срок до пяти лет, либо лишения свободы на срок до пяти лет (ст. 183 УК РФ).

(2) Административная ответственность в соответствии со ст.13.11 КоАП (нарушение законодательства об обработке персональных данных), ст. 13.14 КоАП (за разглашение сведений конфиденциального характера лицом, получившим доступ к таким сведениям с использованием служебного положения). Отдельный состав именно за нарушение банковской тайны КоАП не предусмотрен.

(3) Гражданско-правовая ответственность на основании исков о компенсации морального вреда, возмещения убытков, причинении вреда.

КС РФ рассматривает банковскую тайну как частный случай тайны личной жизни. Соответственно, ее ограничение возможно только на условиях и в порядке, которые предусмотрены ст. 55 Конституции РФ, то есть только на основании федеральных законов. Важные правовые позиции по вопросу соотношения высказал КС РФ (Постановление от 14 мая 2003 года N 8-П; Определение от 14 декабря 2004 года N 453-О. Предусмотренные в законе отступления от банковской тайны не могут быть произвольным. Такие отступления (в частности, предоставление банками, иными кредитными организациями и их служащими сведений о счетах и вкладах и операциях по счету, а также сведений о клиентах государственным органам и их должностным лицам) должны отвечать требованиям справедливости, быть адекватными, соразмерными и необходимыми для защиты конституционно значимых ценностей, в том числе частных и публичных прав и интересов граждан, не затрагивать существо соответствующих конституционных прав, т.е. не ограничивать пределы и применение основного содержания закрепляющих эти права

конституционных положений, и могут быть оправданны лишь необходимостью обеспечения указанных в статье 55 (часть 3) Конституции Российской Федерации целей защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов других лиц и общественной безопасности.

В отличие от иных видов тайн состав сведений, составляющих банковскую тайну, определен в достаточной степени и не содержит оценочных и описательных категорий, которые бы требовали дополнительного толкования. Тем не менее, некоторые авторы отмечают, что имеется коллизия между нормами ГК РФ и Законом о банках, определяющим состав сведений, составляющих банковскую тайну: Закон о банках и банковской деятельности содержит более широкий круг информации[196]. Однако на практике фактический состав сведений, относящийся к банковской тайне, редко бывает предметом спора.

Предоставление третьим лицам. Порядок предоставления сведений, составляющих банковскую тайну, урегулирован в статье 26 Закона о банковской тайне. В основном, данная статья предусматривает случаи и условия предоставления таких сведений различным государственным органам и организациям для исполнения их функций. Среди таких органов налоговые органы, Пенсионный Фонд России, суд, ФСС и т.д. Данная статья прямо предусматривает возможность предоставления сведений, составляющих банковскую тайну, в головную кредитную организацию (управляющую компанию) банковского холдинга, аудиторским организациям. В литературе случаи предоставления банковской тайны по порядку и форме принято делить следующим образом: а) по специальным запросам гос. органов, б) в составе отчетной и иной обещающей документации, в) в порядке уведомления, в силу предписания закона комитету по финансовым рынкам[197]. Каких-либо специальных условий передачи сведений названным организациям Закон о банках и банковской деятельности не содержит (помимо головных организаций, расположенных на территории иностранных государств,). Закон о банках и банковской деятельности не содержит положений и условий предоставления сведений, составляющих банковскую тайну, третьим лицам (таким как коммерческие организации) на основании согласий клиентов и т.д. Из судебной практики следует вывод о том, что сведения, составляющие банковскую тайну,

[196] Алексеева Д.Г. Банковское право: Учебник. М.: Юристъ, 2007. – 357 с., Маркелова К.А. Особенности банковской тайны как правовой категории // Банковское право. М.: Юрист, 2001. – 47 с.

[197] См., например, Селивановский А.С. Банковская тайна: состояние и проблемы [Электронный ресурс] // Авторские курсы А.С. Селивановского [Сайт]. – URL: http://selivanovsky.ru/pages/bankovskaya_tajna/ (дата обращения: 08.08.2018).

могут передаваться третьим лицам при уступке прав требования без согласия клиентов (см., например, Постановление Федерального арбитражного суда Московского округа от 23 марта 2005 г. N КГ-А40/1704-05, Информационное письмо Президиума ВАС РФ от 13.09.2011 N 146).

Напрямую вопрос возможности предоставления банковской тайны третьим лицам с согласия самого субъекта Законодательством не урегулирован. Соответственно, подробно не определены формы согласий, порядок их предоставления и администрирования. В той части, в которой сведения, составляющие банковскую тайну, включают персональные данные, порядок предоставления согласий определяется Законом о персональных данных (то есть согласие должно быть конкретным, информированным и сознательным, должны соблюдаться и иные требования).

Порядок использования банковской тайны также регулируется Законом об информации, из которого следует, что обладатель информации, коим является клиент банка, может по своему усмотрению разрешать использование таких данных (ст. 2, ст. 6 Закона об информации). Препятствием в использовании могут стать положения Закона о персональных данных, которые ограничивают использование целями их обработки. В этой связи в отношении любого вида использования, напрямую не связанного с банковским обслуживанием, вероятно, целесообразно получать не только согласие, но и оформлять соглашение об использовании данных.

Отдельно стоит отметить, что Закон о банках предусматривает специальные случаи предоставления сведений, составляющих банковскую тайну, аффилированным лицам банка без согласия клиента. В частности:

(1) Кредитные организации, являющиеся участниками банковской группы, участниками банковского холдинга и иных объединений с участием кредитных организаций, ***в целях составления отчетности банковской группы, банковского холдинга и иных объединений с участием кредитных организаций***, в том числе для определения рисков, принимаемых на консолидированной основе, разработки и поддержания в актуальном состоянии планов восстановления финансовой устойчивости, ***представляют соответственно в головную кредитную организацию банковской группы, головную организацию (управляющую компанию)*** банковского холдинга и иного объединения с участием кредитных организаций ***сведения о своих***

операциях и об операциях своих клиентов и корреспондентов.

(2) Кредитные организации также вправе предоставить сведения, составляющие банковскую тайну (если такие сведения одновременно не составляют государственную тайну), головным кредитным организациям банковских групп, головным организациям (управляющим компаниям) банковских холдингов, ***расположенным на территориях иностранных государств, при условии обеспечения этими иностранными государствами уровня защиты*** (соблюдения конфиденциальности) предоставляемой информации не меньшего, чем уровень защиты (соблюдения конфиденциальности) предоставляемой информации, предусмотренный законодательством Российской Федерации.

Важно отметить, что в случае отсутствия такой специальной нормы, предусматривающей возможность предоставления аффилированным лицам, такое предоставление могло быть затруднительным. Связано это с тем, что в отсутствие специальных правил основным источником регулирования порядка получения согласий на обработку личной информации является Закон о персональных данных. При этом Закон о персональных данных не делает различий между аффилированными лицами оператора персональных данных и просто иными третьими лицами. Аффилированные лица также считаются третьими лицами и предоставление им информации является раскрытием такой информации. Соответственно, для законного предоставления персональных данных третьим лицам необходимо соблюсти целый ряд требований, предусмотренных Законом о персональных данных, что может быть довольно обременительным. Оценивая возможность, случаи и объемы предоставления кредитными учреждениями конфиденциальных данных, полученных или сформированных при выполнении требований административного законодательства, например, о противодействии отмыванию преступных доходов, правоохранительным органам и иным органам власти, не указанным в таком административном законодательстве, например, в силу общих полномочий указанных органов власти, отметим, что законодательство не содержит правил предоставления таких сведений другим органам власти, за исключением положений о международном обмене информацией с органами власти иностранных государств и в целях предотвращения коррупции (ст.8 и 10 Закона о противодействии легализации). Логическое и телеологическое толкование Законодательства позволяет сделать вывод о том, что полученные в рамках

исполнения служебных обязанностей сведения конфиденциального характера должны использоваться исключительно в таких служебных целях и продолжают охраняться как налоговая, банковская и иные виды тайн, либо переходят в иной режим охраны – аудиторская, государственная и т.п. (см., например ст. 8 Закона о противодействии). При этом запросы о предоставлении соответствующих сведений должны направляться не «вторичным держателям», которые получили их в рамках исполнения своих обязанностей (если иное не предусмотрено законом), а к тем организациям, которые получили их изначально.

Относительно предоставления сведений, подготовленных кредитными организациями в соответствии с законодательством о противодействии отмыванию доходов, полученных пресутпным путем, государственным огранам и должностным лицам, не уполномеченным осуществлять соответсвующий контроль, можно отметить следующее. Как было указано выше, судебная практика и КС РФ относит банковскую тайну к разновидности тайны личной жизни. Соотвествнно, ограничения банковской тайны возможны строго в случаях и в порядке, которые предусмотрены федеральными законами. В этой связи, по общему правилу, кредитные организации не обязаны предоставлять информацию, передаваемую Росфинмониторингу, иным государственным органам. Такая позиция подтверждается судебной практикой. В одном из своих решений ВС РФ высказал следующую правовую позицию:

«*Статья 26 Федерального закона от 2 декабря 1990 года N 395-1 "О банках и банковской деятельности" (далее - Закон N 395-1), регулирующая порядок предоставления банками справок по операциям и счетам их клиентов, содержит исчерпывающий перечень лиц, которые вправе получать от банков информацию, составляющую банковскую тайну. При этом органы Прокуратуры РФ и их должностные лица не указаны в данном перечне.*

Специальные федеральные законы, регламентирующие деятельность конкретных органов, могут содержать нормы, предусматривающие право этих органов получать информацию, составляющую банковскую тайну.

Федеральный закон от 17 января 1992 года N 2202-1 "О прокуратуре Российской Федерации" (далее - Закон N 2202-1) не содержит норм, предоставляющих органам Прокуратуры Российской Федерации и их должностным лицам право получать от банков информацию, относящуюся к банковской тайне».

На этом основании ВС РФ признал незаконным привлечение к ответственности

сотрудника банка, который отказался выдать прокуратуре сведения, составляющие банковскую тайну. Таким образом, обяазнность предоставить сведения, составляющие банковскую тайну, может вытекать исключительно из прямого указания федерального закона. Например, общие формулировки, предусмотренные профильными законами, по нашему мнению, не должны считаться основанием предоставления сведений, составляющих банковскую тайну[198].

Между тем, на наш взгляд, необходимо различать ситуации, когда тот или иной орган не указан среди государственных органов, имеющих право на получение сведений составляющих банковскую тайну (как, например, органы прокуратуры), и ситуации, когда соответсвующий орган вправе получать сведения, составляющие банковскую тайну (как, например, налоговые органы). Во втором случае юридический анализ законности требования государственного органа является более сложной задачей. Строго формально и те государственные органы, которые вправе получать сведения, составляющие банковскую тайну, вправе получать эти свдения в порядке, в форме и в объемах, которые установлены в федеральном законе. Такую точку зрения высказывают и соответсвующие государственные органы (см., например, Ответ Министерства Финансов РФ от 28.12.2005 № 03-02-07/1-350 на Письмо АРБ «О предоставлении ФНС России информации, связанной с осуществлением контроля в области ПОД/ФТ»[199]). Если объем информации, запрашиваемый государственным органом, превышает ту информацию, которую государственный орган вправе запросить, кредитная организация вправе отказать в предоставлении информации. Если запрос является немотивированным, кредитная организация также вправе отказться от предоставления информации. В случае, если запрос государственного органа является мотивированным и объем запрашиваемой ифнормцаии не превыашет предусмотренынй законодательством, то, вероятно, необходимо пресдставить соответсвующию информацию (даже если форма запроса не соответсвует, указанной в законе), соотнеся риски привлеченяи к ответсвтенности за отказ в предоставлении информации и, например, за разглашение мер, принимаемых в соответсвии с законодательством о противодействии легализации доходов, полученных преступным путем.

Таким образом, на данный момент законодательство не является в достаточной

[198] За исключением случаев, когда в таких законах прямо предусмотрено, что соответсвующие органы вправе запрашивать у банков (иных кредитных организаций) соответсвующую информацию.

[199] В данном письме ФНС прямо не отвечает на запрос АРБ, но высказвает позицию о том, что запрос налоговых органов должен быть мотивированным.

степени формально определенным в части порядка, объема и формы представления третьим лицам сведений, составляющих банковскую тайну. По этой причине кредитные организации сталкиваюся со сложностями в части определения обязанности и порядка предоставления соответсвующих сведений третьим лицам. Учитвая, что за разглашение банковской тайны предусмотрена не только администраитвная (ст. 13.14 КоАП), но и уголовная ответсвенность (ст. 183 УК РФ), такая неопределенность порождает существенные правоые риски. КС РФ в постановлениях неоднократно высказывался относительно формальной определенности нормативно-правовых актов и предусмотренных в них обязанностей (см., например, Постановление Конституционного Суда РФ от 10.07.2017 N 19-П, Постановление Конституционного Суда РФ от 08.04.2014 N 10-П).

Обзор требований в части соблюдения информационной безопасности, предусмотренные для банков и иных кредитных организаций. Учитывая специфику деятельности кредитных организаций, утечка или доступ к информации кредитных организаций может нанести серьезный ущерб интересам клиентов. В этой связи к информационной безопасности в банковской сфере предъявляются довольно строгие требования, которые вытекают из специального регулирования.

Условно требования в области информационной безопасности банков (кредитных учреждений) можно разделить на две группы:

1. Специальные требования, предъявляемые к банкам и иным кредитным организациям. Такие требования содержатся в целом ряде НПА, в том числе:
   - Законодательные требования предусмотрены в Законе о национальной платежной системе (ст. 27);
   - «**Стандарт Банка России** «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014». Положения стандарта применяются банками на добровольной основе;
   - **Постановление Правительства РФ от 13.06.2012 № 584** «Об утверждении Положения о защите информации в платежной системе»;
   - «**Положение о требованиях к обеспечению защиты информации** при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (утв. Банком

России 09.06.2012 N 382-П). Как указывают некоторые авторы: «В положении помимо изложенных программных, технических и информационных требований к оператору по переводу денежных средств предъявляются и иные (организационные) требования, направленные на защиту информации. Их фактическая суть сводится к необходимости постоянного мониторинга оператором по переводу денежных средств технического состояния сети банкоматов и терминалов, обеспечения возможности информирования об их неработоспособности третьими лицами, обеспечение регулярного технического обслуживания объектов инфраструктуры уполномоченными сотрудниками, определяет порядок работы с поступающей информацией о выявленных сбоях»[200];

- **Указание Банка России от 10 декабря 2015 г. № 3889-У** «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных»;
- **Положение Банка России от 24 августа 2016 г. № 552-П** «О требованиях к защите информации в платежной системе Банка России»
- Специальные требования к программному обеспечению, подробнее см. на сайте Банка России http://www.cbr.ru/mcirabis/itest/.

2. Общие требования, вытекающие из положений о защите персональных данных и т.д. Данные требования совпадают с таковыми в отношении иных операторов обработки персональных данных.

Заслуживает внимания репрезентативная ***судебная практика Российской Федерации и ЕСПЧ*** по вопросам обработки и защиты информации, составляющей соответствующие виды тайн. В частности, можно отметить следующие судебные решения.

Определение Конституционного Суда РФ от 27.06.2017 N 1338-О. Гражданина Постникова А.П., обращаясь в КС РФ, ставил под сомнение конституционность ч.4ст. 26 Закона о банках, определяющая круг лиц, которым представляются справки о движении денежных средств на счете без согласия клиента кредитной организации. По мнению Постникова А.П., указанная норма носит неопределенный характер. КС РФ отклонил жалобу

[200] Войтенков Е.А. О некоторых вопросах практической реализации требований по защите информации в кредитных организациях при работе с банкоматами и платежными терминалами // Банковское право. – 2016. – № 1. – С. 31 - 34.

и указал следующее:

(1) Закрепление в законе отступлений от банковской тайны не может быть произвольным; такие отступления (в частности, предоставление банками, иными кредитными организациями и их служащими сведений о счетах и вкладах и операциях по счету, а также сведений о клиентах государственным органам и их должностным лицам) должны отвечать требованиям справедливости, быть адекватными, соразмерными и необходимыми для защиты конституционно значимых ценностей, в том числе частных и публичных прав и интересов граждан, не затрагивать существо соответствующих конституционных прав.

(2) Часть 4 ст. 26 Закона о банках, с учетом разъяснений, ВС РФ о том, что запрос справки о движении по счетам денежных средств, не требует предварительного судебного решения (п. 10 Постановление ВС РФ от 1 июля 2017 г. №19), не содержит какой-либо неопределенности в вопросе о том, относятся ли справки по счетам и вкладам физических лиц к числу тех сведений, составляющих банковскую тайну, которые могут предоставляться кредитной организацией органам предварительного следствия по делам, находящимся в их производстве, при наличии согласия руководителя следственного органа, и как таковое конституционные права заявителя, указанные в жалобе, не нарушает.

Определение Конституционного Суда РФ от 27.06.2017 N 1337-О. По своему содержанию данное определение и высказанные в нем позиции аналогичны тем, что высказаны в определении, процитированном выше.

Определение Конституционного Суда РФ от 22.11.2012 № 2192-О. Гр. Леоновой Н.Н. было отказано в возбуждении уголовного дела по ст. 183 УК РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», поскольку сведения о кредитном договоре относится к служебной, а не банковской тайне. Суды поддержали позицию следственных органов. Гражданка Леонова Н.Н. обратилась в КС РФ с жалобой о признании неконституционной ст. 26 Закона о банках и банковской деятельности в той мере, в которой она не относит к банковской тайне содержание кредитного и/или иного договора с банком.

КС РФ не нашел оснований для признания ст. 26 неконституционной, отметив, что казуальное толкование положений этой статьи к его компетенции не относится. Таким образом, КС РФ не обозначил свою позицию в вопросе о том, относятся ли сведения о

договоре к банковской тайне.

Постановление ВС РФ от 20 апреля 2016 г. № 309-АД16-2859. Управление антимонопольной службы по Иркутской области обжаловало решения нижестоящих судов, которые отменили решение о привлечении к административной ответственности банка, который отказался выдать выписку по расчетному счету. Данная информация запрашивалась антимонопольным органом для расследования дела о нарушении законодательства о рекламе.

ВС РФ согласился с судами, отметив, что антимонопольная служба не перечислена в ст. 26 Закона о банках среди тех субъектов, которые вправе запрашивать информацию, составляющую банковскую тайну, без согласия клиента банка. Данное решение имеет большое значение, поскольку закрепляет принцип о недопустимости установлений изъятий в отношении банковской тайны, кроме тех которые прямо и явно установлены в законе (главным образом, в Законе о банках).

Постановление Верховного Суда РФ от 27 февраля 2013 г. № 32-АД12-4. Лицо обратилось в ВС РФ с надзорной жалобой об отмене решения о привлечении к административной ответственности в соответствии со ст. 17.7 КоАП. (невыполнение законных требований прокурора).

ВС РФ отменил решение о привлечении к административной ответственности.

По мнению суда, органам прокуратуры информация, составляющая банковскую тайну, предоставляться не должна, т.к. об этом прямо не сказано в ст. 26 Закона о банках. В ходе разрешения ВС РФ опирался на следующие важные правовые позиции:

(1) Из конституционных гарантий неприкосновенности частной жизни, личной тайны и недопустимости распространения информации о частной жизни лица без его согласия вытекают как право каждого на сохранение в тайне сведений о его банковских счетах и банковских вкладах и иных сведений, виды и объем которых устанавливаются законом, так и соответствующая обязанность банков, иных кредитных организаций хранить банковскую тайну, а также обязанность государства обеспечивать это право в законодательстве и правоприменении.

(2) Институт банковской тайны по своей природе и назначению имеет публично-частный характер и направлен на обеспечение условий для эффективного функционирования банковской системы и гражданского оборота, основанного на свободе его участников, одновременно данный институт гарантирует основные права граждан и защищаемые Конституцией РФ интересы физических и

юридических лиц. Этим должны предопределяться устанавливаемые федеральным законодателем объем и содержание правомочий органов государственной власти и их должностных лиц, являющихся носителями публичных функций, в их отношениях с банками, иными кредитными организациями и их клиентами, а также объем и содержание прав и обязанностей клиентов в их отношениях как с банками, иными кредитными организациями, являющимися носителями финансовой информации, так и с органами государственной власти и их должностными лицами, могущими лишь в целях реализации указанных функций пользоваться банковской тайной, затрагивая тем самым частную жизнь и личную тайну граждан.

(3) Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям; государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и в порядке, предусмотренных законом.

Определение Верховного Суда РФ от 12.02.2018 N 308-КГ17-22368 по делу № А22-3929/2016. В данном определении ВС РФ, поддержав решения судов нижестоящих инстанций, поддержал важную правовую позицию о том, что в отношении лицевых счетов, открытых казначейством в целях исполнения бюджета по получателю РГУ «КУВ», в силу статьи 46 Федерального закона от 10.07.2002 N 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», статей 2, 26 Закона о банках распространяется общий режим банковской тайны.

Информационное письмо Президиума ВАС от 13.09.2013 №146 и Постановление Федерального арбитражного суда Московского округа от 23 марта 2005 г. N КГ-А40/1704-05. Приведенные судебные акты подтверждают правовую позицию о том, что не является нарушением банковской тайны предоставление сведений, составляющих банковскую тайну, коллекторским и иным организациям, не имеющим статуса кредитной организации, при уступке прав требования из кредитных и иных подобных договоров (в случае с потребителями советующее право на уступку должно быт прописано в договоре).

Европейский союз

В большинстве стран институт банковской тайны регулируется положениями

специального законодательства, регулирующего банковскую деятельность в целом. «В то же время, в других странах, источники правового регулирования в данной сфере основываются на традиции и административной практике (хотя в последние годы наметилась тенденция их дополнения законодательными положениями). А в странах с общей системой права действует принцип, в соответствии с которым конфиденциальность отношений между банком и клиентом происходит из контрактных обязательств между банком и клиентом»[201]. По мнению одних авторов, право на сохранение в тайне банковских данных лиц проистекает из права на неприкосновенность частной жизни (*right to privacy*), а в случае с юридическим лицом – из основ его правового статуса[202]. По мнению других – представляет собой договорное обязательство между банком и клиентом[203]. По общему правилу, сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям, а также государственным органам в случаях, предусмотренных законом, в частности, например, в рамках противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (далее - «AML/CFT»).

В целом же вопрос установления режима банковской тайны и его пределов решается в каждом государстве-участнике ЕС самостоятельно. На практике это ведет к трудностям, например, при несовпадении оснований и условий раскрытия сведений, составляющих банковскую тайну в различных государствах в рамках мероприятий по AML/CFT. Например, в некоторых странах ЕС банки не могут раскрывать сведения клиента его материнской компании, если клиент не находится под подозрением и не предоставил свое согласие на такое раскрытие. В других раскрытие сведений допускается, только если это оправдано принципом «необходимого знания» (*need-to-know principle*) и т.д[204]. Оценить уровень защиты банковских данных в отдельных государствах можно, в том числе, с помощью публичных

---

[201] Банковская тайна и налоговое администрирование в странах Европы (часть 2). Законодательные регулирование института банковской тайны в ЕС и ряде других европейских стран [Электронный ресурс] // Taurus Group [Сайт]. – URL: http://taurus-group.eu/ru/news/bankovskaya-tajna-i-nalogovoe-administrirovanie-v-stranax-evropy-chast-2/ (дата обращения: 30.07.2018).

[202] Vishnevskiy A. Bank Secrecy: a Look at Modern Trends from a Theoretical Standpoint [Electronic resource] / Vishnevskiy A. Право в современном мире. // Право. Журнал Высшей школы экономики [Сайт]. – URL: https://law-journal.hse.ru/data/2016/01/13/1134662079/%D0%B2%D0%B8%D1%88%D0%BD%D0%B5%D0%B2%D1%81%D0%BA%D0%B8%D0%B9.pdf (accessed: 30.07.2018).

[203] Booysen S., Neo D. Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres Around the World. - Cambridge University Press, 2017. – 32 P.

[204] Compliance with the anti-money laundering directive by cross-border banking groups at group level – Commission Staff Working Paper – Commission of the European Communities – Brussels, 30.6.2009 – [Electronic resource] // European Commission [Site]. – URL: http://ec.europa.eu/internal_market/company/docs/financial-crime/compli_cbb_en.pdf (accessed: 30.07.2018).

сервисов по типу *Financial Secrecy Index*[205].

Последние тенденции, выразившиеся в принятии и подписании многими государствами ЕС Многостороннего соглашения об автоматическом обмене финансовой информацией (*Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information (MCAA)*), способствовали распространению новостей об отмене банковской тайны как института в целом. Данный документ предусматривает, что финансовые институты всех стран-участниц собирают определенную информацию о своих клиентах (физических и юридических лицах), далее передают информацию в налоговые органы своей страны, затем между налоговыми органами происходит обмен данными. Финансовыми учреждениями в рамках такого обмена являются любые финансовые учреждения страны: банки, брокеры, депозитарии, страховые и др. компании, за исключением правительственных учреждений, международных организаций, центральных банков, государственных пенсионных фондов. Реализация на практике Многостороннего соглашения означает, что автоматический обмен налоговой информацией будет осуществляться на основе разработанного ОЭСР стандарта автоматического обмена информацией о финансовых счетах (*Common reporting standard*, или *CRS*), которым установлены содержательные и технические детали процесса обмена информацией. Тем не менее, в данном случае речь идет только о передаче финансовых данных и обмене ими только между налоговыми структурами и не затрагивает иные аспекты банковской тайны.

На уровне ЕС имеются положения в актах различного уровня о необходимости сохранения сотрудниками финансовых и надзорных учреждений служебной тайны в отношении сведений, которые стали им известны. В статье 37 Устава Европейского Центрального Банка[206] (далее - «ЕЦБ») содержатся положения о том, что члены руководящих органов и персонал ЕЦБ и национальных центральных банков, даже после прекращения своих функций, обязаны не разглашать информацию, которая по своему характеру охватывается профессиональной тайной. Данная обязанность распространяет силу на лиц, которые имеют доступ к данным, подпадающим под действие законодательства Евросоюза, предписывающего хранить тайну. Положения об установлении режимы служебной тайны

[205] Financial Secrecy Index [Electronic resource] // Tax Justice Network [Site]. – URL: https://www.financialsecrecyindex.com/introduction/fsi-2018-results (accessed: 30.07.2018).

[206] Протокол об Уставе Европейской системы центральных банков и Европейского центрального банка (в редакции Лиссабонского договора от 13 декабря 2007 г.) [Электронный ресурс] // Право Европейского Союза [Сайт]. – URL: http://eulaw.ru/treaties/protoc/4 (дата обращения: 30.07.2018).

содержатся во многих директивах, регулирующих различные аспекты банковской деятельности. Например, в Директиве N 2013/36/ЕС Европейского парламента и Совета Европейского Союза «О доступе к осуществлению деятельности кредитными организациями и пруденциальном надзоре за кредитными организациями и инвестиционными компаниями <…>»[207] установлено, что «на всех лиц, которые работают в компетентных органах, а также на аудиторов и экспертов, действующих от имени компетентных органов, распространяется обязательство по соблюдению профессиональной тайны. Конфиденциальная информация, которую такие лица, аудиторы или эксперты могут получать в ходе осуществления их обязанностей, может быть раскрыта только в краткой или обобщенной форме, препятствующей идентификации отдельной кредитной организации, без ущерба случаям, к которым применяется уголовное законодательство»[208]. Разрешается обмен информацией с контролирующими и некоторыми иными органами в установленных случаях.

В равной степени к сфере банковского дела применимы требования законодательства об обработке персональных данных. Во исполнение Регламента Европейского парламента и Совета ЕС 45/2001 от 18.12.2000 «О защите физических лиц при обработке персональных данных, осуществляемой учреждениями и органами Сообщества, и о свободном обращении таких данных» ЕЦБ было принято Решение от 17 апреля 2007[209] об учреждении должности Ответственного за обработку данных (*Data Protection Officer*), его прав и обязанностей.

Таким образом, можно сказать, что на уровне ЕС банковская тайна обеспечивается преимущественно за счет установления режима служебной тайны для работников соответствующих кредитных и контролирующих структур и режима обработки персональных данных клиентов. Особое внимание уделяется регулированию на уровне ЕС единообразных для всех государств-участников правил по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

---

[207] О доступе к осуществлению деятельности кредитными организациями и пруденциальном надзоре за кредитными организациями и инвестиционными компаниями, вносящая изменения в Директиву 2002/87/ЕС и отменяющая Директивы 2006/48/ЕС и 2006/49/ЕС [Электронный ресурс]: директива Европейского парламента и Совета Европейского Союза. – № 2013/36/ЕС – 26.06.2013. – Доступ из справ.-правовой системы «Консультант Плюс». (дата обращения: 30.07.2018).

[208] О доступе к осуществлению деятельности кредитными организациями и пруденциальном надзоре за кредитными организациями и инвестиционными компаниями, вносящая изменения в Директиву 2002/87/ЕС и отменяющая Директивы 2006/48/ЕС и 2006/49/ЕС / Там же

[209] Adopting implementing rules concerning data protection at the European Central Bank [Electronic resource]: Decision of the European central bank – 17 April 2007. // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32007D0001(01)&qid=1532761299631 (accessed: 30.07.2018).

Пределы раскрытия банковской тайны при расследовании AML/CFT преступлений определяет Конвенция Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма[210]. В соответствии со ст. 7 каждая сторона принимает такие законодательные и иные необходимые меры, предоставляющие компетентным органам полномочия принимать решения об истребовании/изъятии банковских, финансовых или коммерческих документов в целях выполнения действий, предусмотренных Конвенцией. Сторона не вправе отказаться выполнять положения настоящей статьи на основании банковской тайны. В целях идентификации и отслеживанию доходов, сбору соответствующих доказательств допускается наблюдение, перехват телекоммуникационных сообщений, доступ к компьютерным системам и постановления о представлении конкретных документов. В соответствии с рекомендациями Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) законодательство о защите банковской тайны не должно препятствовать реализации рекомендаций[211] ФАТФ.

Первая европейская директива о противодействии легализации таких доходов была принята в 1990 году и предусматривала сбор данных о будущем клиенте в целях проведения предварительной проверки его благонадежности. В дальнейшем регулирование было существенно изменено и на сегодняшний день включает в себя:

1. Директиву Европейского Парламента и Совета Европейского Союза 2015/849 от 20 мая 2015 г. «о предотвращении использования финансовой системы для целей отмывания денег или финансирования терроризма <...>» (далее - «Директива 2015/849»)[212];

2. Регламент № 2015/847 Европейского парламента и Совета Европейского Союза «Об информации, сопровождающей переводы денежных средств, и об отмене Регламента (ЕС)

[210] Конвенция Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма [Электронный ресурс]: в г. Варшаве 16.05.2005. – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 30.07.2018).

[211] Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения [Электронный ресурс]: Рекомендации ФАТФ – февраль 2012. // The Financial Action Task Force (FATF) [Сайт]. – URL: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Russian.pdf (дата обращения: 30.07.2018).

[212] О предотвращении использования финансовой системы для целей отмывания денег или финансирования терроризма, об изменении Регламента (ЕС) 648/2012 Европейского парламента и Совета ЕС и об отмене Директивы 2005/60/ЕС Европейского парламента и Совета ЕС и Директивы 2006/70/ЕС Европейской комиссии [Электронный ресурс]: директива Европейского парламента и Совета Европейского Союза. – № 2015/849 – 20.05.2015. – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 30.07.2018).

1781/2006» (далее - «Регламент 2015/847»)[213].

Принятие Директивы 2015/849 свидетельствовало о тенденции на ужесточение норм в области AML/CFT и в целом было направлено на повышение прозрачности корпоративной и финансовой информации. Среди основных положений Директивы 2015/849 можно выделить:

1. создание органов финансовой разведки в каждом государстве-члене ЕС (*Financial Intelligence Units,* или *FIUs*), которым обеспечивается своевременный доступ к финансовой, административной и правоприменительной информации, которая необходима им для надлежащего выполнения их обязанностей;

2. установления круга обязанных субъектов, таких как кредитные организации, финансовые институты и др., на которых возлагаются обязательства по идентификации клиентов, предоставлению информации FIU, как по запросу, акт и по собственной инициативе, если они знают или подозревают, что денежные средства, независимо от их объема, являются доходом от преступной деятельности или связаны с финансированием терроризма;

3. требования к раскрытию информации о бенефициарных владельцах компаний. Указанная информация должна храниться в каждой стране ЕС централизованно и быть доступна их национальным компетентным органам;

4. усиление полномочий компетентных органов стран ЕС по применению мер ответственности.

26 апреля 2018 года Европарламентом и Советом ЕС были приняты поправки к действующему регулированию, а именно «Директива 2018/843/EU Европейского Парламента и Совета Европейского Союза о внесении поправок в Директиву 2015/849/EU о предотвращении использования финансовой системы для отмывания денег и финансирования терроризма, а также о внесении поправок в Директивы 2009/138/ЕС и 2013/36/EU» (далее - «Директива 2018/843/EU»). Данные поправки нацелены на дальнейшее повышение прозрачности транзакций и снижение уровня анонимности пользователей, в том числе, при обороте виртуальных валют (криптовалют) и использовании виртуальных кошельков и предоплаченных карт. Среди основных нововведений Директивы 2018/843/EU следует назвать:

[213] Об информации, сопровождающей переводы денежных средств, и об отмене Регламента (ЕС) 1781/2006 [Электронный ресурс]: регламент Европейского парламента и Совета Европейского Союза. – № 2015/847 – 20.05.2015 – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 30.07.2018).

1. доступ к информации о бенефициарных владельцах компаний, содержащейся в специальных централизованных реестрах бенефициаров, теперь должен быть предоставлен любому желающему;

2. запрет на предоставление анонимных банковских сейфов (ячеек) (*anonymous safe-deposit box*). Их нынешние владельцы должны быть идентифицированы не позднее 10 января 2019 года, но в любом случае до момента использования ими таких сейфов (ячеек) тем или иным способом;

3. расширен круг обязанных субъектов, на которых налагаются обязательства по идентификации и проверке благонадежности своих клиентов, к ним теперь относятся «провайдеры электронных кошельков» (*custodian wallet providers*) и «платформы обмена виртуальных валют» (*virtual currency exchange platforms*);

4. усилены полномочия компетентных органов финансовой разведки;

5. дополнены критерии квалификации третьих стран (не членов ЕС) как «высоко-рискованных», транзакции с гражданами которых должны осуществляться в особом порядке. Перечень таких стран утверждается Еврокомиссией.

В качестве одной из основных законодательных тенденций следует назвать постоянное расширение возможностей для обмена финансовой информацией между органами финансовой разведки, а также другими правоприменительными органами, основной целью которого является ускорение процедур расследования финансовых правонарушений, включая правонарушения, носящие трансграничный характер[214].

Обработка персональных данных в целях предотвращения отмывания денег или финансирования терроризма осуществляется в соответствии с GDPR и считается вопросом общественного интереса в значении GDPR. Применительно к вопросам раскрытия информации и обработки персональных данных следует отметить также следующие ключевые моменты.

1. Статья 37 Директивы 2015/849 закрепляет, что «добросовестное раскрытие информации обязанным субъектом в соответствии с Директивы не является нарушением каких-либо ограничений на раскрытие информации, предусмотренных каким-либо договором или законодательным, регулятивным или административным положением, и не влечет за

[214] Anti-money laundering and counter terrorist financing [Electronic resource] // European Commission [Site]. – URL: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing_en (accessed: 30.07.2018).

собой какой-либо ответственности для обязанного субъекта, если они точно не осознавали преступный характер лежащей в основе деятельности»[215].

2. Одновременно обязанные субъекты не должны раскрывать клиентам или иным третьим лицам факт передачи информация для целей анализа на предмет отмывания денег или финансирования терроризма. Запрет не распространяется на раскрытие информации компетентным органам или в целях правоприменения. Запрет также не препятствует передаче информации между кредитными организациями и финансовыми институтами или между такими организациями и их филиалами и дочерними компаниями с контролирующим участием, расположенными в третьих странах, а также между аудиторами, бухгалтерами-ревизорами, налоговыми консультантами, нотариусами и др. указанными субъектами при выполнении их профессиональных обязанностей.

3. Обязанные субъекты должны хранить документы и информацию по проверке клиентов и сделок в целях осуществления FIU или иными компетентными органами их профессиональных обязанностей, включая расследование потенциальных случаев отмывания денег или финансирования терроризма. По истечении периодов хранения, обязанные субъекты должны уничтожать персональные данные, если иное не предусмотрено национальным законодательством. «Государства-члены ЕС вправе позволять или требовать дальнейшего хранения данных, если после проведения ими тщательной оценки необходимости и соразмерности такого дальнейшего хранения они сочтут его оправданным в целях предотвращения, выявления и расследования случаев отмывания денег или финансирования терроризма. Такое дальнейшее хранение не должно превышать дополнительного пятилетнего периода.»[216]

4. Обработка персональных данных в соответствии с настоящей Директивой 2015/849 регулируется положениями GDPR. Персональные данные должны обрабатываться исключительно в целях предотвращения отмывания денег или финансирования терроризма и обработка не должна осуществляться каким-либо образом, несовместимым с указанными целями. Обработка на основе Директивы 2015/849 в коммерческих и иных целях запрещена.

---

[215] О предотвращении использования финансовой системы для целей отмывания денег или финансирования терроризма, об изменении Регламента (ЕС) 648/2012 Европейского парламента и Совета ЕС и об отмене Директивы 2005/60/ЕС Европейского парламента и Совета ЕС и Директивы 2006/70/ЕС Европейской комиссии / Там же.

[216] О предотвращении использования финансовой системы для целей отмывания денег или финансирования терроризма, об изменении Регламента (ЕС) 648/2012 Европейского парламента и Совета ЕС и об отмене Директивы 2005/60/ЕС Европейского парламента и Совета ЕС и Директивы 2006/70/ЕС Европейской комиссии / Там же.

5. Обязанные субъекты должны предоставить новым клиентам информацию, требуемую в соответствии с GDPR, до установления правоотношений или заключения сделок и уведомить о правовых обязательствах таких субъектов в соответствии с Директивой 2015/849 по обработке персональных данных в целях предотвращения отмывания денег или финансирования терроризма.

6. «Применяя запрет на раскрытие информации, государства-члены ЕС могут ограничить права субъекта данных на доступ к персональным данным, относящимся к нему или к ней, в той степени, в которой такое ограничение представляет собой необходимую и соразмерную меру в демократическом обществе с должным учетом законных интересов заинтересованного лица в целях: (a) предоставления обязанным субъектам или компетентным национальным органам возможности надлежащим образом выполнить свои задачи в целях настоящей Директивы; или (b) недопущения воспрепятствования официальным или правовым запросам, анализам, расследованиям или процедурам, а также устранения рисков для предотвращения, расследования и выявления отмывания денег и финансирования терроризма.»[217]

Если рассматривать вопрос банковской тайны с точки зрения регулирования конфиденциальности расчетов, то некоторые общие принципы можно обнаружить в Рекомендациях № R (90) 19 от 13 сентября 1990 г. о защите персональных данных, используемых для платежей и связанных с ними операций. В частности, в ст. 2 устанавливается, что *privacy* должна обеспечиваться при сборе, использовании, хранении и иной обработке персональных данных, связанных с осуществлением платежей. С этой целью платежные организации, бенефициары и операторы сетей связи обязаны принять меры для обеспечения конфиденциальности таких данных. В Рекомендациях закрепляются требования к сбору, хранению, использованию и передаче, включая трансграничную передачу, данных, связанных с осуществлением платежей. По общему правилу передача данных, используемых для осуществления платежей, осуществляется для целей исполнения обязательств, установленных законом, для целей обеспечения законных интересов органов, осуществляющих платежные операции, с прямого информированного согласия субъекта данных, а также системами, формирующими отчеты об ошибках в платежах.

[217] О предотвращении использования финансовой системы для целей отмывания денег или финансирования терроризма, об изменении Регламента (ЕС) 648/2012 Европейского парламента и Совета ЕС и об отмене Директивы 2005/60/ЕС Европейского парламента и Совета ЕС и Директивы 2006/70/ЕС Европейской комиссии / Там же.

На уровне ЕС применительно к расчетам необходимо отметить Директиву 2015/2366/ЕС[218] (далее - «PSD2»), так называемую вторую директиву об оказании платёжных услуг, направленную на расширение конкуренции на рынке платёжных услуг и гармонизацию законодательства о защите прав потребителей и о правах и обязанностях компаний, предоставляющих платёжные услуги и их пользователей. Директива вступила в силу 12 января 2016 года и до 13 января 2018 года страны-члены ЕС обязаны были привести национальное законодательство в соответствие с новыми нормами. Одним из ключевых изменений PSD2 является возможность предоставления доступа к счету клиента, открытому у другого оператора по переводу денежных средств внешним операторам платежных услуг, а также использовать информацию о денежных средствах на счете. Одновременно на операторов по переводу денежных средств возлагается обязанность предоставлять внешним операторам доступ в свои системы. PSD2 устанавливает правила и условия предоставления доступа к финансовой информации клиента, которые, в том числе, включают в себя необходимость получения предварительного согласия плательщика на передачу информации в ответ на запрос со стороны конкретного оператора, предоставление строго ограниченного набора сведений, обеспечение недоступности персонализированных параметров доступа клиентов третьим лицам и осуществление передачи таких данных по защищенным и исправным каналам связи и др. Таким образом, внешнему оператору платежных услуг может быть предоставлен доступ только к информации, необходимой для выполнения поручения. В частности, внешним операторам может быть предоставлена только информация о наличии денежных средств на счете, а агрегаторам финансовой информации - информация, согласованная плательщиком в объеме, необходимом для оказания услуги. В качестве меры обеспечения безопасности платежей операторы по переводу денежных средств обязаны применять процедуру многофакторного удостоверения личности клиента (так называемую многофакторную аутентификацию) при отправке плательщиком распоряжения о переводе денежных средств по электронным каналам связи. PSD2 также регламентирует ответственность между банком плательщика и оператором по оформлению платежных поручений.

[218] On payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC – Directive (EU) of the European parliament and of the Council – No. 2015/2366 – November 25, 2015 – [Electronic resource] // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366 (accessed: 30.07.2018).

Что касается вопросов ***информационной безопасности,*** то помимо отдельных положений в директивах, приведенных в настоящем разделе, также необходимо отметить и общее регулирование, применимое ко всем информационным системам ЕС. В частности, необходимо выделить Директиву N 2016/1148 Европейского парламента и Совета Европейского Союза «О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза» (далее - «Директива NIS»)[219]. Данная Директива возлагает на все государства-члены ЕС обязательства по принятию национальной стратегии по обеспечению безопасности сетевых и информационных систем; по назначению национальных компетентных органов, единого контактного пункта и CSIRTs с возложением на них задач по обеспечению безопасности сетевых и информационных систем, а также устанавливает требования к операторам основных услуг и провайдерам цифровых услуг по обеспечению безопасности и уведомлению.

«Обмен конфиденциальной информацией может быть осуществлен, <…> только если он необходим для применения настоящей Директивы. Информационный обмен должен быть ограничен рамками соответствия и пропорциональности целям указанного обмена. Указанный обмен информацией должен соблюдать режим конфиденциальности информации и охранять безопасность и коммерческие интересы операторов основных услуг и провайдеров цифровых услуг.»[220]

Директива NIS налагает обязательства, как на государственных, так и на частных «операторов основных услуг». Эти услуги включают энергетику, транспорт, банковское обслуживание, инфраструктуру финансовых рынков, здравоохранение, подачу и распределение питьевой воды, цифровую инфраструктуру. Если оператор основных услуг подпадает под действие Директивы NIS и размещается в государстве-участнике, то он должен:

1. принимать необходимые пропорциональные технические и организационные меры, направленные на управление рисками, связанными с используемыми ими в процессе работы сетевыми и информационными системами.

2. принимать необходимые меры, направленные на предупреждение и минимизацию

[219] О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза [Электронный ресурс]: директива Европейского парламента и Совета Европейского Союза. – № 2016/1148 – 06.07.2016. – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 30.07.2018).

[220] О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза / Там же.

воздействия инцидентов, влияющих на безопасность сетевых и информационных систем, используемых для оказания основных услуг, с точки зрения их непрерывности.

3. незамедлительно уведомлять компетентный орган или CSIRT об инцидентах, оказывающих существенное воздействие на непрерывность оказываемых ими услуг.

Уполномоченные органы вправе требовать от операторов основных услуг предоставления информации и доказательства эффективной реализации политик безопасности, например, результаты аудита безопасности, проведенного уполномоченным органом или аудитором. По результатам оценки информации или материалов аудита безопасности, уполномоченный орган может выдать оператору основных услуг обязывающие инструкции по исправлению практик своей операционной деятельности.

Директива NIS налагает обязательства на провайдеров цифровых услуг, к которым относятся интернет-магазины, онлайн-поисковый системы и операционные системы на базе облака. Уполномоченный орган может потребовать от провайдера цифровых услуг предоставить информацию, необходимую для оценки безопасности его сетей и информационных систем, включая документально оформленные политики безопасности и исправить любую ситуацию, связанную с неспособностью выполнить релевантные требования Директивы NIS.

Отдельное внимание также следует уделить ***судебной практике***, и в качестве репрезентативных дел допустимо привести следующие.

Coty Germany GmbH v Stadtsparkasse Magdeburg (Case C-580/13).[221] В этом деле Суд ЕС разъяснил вопросы пределов действия института банковской тайны в соотношении с правом на информацию, предусмотренным Директивой N 2004/48/EC Европейского парламента и Совета Европейского Союза «Об обеспечении прав на интеллектуальную собственность» (*On the enforcement of intellectual property rights*). По условиям дела заявитель являлся правообладателем товарного знака DAVIDOFF HOT WATER, зарегистрированным в отношении парфюма. В 2011 году он приобрел одноименный парфюм на аукционной платформе в сети Интернет, переведя определенную сумму на счет в банке Stadtsparkasse Magdeburg. После обнаружения того, что приобретённый товар является контрафактным, заявитель обратился в банк с требованием сообщить ему данные держателя счета, куда были

[221] Judgment of the European court of justice dated July 16, 2015 - Coty Germany GmbH v Stadtsparkasse Magdeburg (C-580/13) [Electronic resource] // The Court Of Justice Of The European Union [Site]. – URL: http://curia.europa.eu/juris/celex.jsf?celex=62013CJ0580&lang1=en&type=TXT&ancre= (accessed: 30.07.2018).

переведены деньги. В предоставлении сведений было отказано со ссылкой на банковскую тайну. Суды поддержали позицию банка. Рассмотрев материалы дела, Суд ЕС пришел к выводу, что соответствующие положения Директивы «Об обеспечении прав на интеллектуальную собственность» должны толковаться как препятствующие финансовым учреждениям безоговорочно и в неограниченном порядке отказывать в предоставлении информации об имени и адресе держателя счета по основанию наличия банковской тайны.

Sparkasse Allgäu v Finanzamt Kempten (Case C-522/14).[222] Суд ЕС разъяснил национальным судам, что статья 49 Договора о функционировании Европейского Союза должна толковаться как не запрещающая установление следующего регулирования. По законодательству одного государства-участника ЕС головной офис кредитного учреждения, обязанный уведомить национальные власти об активах, находящихся на территории другого государства-участника ЕС, где расположен филиал или представительство кредитного учреждения, в случае смерти собственника таких активов, являющегося гражданином первого государства-участника, вправе сделать это даже в случае, если в законодательстве второго государства-участника не содержится аналогичного требования об уведомлении и кредитные учреждения на его территории обязаны соблюдать банковскую тайну, раскрытие которой уголовно наказуемо.

Германия

Понятие банковской тайны прямо не закреплено в законодательстве Германии. Однако она была определена Федеральным высоким судом Германии как обязанность банка сохранять в тайне всю информацию, которую клиент хочет сохранить в тайне[223].

Банковская тайна тесно связана с обязательством по сохранению конфиденциальности - общим принципом, который применяется к любым частным отношениям, а не только к отношениям банк-потребитель. Такое обязательство не требует наличия действительного

[222] Judgment of the European court of justice dated April 14, 2016 - Sparkasse Allgäu v Finanzamt Kempten (Case C-522/14) [Electronic resource] // The Court Of Justice Of The European Union [Site]. – URL: http://curia.europa.eu/juris/document/document.jsf?text=banking%2Bsecrecy&docid=176343&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=173499#ctx1 (accessed: 30.07.2018).

[223] Bundesgerichtshof Urteil vom 24.01.2006, XI ZR 384/03 [Electronic resource] // Bundesgerichtshof [Site]. – URL: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=35317&pos=0&anz=1 (accessed: 07.08.2018).

договора, то есть банк обязан сохранять информацию конфиденциальной даже в тех случаях, когда договор признан недействительным или когда стороны решили не заключать договор, и отношения сторон остаются на преддоговорном этапе (немецкое право по общему правилу распространяет контрактные обязательства и на преддоговорный этап)[224].

Общие условия, включаемые в договоры между банком и клиентом в Германии и называемые «AGB Banken», также предусматривают условие о том, что банк обязан сохранять тайну в отношении любых относящихся к клиенту фактов и оценок, которые банк может получить исходя из своих знаний. Общие условия рекомендуемы к использованию и подготовлены Ассоциацией немецких банков для своих членов. Тем не менее, как правило, текст AGB-Banken принимается банками без изменений.

При этом банковская тайна не является абсолютной. В качестве иллюстрации можно привести дело № C-580/13, позиция по которому была выражена в том числе на уровне Европейского суда[225]. Суть дела состояла в том, что правообладатель товарного знака «Davidoff Hot Water» проведя закупку товара под данным товарным знаком обнаружило, что товар является контрафактным. Правообладатель запросил данные о продавце у оператора платформы, однако продавец отрицал нарушение прав на товарный знак. Впоследствии правообладатель обратился к банку продавца с просьбой раскрыть данные владельца счета. Однако банк отказал, сославшись на действие банковской тайны. Истец настаивал на своем праве получить такую информации на основе ст.8 Директивы 2004/48, согласно которой государства-члены ЕС должны обеспечить, чтобы при защите прав на интеллектуальную собственности компетентные органы могли предоставить правообладателям по их запросам необходимую информацию в отношении товаров, услуг, нарушающих их права. При этом такая информация включает, в том числе, имена и адреса производителей, дистрибьюторов, поставщиков (п.2 ст.8 Директивы). Кроме того, указанное выше право не ограничивает положения, касающиеся защиты конфиденциальности источников информации или обработку персональных данных. Вопрос заключался в том, должна ли ст.8 (3) Директивы толковаться как ограничивающая национальные положения, позволяющие банковским учреждениям отказывать, ссылаясь на банковскую тайну, предоставлять информацию в

[224] Booysen S., Neo D. Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres Around the World. - Cambridge University Press, 2017. – 65 P.

[225] Opinion of Mr Advocate General Cruz Villalón delivered on 16.04.2015. Case C-580/13 Coty Germany GmbH v. Stadtsparkasse Magdeburg. [Electronic resource] // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CC0580 (accessed: 07.08.2018).

соответствии со ст.8 (1) Директивы Европейский суд ответил на данный вопрос утвердительно, отметив, однако, что при этом национальный суд должен оценить законность ограничения таких прав.

В результате в указанном деле Федеральный суд Германии, руководствуясь позицией Европейского суда, вынес решение о том, что банковская тайна может быть ограничена, а ее пределы должны толковаться исходя из баланса интересов[226].

В отсутствие законодательного определения банковской тайны факт отнесения той или иной информации к ней подлежит исследованию в каждом конкретном деле. В связи с этим, можно сказать, что принцип формирования является открытым.

Состав сведений, составляющих банковскую тайну, не определен законодательно. В то же время, к ним можно отнести данные, являющиеся персональными, то есть данные, идентифицирующие лицо или позволяющие идентифицировать лицо. В рамках процедур KYC такие данные могут быть квалифицированы, в том числе, и как специальные категории персональных данных (например, если речь идет о сведениях о здоровье или судимости).

В части вопроса о разграничении сведений, составляющих банковскую тайну, и сведений ограниченного доступа между собой следует отметить, что институт сведений ограниченного доступа в законодательстве и судебных решениях не выявлен.

Сведения, составляющие банковскую тайну, могут подпадать одновременно под несколько видов тайн и иных категорий охраняемой законом информации:

1. Информация, являющаяся тайной
2. Персональные данные
3. Специальные категории персональных данных (сведения о судимости, медицинские данные для целей процедур KYC, получения пособий).

При этом Верховный суд Германии полагает, что защита данных в отношениях между банком и клиентом преимущественно регулируется банковской тайной («Bankgeheimnis»), в то время как закон о защите персональных данных применяется только к остальным аспектам, которые не затрагивают обязательство по сохранению профессиональной тайны[227].

В качестве механизмов защиты в случае нарушения банковской тайны можно

[226] Bundesgerichtshof Urteil vom 21.10.2015 I ZR 51/12 [Electronic resource] // Bundesgerichtshof [Site]. – URL: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2015&anz=179&pos=0&nr=74346&linked=urt&Blank=1&file=dokument.pdf (accessed: 07.08.2018).

[227] Bundesgerichtshof Urteil vom 27.02.2007 – XI ZR 195/05 [Electronic resource] // Institut für Wissen in der Wirtschaft [Site]. – URL: https://www.iww.de/quellenmaterial/id/15611 (accessed: 07.08.2018).

использовать взыскание убытков или неустойки, поскольку в таком случае это будет квалифицировано как нарушение гражданско-правового обязательства.

Субъекты персональных данных могут также подать жалобу в надзорный орган по месту проживания, работы или места предполагаемого нарушения (ст.77 GDPR) в том случае, когда раскрытая банковская тайна относится к их персональным данным.

За нарушение банковской тайны может наступать только гражданско-правовая ответственность. Так, в договоре могут быть предусмотрены заранее оцененные убытки (liquidated damages) или штрафы. Что касается уголовной ответственности, то статья 203 Уголовного кодекса Германии (StGB) о нарушении конфиденциальной информации не применима к банкам.

В качестве яркого судебного спора об ответственности за нарушение банковской тайны может привести дело Kirch Media.

Дело Kirch Media - одно из самых известных судебных споров Германии, связанных с банковской тайной. Иск был инициирован Лео Кирхом от имени двух компаний, принадлежащих его несостоятельной, но когда-то влиятельной медиа-империи, против Deutsche Bank и его бывшего главы правления Рольфа Браера.

Deutsche Bank был одним из основных кредиторов группы Кирха. Когда в 2002 году был распространена новость о том, что медиа группа испытывает финансовые трудности, Рольфа Бройера спросили в ходе интервью о финансовом состоянии группы. Он не отвечал в тот момент на вопрос как официальный представитель Deutsche Bank, однако сказал, что в текущих обстоятельствах он (лично) сомневается в том, что финансовой сектор поддержит медиа группу с последующими кредитами.

Это заявление было расценено обществом как суждение человека, который знает финансовую ситуацию, сложившуюся в медиа группе, а также показателем того, что Deutsche Bank не будет предоставлять ей дополнительную финансовую поддержку. В результате, многие кредиторы потеряли доверие к группе и ее усилиям по улучшению ситуации, которые до заявления Бройера казалась не такими безнадежными. Это привело к банкротству всей группы и краху медиа империи и ее руководителя Лео Кирха.

Суд Германии пришел к выводу, что Бройер нарушил обязательство Deutsche Bank по сохранению банковской тайны. Его утверждение как главы правления одного из самых главных кредиторов было расценено как негативный сигнал о будущем медиа группы. После 12 лет судебных споров в 2014 году дело Кирха и Deutsche Bank было завершено мировым

соглашением, по которому Deutsche Bank был обязан выплатить 775 млн. евро, а также проценты[228].

Оценка соотношения банковской тайны с другими правами осуществляется в рамках каждого конкретного дела. В этой части оценка касается соотношения права на частную жизнь с иными конституционными правами. В качестве примера можно привести следующее дело.

Sommer v. Germany (Решение ЕСПЧ от 27 апреля 2017 г.)[229]

ЕСПЧ признал нарушение статьи 8 Европейской Конвенции о защите прав человека и основных свобод (04.11.1950), а именно права на частную жизнь.

Дело было инициировано по жалобе юриста по уголовным делам Ульриха Соммера в связи с проверкой его профессионального банковского счета со стороны прокуратуры. Запрос прокуратуры на проверку счета гр. Соммера был сделан в рамках расследования мошенничества, одним из подозреваемых по которому был клиент гр. Соммера. Прокуратура попросила банк не раскрывать Соммеру информацию о том, что ею был сделан запрос. Банк подготовил список из 53 операций по счету Соммера.

Соммер полагал, что немецкие правоохранительные органы незаконно собирают, хранят и делают доступной информацию о его профессиональном банковском счете, содержащем информацию и о его клиентах.

Суд в Германии вынес решение о том, что такая проверка счета законна и банк предоставил информацию о банковском счете Соммера на добровольной основе.

ЕСПЧ напротив посчитал, что проверка банковского счета гр. Соммера несоразмерна, несмотря на то, что сама цель – предотвращение преступления, является законной. При этом учитывалось, что прокурата запросила всю информацию о банковском счете и банковских операциях, а также в последующем была раскрыта и сохранена его личная информация.

Порядок и условия передачи сведений, составляющих банковскую тайну, в той части, в которой они относятся к персональным данным, определены в Законе о ПД и GDPR. Порядок и условия передачи таких сведений аналогичны общим требованиям GDPR к

[228] Deutsche Bank 'to pay €800 mln' in Kirch case 13.02.2012 [Electronic resource] // The Local [Site]. – URL: https://www.thelocal.de/20120213/40709 (accessed: 07.08.2018).

[229] Inspection of a lawyer's bank account breached his right to professional confidentiality and private life. Press Release issued by the Registrar of the Court [Electronic resource] // European Court of Human Rights [Site]. – URL: https://hudoc.echr.coe.int/app/conversion/pdf?library=ECHR&id=003-5701328-7233297&filename=Judgment%20Sommer%20v.%20Germany%20-%20inspection%20of%20a%20lawyer%27s%20bank%20account.pdf (accessed: 07.08.2018).

обработке персональных данных, и персональных данных относящихся к специальным категориям (в части сведений о судимости и данных о здоровье).

Обязательство по сохранению конфиденциальности информации о клиентах применимо ко всему банку. Каждый его орган, представители, работники связаны этим обязательством, независимо от того, получена ли информация о клиенте от него самого или от представителя банка или из документов[230].

Поскольку банки взаимосвязаны между собой (по разным причинам – от совместной выдачи синдицированных займов до финансирования друг друга), иногда данные клиентов могут передаваться между ними. Такие банки, получающие информацию о клиентах, также обязаны выполнять требования о сохранении банковской тайны, как если бы это были их клиенты[231]. Например, оператор платежных операций «Easycash» был оштрафован на 60, 000 евро за незаконную передачу данных о банковских счетах, в том числе, данных местоположения, времени и размера определенных транзакций своей аффилированной компании для анализ клиентской лояльности и подготовки бонусной программы. Были выявлены примерно 400 тыс. случаев передачи данных[232].

Однако суд может ограничить объем информации, на которую распространяются требования о конфиденциальности. Так, только такая информация, которая проистекает из деловых отношений банка и клиента, покрывается банковской тайной. Этот критерий называется «inner connection» (внутренние взаимоотношения) между деловыми отношениями и тем, как банк получает соответствующую информацию[233].

Отдельно необходимо упомянуть SCHUFA – агентство по оценке кредитоспособности (Агентство)[234].

Клиенты дают согласие банкам на раскрытие их данных немецкому агентству по оценке кредитоспособности SCHUFA в качестве обязательного условия для вступления в отношения с банком. Они получают разрешение на передачу данных SCHUFA и получение данных из

---

[230] Booysen S., Neo D. Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres Around the World. - Cambridge University Press, 2017. – 54 P.

[231] Bundesgerichtshof Urteil vom 12.05.1958, II ZR 103/57 [Electronic resource] // Matthias Prinz Rechtsanwalt [Site]. – URL: https://www.prinz.law/urteile/bgh/II_ZR_103-57 (accessed: 07.08.2018).

[232] German State DPA Fines Payment Transaction Provider for Unlawful Transfer of Transaction Data. 12.09.2011 [Electronic resource] // HUNTON Andrews Kurth [Site]. – URL: https://www.huntonprivacyblog.com/2011/09/12/german-state-dpa-fines-payment-transaction-provider-for-unlawful-transfer-of-transaction-data/ (accessed: 08.08.2018).

[233] Bundesgerichtshof Urteil vom 24.01.2006, XI ZR 384/03 // Там же.

[234] SCHUFA [Electronic resource] – URL: https://www.schufa.de/de/ (accessed: 07.08.2018).

него. Агентство собирает данные обо всех должниках Германии и предает собранную информацию кредиторам. Банки, торговые компании и компании иных секторов экономики являются такими кредиторами и могут получить доступ к базе данных Агентства на основе принципа взаимности. То есть если они сами сообщают данные о своих должниках в Агентство, они вправе получить доступ ко всей информации, которую предоставляют и иные кредиторы. Для банков такой доступ крайне важен.

Согласно ст.31 Закона о защите персональных данных 2017 года Германии (Закон о ПД)[235] при принятии решения о начале договорных отношений, исполнения обязательств или прекращения отношений с физическим лицом, использование значения вероятности в отношении определенных будущих действий такого лица (скоринг) допускается только если будут соблюдены положения Закона о ПД, а также необходимо, чтобы данные рассчитывались на основе научно-признанной математико-статистической процедуры, кроме того в дополнение к адресным данным могут использоваться и другие данные (при этом физическое лицо должно быть уведомлено заранее о планируемом использовании таких данных, и уведомление должно быть документально оформлено).

Использование значения вероятности, исчисляемого Агентством для определения способности и готовности физического лица к оплате, допустимо только при условии, если выполнены положения Закона о ПД, а кроме того соблюдена специальная процедура предъявления требований об исполнении просроченных обязательств. Например, это должны быть требования, подтвержденные окончательным решением суда, исполнительными листом; признанные должником; либо в отношении которых должник получал не менее двух письменных напоминаний после предъявления требований, по прошествии не менее четырех недель после первого напоминания; должник не оспаривал предъявление к нему требований и т.д.

Трансграничная передача банковских данных как персональных данных регулируется GDPR.

В отношении случаев, условий и порядка передачи сведений, составляющих банковскую тайну, третьим лицам без согласия субъектов необходимо отметить, что с точки зрения Закона о ПД и GDPR согласие – это лишь одно из нескольких оснований обработки

[235] Federal Data Protection Act (BDSG) of 30 June 2017 [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf (accessed: 07.08.2018).

персональных данных. Таким образом, по умолчанию, допустима обработка данных, относящихся к банковской тайне при наличии иных, помимо согласия, оснований для обработки. Порядок и условия передачи сведений государственным органам рассмотрены ниже.

Прямое регулирование в отношении изъятия из режима охраны сведений, составляющих банковскую тайну, в целях обеспечения возможности обработки накопленных данных для достижения социальных (вкл. повышения уровня здоровья населения), государственных, экономических целей, отсутствует.

В качестве случаев раскрытия сведений, составляющих банковскую тайну, в том числе в форме открытых данных, можно привести только публикацию официальной банковской статистики[236].

Вопрос о возможности доступа третьих лиц к данным, составляющим банковскую тайну, был раскрыт выше. Администрирование согласий субъектов банковской тайны на обработку сведений, составляющих банковскую тайну и/или их передачу третьим лицам (в т.ч. наличие права субъекта определять порядок использования таких сведений, делегирования права на выдачу согласий, отзыва согласий на их сбор, обработку и/или передачу и т.д.) подчиняется общим правилам, установленным в GDPR.

Специальные нормы по идентификации субъектов тайн (в т.ч. их законных представителей) не выявлены.

В отношении форм и способов получения согласий, порядка фиксации и хранения подтверждения согласий следует отметить, что согласие на обработку сведений, составляющих банковскую тайну, аналогично согласиям на обработку иных персональных данных. Способ получения, передачи и хранения также аналогичен общим требованиям, установленным GDPR.

Немецкое право обеспечивает доступ к банковской тайне со стороны уполномоченных органов. Вмешательство в частную сферу ограничено Конституцией Германии. Положения статей 1(1) и 2(1) Конституции касаются защиты конфиденциальной информации[237]. Указанные статьи гарантируют право на информационное самоопределение, понимаемое в

[236] Banking statistics. Deutsche Bundesbank [Electronic resource] // Bundesbank [Site]. – URL: https://www.bundesbank.de/Navigation/EN/Service/Reporting_systems/Banking_statistics/banking_statistics.html (accessed: 07.08.2018).

[237] Basic Law for the Federal Republic of Germany. [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: http://www.gesetze-im-internet.de/gg/GG.pdf (accessed: 07.08.2018).

том смысле, что лицо вправе самостоятельно решать, в каком объеме оно желает раскрывать личную информацию[238]. Банки же защищены положениями ст.12 Конституции, которая применяется как к юридическим, так и к физическим лицам, и защищает свободу на осуществление своей деятельности. Ограничения указанных прав должны быть пропорциональными.

Наибольший доступ к данным, находящимся у банка, предоставляется финансовым регуляторам и контролирующим органам. Контроль банковской сферы осуществляется совместно федеральным агентством, осуществляющим контроль над всеми финансовыми услугами в Германии, федеральным финансовым надзорным ведомством – BaFin, а также центральным банком Германии (Deutsche Bundesbank). Кроме того, надзор осуществляется и Европейским центральным банком.

Полномочия осуществляются в соответствии с Законом о банковской деятельности (German Banking Act)[239].

Согласно ст.44 Закона о банковской деятельности все банки и иные финансовые институты обязуются предоставлять информацию, запрашиваемую уполномоченными органами – BaFin и Deutsche Bundesbank.

В то же время в п.6 ст.44 содержится исключение из обязанности предоставлять информацию. Так, лицо обязанное предоставлять информацию может отказаться от ее предоставления, если предоставление такой информации может поставить его или одного из его родственников под угрозу уголовного преследования.

В дополнение к указанному выше банки обязаны сообщать о крупных займах в Deutsche Bundesbank на основании статей 13a (1), 14 (1) Закона. Однако наиболее серьезно вмешательство осуществляется на основании ст. 24c (1), согласно которой все контролируемые учреждения постоянно должны обновлять списки с указанием имени и даты рождения владельца каждого счета, номера их счетов и даты открытия счетов и, если

---

[238] Данная позиция выведена из нескольких решений Конституционного суда Германии. Например, см. BverfG of 15.12.1983 [Electronic resource] // Telemedicus [Site]. – URL: https://www.telemedicus.info/urteile/Datenschutzrecht/88-BVerfG-Az-1-BvR-209,-269,-362,-420,-440,-48483-Volkszaehlungsurteil.html (accessed: 07.08.2018); BverfG of 11.06.1991 - 1 BvR 239/90 [Electronic resource] // Jurion [Site]. – URL: https://www.jurion.de/urteile/bverfg/1991-06-11/1-bvr-239_90/?from=1%3A3191944%2C0 (accessed: 07.08.2018); BverfG of 13.06.2007 – 1 BvR 1550/03 [Electronic resource] // Jurion [Site]. – URL: https://www.jurion.de/urteile/bverfg/2007-06-13/1-bvr-1550_03_-1-bvr-2357_04_-1-bvr-603_05/ (accessed: 07.08.2018).

[239] Gesetz über das Kreditwesen (Kreditwesengesetz - KWG) 10.07.1961 [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/kredwg/KWG.pdf (accesed: 07.08.2018).

применимо, закрытия. Данные о суммах и транзакциях не включены в эти списки.

Кроме того, контролирующие органы могут получить доступ к данным, если это необходимо для осуществления их задач в рамках Закона об отмывании денег. Для предотвращения отмывания денег банки обязаны осуществлять мониторинг подозрительной активности клиентов и сообщать о ней уполномоченным органам при ее выявлении (ст.11). Эти обязанности имплементированы в Закон из соответствующего Европейского регулирования (Директива 2015/849 от 20 мая 2015), а также рекомендаций ФАТФ.

Согласно абз.2 ст.24(1) банки обязаны обеспечить, чтобы BaFin имел постоянный автоматический доступ к данным с помощью специальных программно-технических средств. При этом ни банк, ни клиент не должны знать, когда осуществляется доступ к данным. Конституционность данных положений была оценена Федеральным конституционным судом, который признал, что данная статья соответствует Конституции Германии, поскольку есть пропорциональная цель (предотвращение, расследование преступлений), а кроме того доступ осуществляется только к ограниченным, заранее определенным данным, а не ко всем[240].

Уполномоченные органы также обязаны выполнять требования по защите полученных данных, и могут передавать данные другим органам, в том числе в других государствах, только если они выполняют те же самые обязательства по сохранению конфиденциальности (ст.9(1)).

В рамках уголовного преследования против клиентов банков банковская тайна не защищает отношения банк-клиент. Это правило применяется независимо от природы обвинения. То есть это может быть и отмывание денег, уклонение от налогов, а может быть и взяточничество, мошенничество и т.д[241].

Согласие на обработку сведений, составляющих банковскую тайну, аналогично согласиям на обработку иных персональных данных. Способ получения, передачи и хранения также аналогичен общим требованиям, установленным GDPR.

Вопрос о возможности доступа третьих лиц к данным, составляющим банковскую тайну, с согласия субъекта был рассмотрен выше. Права и обязанности регулируются GDPR и Законом о ПД.

[240] BverfG of 13.06.2007 – 1 BvR 1550/03 // Ibid.

[241] Booysen S., Neo D. Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres Around the World. - Cambridge University Press, 2017. – 86 P.

В части информационной безопасности в разделе 25a Закона о банковской деятельности содержится требование о том, что каждый обладатель банковской лицензии должен внедрить соответствующую систему управления рисками. Согласно инструкции BaFin «Минимальные требования к управлению рисками» (MaRisk) система должна также учитывать требования в отношении информационной безопасности[242]. Помимо этого разработаны «Требования к банковскому контролю информационных систем» (BAIT)[243]. Так, должна быть определена информационная стратегия, определяющая цели и средства их достижения. На основе стратегии должно осуществляться управление корпоративными информационными системами. Организация должна обеспечить наличие соответствующего персонала, который мог бы управлять информационными рисками, информационной безопасностью, IT-задачами и разработкой приложений. Отдельные требования предъявляются к управлению информационными рисками, информационной безопасности, доступу пользователей, IT проектам, приложениям, IT-операциям (включая резервному копированию данных), аутсорсингу и иному внешнему использованию IT системам.

Во исполнение директивы 2015/2366/EC об оказании платежных услуг был принят специальный закон, также содержащий требования о необходимости определения провайдером услуг политики информационной безопасности.

Испания

На уровне законодательства Испании вопросы банковской тайны прямо не урегулированы, кроме нескольких общих положений о необходимости обеспечивать конфиденциальность соответствующей информации. В целом, вопросы банковской тайны в Испании регулируются с учетом приведенных в настоящем отчете положений международных актов, законодательства Европейского союза и, в частности, GDPR, что более подробно раскрывается в иных частях исследования.

[242] Rundschreiben 09/2017 (BA) – Mindestanforderungen an das Risikomanagement – MaRisk [Electronic resource] // Bundesanstalt für Finanzdienstleistungsaufsicht [Site]. – URL: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1709_marisk_ba.html;jsessionid=FAB34214A16E8EA7AB894DABC37F1AB3.1_cid298?nn=8249098 (accessed: 07.08.2018).

[243] Circular 10/2017 (BA): Supervisory Requirements for IT in Financial Institutions [Elecrtonic resource] // Bundesanstalt für Finanzdienstleistungsaufsicht [Site]. – URL: https://www.bafin.de/SharedDocs/Downloads/EN/Rundschreiben/dl_rs_1710_ba_BAIT_en.html;jsessionid=FAB34214A16E8EA7AB894DABC37F1AB3.1_cid298?nn=8249098 (accessed: 07.08.2018).

Эстония

Положения о банковской тайне содержатся в статье 38 Закона о кредитных организациях (далее - «*Закон о кредитных организациях*»)[244]. Сведения, составляющие банковскую тайну, включает в себя все данные, известные кредитному учреждению о клиенте такого учреждения или другого кредитного учреждения, включая данные о финансовом состоянии, персональные данные, транзакциях, экономической деятельности, собственности и др. Перечень данных является открытым. При этом данными, которые не охватываются банковской тайной, являются:

1) публичные данные, доступные заинтересованным лицам из иных открытых источников;

2) обобщенные данные, на основе которых не представляется возможным определить данные, относящиеся к конкретному лицу;

3) данные об участниках и/или учредителях кредитного учреждения или данные, относящиеся к размеру их долей в уставном капитале кредитного учреждения, вне зависимости от того, являются ли они клиентами такого учреждения;

4) сведения об исполнении клиентом кредитного учреждения своих обязательств перед учреждением.

Данные, охраняемые банковской тайной, могут быть раскрыты кредитным учреждением третьим лицам только с согласия клиента в письменной форме, либо в случае, прямо предусмотренном Законом о кредитных организациях. Сохранение конфиденциальности сведений, составляющих банковскую тайну, обеспечивается за счет возложения соответствующих обязанностей по сохранению конфиденциальности на акционеров, участников, членов, работников банков, а также любых иных лиц, имеющих доступ к таким сведениям.

Кредитное учреждение обязано раскрывать сведения, составляющие банковскую тайну:

1) органу финансового надзора Эстонии (*Eesti Pank*) или органам финансового надзора других государств, в том числе, Европейскому центральному банку для целей

[244] Credit Institutions Act of February 09, 1999 (as revised May 02, 2018) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523052018002/consolide. (accessed: 30.07.2018).

исполнения такими органами своих обязательств;

2) подразделению финансовой разведки или службе внутренней безопасности Эстонии в соответствии с положениями законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

3) налоговой и таможенной службам в случаях, установленных законом, включая исполнение обязанностей в соответствии с законодательством об азартных играх;

4) органам полиции и пограничной службы в установленных случаях, в том числе, при использовании данных из национальных информационных систем;

5) службам информационной безопасности Эстонии при осуществлении государственного надзора в соответствии с законом о кибербезопсаности:

6) судам в случае направления судебного запроса;

7) органам предварительного следствия и прокуратуре в связи с расследование уголовных правонарушений;

8) службам безопасности в целях расследования дел, связанных с государственной тайной;

9) службе исполнения наказании для целей исполнения наказаний;

10) уполномоченным органам в целях осуществления процедур банкротства, включая трансграничное банкротство;

11) государственным аудиторам в целях проведения аудита;

12) лицам, назначенным в соответствии с законодательством о гарантийном фонде;

13) наследнику, уполномоченному им лицу, нотариусу или иному лицу, осуществляющему инвентаризацию наследства, консульскому представителю другого государства по вопросам наследования при условии предоставления соответствующих документов;

14) депозитарию, действующему в соответствии законодательством о противодействии коррупции.

Запрос на раскрытие информации, составляющей банковскую тайну, должен содержать сведения о лице, направившем запрос, его должности, адресе и контактных данных, о клиенте, в отношении которого запрашивается информация, цель запроса и исчерпывающий перечень запрашиваемых данных, юридическое основание и подпись лица.

На основании соответствующего письменного запроса кредитное учреждение вправе раскрыть информации следующим лицам:

1) материнской компании юридического лица – клиента для целей составления консолидированной отчетности;

2) финансовому учреждению, относящемуся к той же группе компаний, или другому кредитному учреждению сведений об истории платежей клиента для оценки кредитных рисков и реализации принципа ответственного кредитования;

3) компании, входящей в ту же группу, что и кредитное учреждение, которой такие сведения требуются для проведения проверки благонадежности клиента в соответствии с требованиями законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Перечисленные в последнем абзаце лица вправе передать третьим лицам сведения о нарушении клиентом своих обязательств до истечения семи лет с даты прекращения нарушения, а также персональные данные клиента до истечения пяти лет с даты прекращения нарушения.

Лица, получившие сведения, составляющие банковскую тайну, могут использовать такие сведения только для выполнения своих обязательств в соответствии с законодательством и для целей, прямо указанных в запросе информации. Они также обязаны сохранять конфиденциальность полученных сведений и несут ответственность за нарушение установленного обязательства.

Дополнительно, кредитное учреждение вправе раскрыть сведения, составляющие банковскую тайну, органам предварительного следствия, прокуратуре или судам в целях защиты собственных нарушенных или оспариваемых прав в порядке, предусмотренном законом.

Отдельно следует отметить право кредитного учреждения раскрыть банковскую тайну в части сведений об обстоятельствах совершения платежа клиенту или платежному сервису, осуществившему платеж:

1) в случае если это требуется для уведомления о результатах рассмотрения вопроса о просроченных или неправильно выполненных платежах;

2) в целях предоставления клиенту банка или оператору другого платежного сервиса возможности предъявить претензию в отношении получателя средств для возврата средств, если последний не мог быть осуществлен через оператора платежного сервиса, обслуживавшего платеж клиента.

Закон о кредитных учреждениях не содержит специальных положений о

трансграничной передаче сведений, составляющих банковскую тайну.

В соответствии с законом о противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма[245], работники уполномоченных органов обязаны сохранять конфиденциальность сведений, включая сведения, составляющие банковскую тайну, ставших им известными в связи с выполнением служебных обязанностей, даже после прекращения служебных правоотношений. На ответственный орган также возлагается обязанность соблюдать требования законодательства об обработке персональных данных. Согласно ст. 48 обработка персональных данных допускается только в целях осуществления такого противодействия и не должна осуществляться в иных целях, включая маркетинг.

Ответственность за нарушение обязательства по сохранению конфиденциальности сведении, составляющих банковскую тайну включает в себя: штраф в размере до 300 штрафа (порядка 1200 Евро) для работников кредитных учреждений и иных лиц, действующих в их интересах, обязанных соблюдать конфиденциальность, и штраф в размере 32000 Евро для юридических лиц.

Обратимся к репрезентативному примеру ***судебной практики***.

Дело 3-2-1-19-17 Swedbank AS-i против Vladimir Kutšmei[246] В данном деле суд указал, что понятие банковской тайны необходимо трактовать в широком смысле для защиты интересов клиента и все данные и оценки, которые принадлежат кредитной организации, рассматриваются в качестве банковской тайны. Раскрытие таких сведений приставам-исполнителям допускается только в установленных законом случаях. В данном деле судебный пристав запросил предоставить данные о состоянии баланса, которые относятся к банковской тайне. Согласно действующему законодательству, соответствующий запрос должен содержать исчерпывающий перечень запрашиваемых сведений и указание на цель запроса. В предоставлении сведений было отказано. Судебный пристав ошибочно полагал, кредитная организация не вправе была оценивать целесообразность предоставления

[245] Money Laundering and Terrorist Financing Prevention Act of October 26, 2017 [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/521122017004/consolide (accessed: 30.07.2018).

[246]Case No. 3-2-1-19-17 Swedbank AS-i v.Vladimir Kutšme [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/kohtulahendid/otsingutulemus.html?aktiivneTab=KOIK&sort=LahendiKuulutamiseAeg&asc=false&kohtuasjaNumber=&lahendiKpvAlgus=&lahendiKpvLopp=&menetluseKpvAlgus=&menetluseKpvLopp=&kohus=&kohtunik=&annotatsiooniSisu=&menetluseLiik=&lahendiLiik=&ecliNumber=&lahendiTekst=pangasaladus (accessed: 30.07.2018).

запрошенной информации и отказывать в ее предоставлении.

Окружной суд установил, что требование судебного пристава не обоснованы. Запрос информации не соответствовал требованиям и не содержал достаточного обоснования для раскрытия банковской тайны, судебный пристав мог получить необходимые данные из иных публичных источников. Кроме того, в соответствии с законом кредитная организация обязана оценивать содержание каждого полученного запроса на предоставление сведений, содержащих банковскую тайну, поскольку несет ответственность за разглашение конфиденциальной информации без законных оснований.

Дело 2-14-50251 о банкротстве компании Johnny H.W.[247] В этом деле речь шла об отказе кредитного учреждения в предоставлении сведений, составляющих банковскую тайну, в рамках банкротного производства. Суд установил, что в соответствии с законом кредитная организация должна раскрывать банковскую тайну по запросу, в том числе, суда в письменной форме или в электронной форме. Суд проанализировал материалы дела и установил, что запрос конфиденциальной информации арбитражного управляющего являлся обоснованным, в запросе содержался конкретный перечень сведений, подлежащих представлению. Соответственно, запрос подлежал исполнению банком. В целях обеспечения безопасности сведений законодательство предусматривает дополнительные процессуальные возможности для сторон таким образом, чтобы данные, представленные по судебному запросу, не были в дальнейшем раскрыты общественности.

Великобритания

Поскольку Великобритания является страной общего права (*common law),* то есть страной, в которой существенную и главенствующую роль играет прецедентное право, в Великобритании отсутствует кодифицированное понятие банковской тайны.

Банковская тайна проистекает из доктрины справедливости о нарушении конфиденциальности (*"breach of confidence)* (более подробно см. раздел Медицинская тайна).

[247]Case No. 2-14-5025 [Electronic resource] // Riigi Teataja [Site]. – URL:https://www.riigiteataja.ee/kohtulahendid/otsingutulemus.html?aktiivneTab=KOIK&sort=LahendiKuulutamiseAeg&asc=false&kohtuasjaNumber=&lahendiKpvAlgus=&lahendiKpvLopp=&menetluseKpvAlgus=&menetluseKpvLopp=&kohus=&kohtunik=&annotatsiooniSisu=&menetluseLiik=&lahendiLiik=&ecliNumber=&lahendiTekst=pangasaladus (accessed: 30.07.2018).

Ключевое дело, касающееся банковской тайны – это дело Tournier v National Provincial and Union Bank of England (1924)[248]. Суд указал, что в контракте между клиентом и банком подразумевается, что последний будет хранить конфиденциальность клиентов. При этом не важно, от кого были получены сведения о клиенте, от него самого или от третьих лиц. Главным критерием возникновения отношений банк-клиент является открытие банковского счета[249]. При этом обязанность по сохранению конфиденциальности не является абсолютной.

В частности, серьезным образом право на сохранение конфиденциальности ограничивается в рамках соблюдения процедур по:

- противодействию легализации доходов, полученных преступным путем (AML и KYC процедуры);
- противодействию финансирования терроризма;
- противодействию уклонения от налогов;

Принцип, сформулированный в деле Tournier, был использован в добровольном для исполнения Кодексе практики для банков. Кодекс не являлся обязательным для исполнения, однако его условия могли приниматься во внимание при решении вопроса о том, действовал ли банк разумно. Сейчас Кодекс заменен прямым регулированием, содержащимся в FCA Handbook[250], нарушение положений которого может привести к дисциплинарной ответственности (PRIN. 1.1.7). Также действует отдельный добровольный для исполнения кодекс - Lending Code[251], в котором указывается, что персональная информация рассматривается как частная и конфиденциальная, а также, что запрещено раскрывать имя клиента, адрес любой компании, включая компании, входящей в одну группу компаний с банком без специального разрешения от клиента (п.23 Кодекса).

[248] Tournier v. National Provincol and Union Bank of England [Electronic resource]: Judgment of the Court of Appeal dated of December 17, 1923 // United Settlement [Site]. – URL: http://www.uniset.ca/other/css/19241KB461.html (дата обращения: 31.07.2018).

[249] Commissioner of Taxation v English, Scotishand Australian Bank Ltd dated of 1920 [Electronic resource] // Swarb.co.uk [Site]. – URL: https://swarb.co.uk/commissioners-of-taxation-v-english-scottish-and-australian-bank-limited-pc-2-jan-1920/ (accessed: 31.07.2018).

[250] FCA Handbook [Electronic resource] // FCA Handbook [Site]. – URL: https://www.handbook.fca.org.uk/ (acceesed: 31.07.2018).

[251] The Lending Code. Setting standards for banks, building societies and credit card providers. – March 2011. [Electronic resource] // Landing Standards Board [Site]. – URL: www.lendingstandardsboard.org.uk (accessed: 31.07.2018).

Кроме того, банки могут заключать соглашения о конфиденциальности или указывать в других контрактах четкие условия о соблюдении конфиденциальности[252].

Помимо конфиденциальности в широком смысле банковская тайна также содержит в себе сведения, относящиеся к персональным данным, то есть сведения, относящиеся к идентифицируемому лицу или лицу, которое может быть идентифицировано (п.2 ст.3 Закона О ПД»).

В отсутствие самого понятия банковской тайны факт отнесения той или иной информации к банковской тайне подлежит исследованию в каждом конкретном деле. В связи с этим, можно сказать, что принцип формирования является открытым.

Состав сведений, составляющих банковскую тайну, не определен законодательно. В то же время, в качестве иллюстрации примеров сведений, относящихся к банковской тайне можно привести регулирование, существующее в рамках Закона о ПД как персональные данные, как данные идентифицирующие лицо или позволяющие его идентифицировать. При этом такие данные также могут содержать в себе специальные категории персональных данных, а именно сведения о судимости (для целей процедур KYC и предупреждения преступности), а также медицинские данные (для целей процедур KYC и получения пенсионных пособий).

В процессе анализа сведения ограниченного доступа не выявлены.

Сведения, составляющие банковскую тайну, могут подпадать одновременно под несколько видов тайн и иных категорий охраняемой законом информации:

4. Конфиденциальная информация в широком смысле;
5. Персональные данные;
6. Специальные категории персональных данных (сведения о судимости (для целей процедур KYC и предупреждения преступности), а также медицинские данные (для целей процедур KYC и получения пенсионных пособий).

Агентства по оценке кредитоспособности собирают информацию о кредитоспособности физических лиц, а затем продают ее. В данном случае может возникать сомнение в том, что такие действия не покрываются общим требованием о сохранении конфиденциальности данных. В случае, если применяется Lending Code, то он устанавливает обстоятельства, при

[252] United Pan-European Communications NV v Deutsche Bank AG [Electronic recourse]: [2000] EWCA Civ 166, [2000] 2 BCLC 461 // BAILII [Site]. – URL: https://swarb.co.uk/united-pan-europe-communications-n-v-v-deutsche-bank-ag-ca-19-may-2000/ (accessed: 31.07.2018).

наличии которых банк может передать информацию агентствам по оценке кредитоспособности. Этому посвящен раздел 3 Кодекса. Так, банк обязуется предупредить клиента о том, что его данные могут быть переданы в такое агентство. Банк может передать в агентства информацию о долгах потребителя, если:

- клиент имеет просрочку по платежам; и

- клиент не оспаривает сумму задолженности; и

- клиент не предложил банку решение, направленное на погашение долга, которое бы удовлетворяло банк.

Независимо от того, был ли клиент уведомлен, и было ли получено согласие клиента в момент открытия счета, раскрытие информации о просрочке может быть осуществлено. Однако в любом случае клиенту должно быть направлено уведомление о намерении раскрыть такую информацию не менее, чем за 28 дней до раскрытия. Если отсутствует согласие клиента, то в соответствии с Законом о ПД должно быть иное основание для передачи таких данных. Кодекс указывает, что разрешение на передачу может быть указано в положениях и условиях договора, или оно может быть получено в момент раскрытия информации.

Отдельного внимания заслуживают аспекты **«Больших данных» / Big Data**. 6 ноября 2014 года Управление по защите конкуренции и рынкам Великобритании запустило большое исследование рынка розничных банковских услуг для физических лиц и малых и средних предприятий[253]. В финальном отчете по результатам исследования, которое проводилось 2 года, были указаны ключевые проблемы, существующие на банковском рынке. Один из аспектов касался Big Data технологий. В частности, использование Big Data применительно к имеющимся у банка данным, либо же данным третьих лиц может способствовать усилению конкуренции. В отчете также указаны и иные преимущества использования технологий Big Data (п.5.170)[254]. Учитывая, что крупные банки обладают большим количеством информации, было принято решение, что к таким данным должен быть обеспечен доступ для других компаний посредством разрешения использования API крупных банков.

2 февраля 2017 года Управление приняло Приказ об исследовании розничного

[253] Retail banking market investigation [Electronic resource] // Gov.uk [Site]. – URL: https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk#terms-of-reference (accessed: 31.07.2018).

[254] Retail banking market investigation. Final Report [Electronic resource] // Gov.uk [Site]. – URL: https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf (accessed: 31.07.2018); приложения см. на Retail banking market investigation [Electronic resource] // Gov.uk [Site]. – URL: https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk#final-report (accessed: 31.07.2018).

банковского рынка[255]. Полномочия Управления по изданию такого приказа установлены в ст.138 Закона о предпринимательской деятельности 2002 года[256]. В Приказе определены 9 крупнейших банков Великобритании, которые должны открыть свои API к 13 января 2018 года (дата вступления в силу Директивы 2015/2366/ЕС «Об платежных услугах»).

Для реализации проекта была создана некоммерческая организация «Open Banking Limited"[257], которая является ответственной за работу системы. Она также утверждает рекомендации в части стандартов API, и иные[258]. Клиенты банка участвуют в данном проекте только после дачи согласия (по общим правилам GDPR). Учитывая положения GDPR и Закона О ПД в личном кабинете физическое лицо может указать, к каким именно данным открыт доступ, как долго они могут обрабатываться. В целом проект позволяет пользователям видеть свои банковские аккаунты в режиме «одного окна», а также получить более персонализированные предложения.

Данные, которые становятся доступными для третьих лиц через API, включают в себя, например, расположение филиалов банков, сведения о банковских продуктах и т.д. Цель – облегчение поиска банков, сравнение банковских продуктов для выбора лучшего предложения. Что более важно, доступными становятся и данные о транзакциях.

Для того чтобы стартап мог участвовать в данном проекте он должен пройти специальную процедуру[259]. В том числе, сервис должен быть включен в реестр финансовых сервисов FCA[260].

В отношении механизма правовой защиты субъектов следует отметить, что если клиент полагает, что банк может нарушить или уже нарушил обязанность по сохранению конфиденциальности, у него есть два средства правовой защиты:

- подача иска в суд с требованием возмещения ущерба, или

---

[255] Retail Banking Market Investigation Order 2017 [Electronic resource] // Gov.uk [Site]. – URL: https://assets.publishing.service.gov.uk/media/5893063bed915d06e1000000/retail-banking-market-investigation-order-2017.pdf (accessed: 31.07.2018).

[256] Enterprise Act 2002 [Electronic resource] // Legislation.gov.uk. [Site]. – URL: http://www.legislation.gov.uk/ukpga/2002/40/contents (accessed: 31.07.2018).

[257] Open Banking [Electronic resource]– URL: https://www.openbanking.org.uk/ (accessed: 31.07.2018).

[258] Open Banking. Guidelines for Read/Write Participants. – March 2018. Version 3.1 [Electronic resource] // Open Banking [Site]. – URL: https://www.openbanking.org.uk/wpcore/wp-content/uploads/Open-Banking-Guidelines-for-ReadWrite-Participants-v3.1.pdf (accessed: 31.07.2018).

[259] Third party providers. Open Banking [Electronic resource] // Open Banking [Site]. – URL: https://www.openbanking.org.uk/providers/third-party-providers/ (accessed: 31.07.2018).

[260] Financial Services Register [Electronic resource] – URL: https://register.fca.org.uk/ (accessed: 31.07.2018).

- требование судебного запрета на раскрытие или запрета на повторение раскрытия информации

См. например, дело Primary Group (UK) ltd v. The Royal Bank of Scotland plc261. Банк ответчик хотел получить информацию о положении его клиента на рынке, и в результате раскрыл данные клиента работникам дочерней компании, которая являлась конкурентом клиента. Размер убытков, которые были выплачены клиенту, составил 5 000 фунтов.

Перед принятием судебного запрета суд должен исследовать вопрос о том, что компенсация ущерба не будет адекватным средством правовой защиты. На практике возмещение ущерба редко является адекватным средством правовой защиты, поскольку после того как раскрытие информации произошло трудно измерить потерю клиента в денежном эквиваленте.

Кроме того, можно воспользоваться Financial Ombudsmen Services (FOS) – механизмом разрешения споров, разработанным самой индустрией. Он бесплатен для обращающихся. Это лучшее решение для частного потребителя, который пострадал от раскрытия его конфиденциальной информации. В то же время такие решения имеют мало ценности. Если решение и выносится в пользу потребителя, то обычно оно ограничивается извинением и маленькой суммой компенсации за причиненные неудобства.

Примеры дел, рассмотренных по процедуре FOS. Дело DRN515001 – женщина пожаловалась на то, что она подверглась нападкам со стороны ее бывшего партнера, который, воспользовавшись своей позицией работника в банке узнал адрес, где она живет. Она не понесла финансовых потерь в результате раскрытия информации. Омбудсмен решил, что банк ответственен за действия своего работника при получении доступа к счету его клиента, и квалифицировал это как использование в неправильных целях. Банк был обязан выплатить 600 фунтов стерлингов.

Дело 45/5[262] Гр. А торговал в помещениях, арендованных у компании P Ltd. Банку было дано указание направлять отчеты в «A c / o P Ltd». Однажды банк ошибочно направил заявление в «P Ltd.». В компании «P Ltd.» открыли это письмо и обнаружили, что у А имеется большой овердрафт, и при этом у А была непогашенная задолженность по оплате

[261] Primary Group (UK) Ltd and others v Royal Bank of Scotland Plc and another [2014] EWHC 1082 (Ch) [Electronic resource] // Rosling King [Site]. – URL: https://www.rkllp.com/2014/05/08/may-2014-banking-update/ (accessed: 31.07.2018).

[262] Financial Ombudsmen Service. Issue 45. – April 2005. [Electronic resource] // Financial Ombudsmen [Site]. – URL: http://www.financial-ombudsman.org.uk/publications/ombudsman-news/45/45.pdf (accessed: 31.07.2018).

аренды. Это привело к тому, что «P Ltd.» направило судебных приставов и в результате, это привело к тому, что бизнес А развалился. Омбудсмен пришел к выводу, что убытки А были вызваны раскрытием банком конфиденциальной информации. В итоге А были присуждены убытки в размере 40 000 фунтов стерлингов.

Субъекты персональных данных могут также подать жалобу в надзорный орган по месту проживания, работы или места предполагаемого нарушения (ст.77 GDPR).

В части особенностей юридической ответственности, FCA устанавливает общие принципы, которые применяются ко всем организациям и принимаются во внимание в случаях нарушения конфиденциальности. Например, третий принцип – принимать разумные меры по организации охраны и контролю. Нарушение этого принципа в части распространения информации клиентов среди работников разных банков было положено в основу привлечения к ответственности по делу о манипулировании рынком FOREX (штраф составил в совокупности 1 млрд фунтов и был наложен на 5 крупных банков)[263].

В другом случае Bank of Scotland был обязан выплатить штраф в размере 75,000 фунтов в 2013 г за неоднократное направление информации о клиентах по факсу ошибочным получателям[264].

Еще одно дело касалось наложения штрафа в размере 38,198 фунтов на Christopher Niehaus, в прошлом инвестиционного банкира, который распространил конфиденциальные данные о клиенте с помощью мобильного приложения WhatsApp[265].

Помимо штрафов, накладываемых FCA, банки могут быть привлечены к ответственности за нарушение персональных данных по Закону О ПД.

---

[263] FCA fines five banks £1.1 billion for FX failings and announces industry-wide remediation programme [Electronic resource] // Financial Conduct Authority [Site]. – URL: https://www.fca.org.uk/news/press-releases/fca-fines-five-banks-%C2%A311-billion-fx-failings-and-announces-industry-wide (accessed: 31.07.2018); Final notices: Citibank N.A. [Electronic resource] // Financial Conduct Authority [Site]. – URL: https://www.fca.org.uk/your-fca/documents/final-notices/2014/citibank-na (accessed: 31.07.2018); Final Notice of FCA for HSBC Bank Plc. [Electronic resource] // Financial Conduct Authority [Site]. – URL: https://www.fca.org.uk/your-fca/documents/final-notices/2014/hsbc-bank-plc (accessed: 31.07.2018); Final Notice of FCA for JPMorgan Chase Bank N.A. [Electronic resource] // Financial Conduct Authority [Site]. – URL: https://www.fca.org.uk/your-fca/documents/final-notices/2014/jpmorgan-chase-bank (accessed: 31.07.2018); Final Notice of FCA for The Royal Bank of Scotland Plc. // Financial Conduct Authority [Site]. – URL: https://www.fca.org.uk/your-fca/documents/final-notices/2014/royal-bank-of-scotland (accessed: 31.07.2018); Final Notice of FCA for UBS AG. [Electronic resource] // Financial Conduct Authority [Site]. – URL: https://www.fca.org.uk/your-fca/documents/final-notices/2014/ubs-ag (accessed: 31.07.2018).

[264] Bank of Scotland's fax blunder leads to fine. [Electronic resource] // BBC News [Site]. – URL: https://www.bbc.com/news/business-23572574 (accessed: 31.07.2018).

[265] FCA fines former investment banker for sharing confidential information over WhatsApp. [Electronic resource] // Financial Conduct Authority [Site]. – URL: https://www.fca.org.uk/news/press-releases/fine-former-investment-banker-sharing-confidential-information-whatsapp (accessed: 31.07.2018).

Оценка соотношения права на сохранение банковской тайны с другими правами осуществляется в рамках каждого конкретного дела.

Соотношение процедур AML и права на справедливое судебное разбирательство (ст.6 Конвенции о защите прав и основных свобод)[266]. Суд установил, что сообщение банка о подозрении клиента в отмывании денег допускается и считается пропорциональным ограничением.

В части вопроса о порядке и условиях передачи сведений, составляющих банковскую тайну, третьим лицам, а также аффилированным лицам и аудиторам, ключевое дело, касающееся банковской тайны – это дело Tournier v National Provincial and Union Bank of England (1924)[267]. В деле указывается, что в контракте между клиентом и банком подразумевается, что последний будет хранить конфиденциальность клиентов. При этом объем обязанности по сохранению конфиденциальности не является абсолютным. В частности, были установлены следующие случаи, позволяющие банку не соблюдать требование о конфиденциальности:

- когда раскрытие основано на подразумеваемом или явно выраженном согласии клиента
- когда интересы банка требуют такого раскрытия
- когда раскрытие является обязательным с точки зрения закона
- когда раскрытие необходимо в целях соблюдения публичных интересов.

Порядок и условия передачи сведений, составляющих банковскую тайну в той части, в которой они относятся к персональным данным, определены в Законе о ПД.

В части порядка и условий передачи сведений, составляющих банковскую тайну, третьим лицам, а также аффилированным лицам и аудиторам применительно к персональным данным, см. соответствующий раздел о медицинской тайне. Порядок и условия передачи сведений государственным органам рассмотрены ниже.

К трансграничной передаче применяются требования, аналогичные случаю с медицинской тайной в силу того, что основные ограничения обусловлены законодательством о персональных данных. Кроме того трансграничная передача сведений может осуществляться в рамках оказания взаимной юридической помощи по уголовным делам (в

[266] K LTD v. National Westminster Bank pls. [Electronic resource]: Judgment of Royal Courts of Justice Strand, London dated of 19 July 2006 // BAILII [Site]. – URL: http://www.bailii.org/ew/cases/EWCA/Civ/2006/1039.html (accessed: 31.07.2018).

[267] Tournier v. National Provincol and Union Bank of England / Там же.

соответствии с Crime (International Cooperation) Act 2003[268]) и Proceeds of Crime Act 2002 (External Requests an Orders) Order 2005.[269] Указанные законы позволяют Великобритании искать, предоставлять помощь разными способами, в том числе, предоставлять банковскую информацию в связи с уголовными расследованиями.

В отношении передачи сведений без согласия субъектов следует отметить, что, с точки зрения Закона о ПД и GDPR согласие – это лишь одно из нескольких оснований обработки персональных данных. Таким образом, по умолчанию, допустима обработка данных, относящихся к банковской тайне при наличии иных, помимо согласия, оснований для обработки. Порядок и условия передачи сведений государственным органам рассмотрены ниже.

Изъятий из режима охраны сведений, составляющих банковскую тайну, в целях обеспечения возможности обработки накопленных данных для достижения социальных, государственных и экономических целей, в процессе анализа не обнаружено. Статистические банковские данные опубликовываются Банком Англии[270].

К случаям доступа третьих лиц к данным, составляющим банковскую тайну, с согласия субъекта, применимы общие положения законодательства о персональных данных. Администрирование согласий субъектов банковской тайны на обработку сведений, составляющих банковскую тайну и/или их передачу третьим лицам (в т.ч. наличие права субъекта определять порядок использования таких сведений, делегирования права на выдачу согласий, отзыва согласий на их сбор, обработку и/или передачу и т.д.) подчиняется общим правилам, установленным в GDPR.

Специальные нормы по идентификации субъектов тайн не выявлены.

Основные акты, регулирующие раскрытие данных правоохранительным органам (перечень не исчерпывающий):

- Proceeds of Crimes Act 2002[271]

[268] Crime (International Co-operation) Act 2003 [Electronic resource] // Legislation.gov.uk [Site]. – URL: https://www.legislation.gov.uk/ukpga/2003/32/contents (accessed: 31.07.2018).

[269] Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005 [Electronic resource] // Legislation.gov.uk [Site]. – URL: http://www.legislation.gov.uk/uksi/2005/3181/contents/made (accessed: 31.07.2018).

[270] Statistics [Electronic resource] // Bank of England [Site]. – URL: https://www.bankofengland.co.uk/statistics (accessed: 31.07.2018).

[271] Proceeds of Crime Act 2002 [Electronic resource] // Legislation.gov.uk. [Site]. – URL: http://www.legislation.gov.uk/ukpga/2002/29/contents (accessed: 31.07.2018).

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 No. 692[272]
- Terrorism Act 2000[273]

Уполномоченным органом в данной сфере является Национальное агентство по борьбе с преступностью (National Crime Agency, NCA)[274].

Наиболее серьезное вмешательство в банковскую тайну предусмотрено в ст.330 Proceeds of Crimes Act 2002. В частности криминализованы действия по непредставлению отчета или нераскрытию сведений, подозрений в отмывании денег уполномоченному органу или ответственному сотруднику по финансовому мониторингу. Раскрытие информации в таком случае не считается нарушением тайны. Может быть раскрыта информация о знании или подозрении в отмывании денег, информация о личности лица, подозреваемого в отмывании денег, и информация о местонахождении денег или имущества. При этом должны быть соблюдены следующие три условия:

- информация должна быть предоставлена лицу, которое раскрывает ее, в связи с осуществляемой им торговлей, профессией, бизнесом или работой;
- информация должна давать основания знать или подозревать или иметь разумные основания для подозрений в отмывании денег;
- разглашение должно быть осуществлено соответствующему лицу (то есть полицейскому, сотруднику налогово-таможенной службы ее Величества, ответственному сотруднику по финансовому мониторингу). При этом существует механизм подготовки официальных отчетов Национальному агентству по борьбе с преступностью в рамках подготовки отчета о подозрительной деятельности.

Государственный секретарь может предусмотреть форму и способ раскрытия такой информации. В настоящее время в NCA действует онлайн-система подготовки отчетов о подозрительной деятельности, а также руководства по подготовке отчетов в бумажном

[272] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 No. 692 [Electronic resource] // Legislation.gov.uk. [Site]. – URL: http://www.legislation.gov.uk/uksi/2017/692/made#regulation-10-1 (accessed: 31.07.2018).

[273] Terrorism Act 2000 [Electronic resource] // Legislation.gov.uk. [Site]. – URL: http://www.legislation.gov.uk/ukpga/2000/11 (accessed: 31.07.2018).

[274]National Crime Agency [Electronic resource] // National Crime Agency [Site]. – URL: http://www.nationalcrimeagency.gov.uk/ (accessed: 31.07.2018).

виде[275]. При раскрытии такой информации банку запрещено информировать об этом своего клиента под страхом ответственности.

Согласно The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 No. 692 ст.66 (1) контролирующий орган может направить уведомление банку с требованием предоставить определенную информацию или документы (или информацию и документы, соответствующие определенному описанию), посетить уполномоченного сотрудника в указанное время и месте для ответа на его вопросы.

Такие полномочия могут осуществляться только в отношении информации или документов, которые разумно требуются надзорному органу в связи с осуществлением им какой-либо из своих надзорных функций.

Согласие на обработку сведений, составляющих банковскую тайну, аналогичны согласиям на обработку иных персональных данных. Способ получения, передачи и хранения также аналогичен общим требованиям, установленным GDPR.

Положениями The Network and Information Systems Regulations 2018[276] предусматриваются меры, направленные на обеспечение ***безопасности критически важных IT систем*** в важнейших секторах экономики, в том числе, в банковском секторе. Требования будут применяться к оператором таких услуг, а также к поставщикам информационных услуг. В качестве некоторых требований можно отметить обязанность уведомлять об инцидентах безопасности уполномоченным органам.

Кроме того в ст.98 Положения о платежных услугах (финансовые сервисы и рынки) № 752 2017 г.[277] указывается, что каждый провайдер сервиса должен утвердить программу с мерами защиты от воздействия и контрольными механизмами в отношении производственных рисков и рисков безопасности. Каждый провайдер должен предоставить FCA действительную и комплексную оценку таких рисков, которые могут возникнуть в связи с предоставляемыми сервисами (оказываемыми услугами).

Соединенные Штаты Америки

[275] How to report SARs. National Crime Agency [Electronic resource] // National Crime Agency [Site]. – URL: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu/how-to-report-sars (accessed: 31.07.2018).

[276] The Network and Information Systems Regulations 2018 No. 506 [Electronic resource] // Legislation.gov.uk. [Site]. – URL: https://www.legislation.gov.uk/uksi/2018/506/made (accessed: 31.07.2018).

[277] The Payment Services Regulations 2017 “Financial Services and Markets” 2017 No. 752 [Electronic resource] // Legislation.gov.uk. [Site]. – URL: http://www.legislation.gov.uk/uksi/2017/752/pdfs/uksi_20170752_en.pdf (accessed: 31.07.2018).

В 1961 году дело *Peterson v. Idaho First National Bank*[278] утвердило принцип, согласно которому раскрытие информации банком незаконно, если клиент и банк оговорили в договоре то, что такое разглашение информации является недопустимым. Данный принцип в деле *Indiana National Bank v. Chapman* нашел свое исключение, в связи с которым раскрытие информации, относимой к банковской, допускается, если это требуется для поддержания публичных интересов. На сегодняшний день вышеназванные принципы переросли в нормативно-правовые акты федерального уровня, которые предметом своего регулирования имеют банковскую тайну и сведения ее составляющие: Закон о праве на финансовую тайну (RFPA)[279], Закон о банковской тайне (BSA), Закон о добросовестном предоставлении кредитной информации (FCRA)[280], Закон Gramm-Leach-Bliley ("GLBA")[281].

GLBA регулирует сбор, использование, защиту и раскрытие (передачу) финансовыми организациями непубличной личной информации потребителей. Целью закона является ограничение передачи такой информации и установление обязанности по уведомлению потребителей об обработке персональных данных.

Перечисленные выше нормативно-правовые акты не содержат понятия банковской тайны.

Так как США относится к семье общего права, для него характерно явление прецедента как одного из видов нормотворчества, поэтому, во многом, статутное право не закрепляет принципов формирования состава сведений, относимых к понятию банковской тайны. Та или иная информация понимается в качестве относящейся к банковской тайне, исходя из конкретного рассматриваемого случая, а критерием формирования является отнесение признаков той или иной информации под конкретное нормативно-правовое регулирование, перечисленное в п. 3.2.1.

---

[278] Supreme Court of Idaho. Peterson v. Idaho First National Bank No.9027 [Electronic resource] // Google Scholar [Site]. – URL: https://scholar.google.ru/scholar_case?case=13922878689066094550&q=Peterson+v.+Idaho+First+National+Bank&hl=en&as_sdt=2006&as_vis=1 (accessed: 31.07.2018).

[279] THE RIGHT TO FINANCIAL PRIVACY ACT [Electronic resource] // U.S. Government Publishing Office [Site]. – URL: https://www.gpo.gov/fdsys/pkg/CFR-2011-title31-vol1/pdf/CFR-2011-title31-vol1-part14.pdf (accessed: 31.07.2018).

[280] THE FAIR CREDIT REPORTING ACT [Electronic resource] // U.S. Government Publishing Office [Site]. – URL: https://www.gpo.gov/fdsys/pkg/CFR-2011-title16-vol1/pdf/CFR-2011-title16-vol1-chapI-subchapF.pdf (accessed: 31.07.2018).

[281] THE GRAMM–LEACH–BLILEY ACT [Electronic resource] // U.S. Government Publishing Office [Site]. – URL: https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf (accessed: 31.07.2018).

Долгое время США не рассматривали информацию о транзакциях и прочую финансовую информацию в качестве подпадающей под защиту Четвертой Поправки(*United Stated v. Miller*), и только после введения Закона о частной жизни (Privacy Act of 1974) записи, содержание персональные данные, включая финансовую информацию, стали объектом защиты.

На сегодняшний день вышеназванный Закон GLBA содержит определение «непубличной персональной информации»[282], под которой понимается финансовая информация, относящаяся к определенному потребителю (физическому лицу), (i) предоставленная потребителем финансовой организации, (ii) сформированная в результате любой сделки с потребителем или любой услуги, выполняемой для потребителя или (iii) полученная финансовой организацией иным способом.

Следующие сведения составляют банковскую тайну: (1) сведения о клиентах кредитной организации и о корреспондентах клиентов; (2) сведения об операциях, счетах и вкладах клиентов и корреспондентов, (3) иная информация, содержащаяся в записях (records) финансовой организации.

Согласно рекомендациям Экспертного совета по финансовым институтам (FFIEC), к «чувствительной» информации потребителя относится: имя, адрес или номер телефона в сочетании с номером социального страхования, номером кредитной или дебетовой карты или личным идентификационным номером или паролем, которые позволят получить доступ к банковскому счету потребителя. Чувствительная информация о потребителе также включает любую комбинацию, позволяющую кому-либо войти в систему или получить доступ к учетной записи потребителя, например, имя пользователя и пароль или пароль и номер учетной записи.[283]

Ввиду секторального подхода законодательного регулирования в США, сведения, составляющие банковскую тайну, могут одновременно охраняться как иные виды тайн или иметь статус информации ограниченного доступа по иным основаниям, в том числе: сведения о денежных переводах одновременно охраняются как тайна связи; сведения о вкладах, счетах, операциях по счету и иная подобная информация как тайна частной жизни;

---

[282] 15 U.S.C. §6809(4) [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/uscode/text/15/6809 (accessed: 09.08.2018).

[283] The Federal Financial Institutions Examination Council / Final Guidance on Response Programs Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice – April 1, 2005 [Electronic resource] // Federal Deposit Insurance Corporation [Site]. – URL: https://www.fdic.gov/news/news/financial/2005/fil2705.html (accessed: 31.07.2018).

сведения о клиенте и его корреспонденте как персональные данные, кроме того банковская и налоговая тайна, ввиду схожих между собой предметов регулирования, пересекаются во многих случаях.

Как указано ранее, некоторые сведения составляющие банковскую тайну могут одновременно охраняться как иные виды тайн.

Защита прав субъектов банковской тайны обеспечивается наличием юридической ответственности за неправомерное разглашение (передачу) финансовой информации, относимой к конкретному субъекту, за нарушение процедур уведомления потребителей и сбора согласий и т.д. (подробнее см. ниже).

За нарушение банковской тайны предусмотрены следующие виды ответственности.

Банк, не соблюдающий FCRA, может быть привлечен к гражданской (материальной) ответственности в виде реального ущерба и/или убытков, взыскиваемых в порядке наказания (если противоправное деяние совершено умышленно)[284].

Кроме того, предусмотрена административная ответственность в виде штрафов за несоблюдение законов, привлечение к ответственности осуществляется Федеральной торговой комиссией.

Несоблюдение GLBA влечет уголовную (до 100 000 000 долларов США за каждый инцидент, если нарушителем является юридическое лицо) и гражданскую ответственность (до 100 000 долларов США за каждый инцидент).

На сегодняшний день существует большое количество споров вокруг механизма использования opt-out.

Согласно GLBA под потребителем понимается «лицо, которое получает от финансовой организации финансовые продукты или услуги, которые должны использоваться в первую очередь для личных, семейных или домашних целей, а также его законный представитель»[285]. В отличие от и иных юрисдикций, например, Японии, фактический состав сведений в США зависит от принадлежности потребителя к институту, в данном случае – к финансовой организации, но не является характеристикой самих сведений[286].

---

[284] 15 U.S.C. §1691n [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/uscode/text/15/1691 (accessed: 09.08.2018).

[285] 15 U.S.C. § 6809(9) [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/uscode/text/15/6809 (accessed: 09.08.2018).

[286] Ryan L. Waggoner Privacy of Personal Information in the Financial Services Sectors of the United States and Japan: The Gramm-Leach-Bliley Act and the Financial Services Agency Guidelines [Electronic resource] // Moritz

GLBA содержит (1) обязанность ввести риск ориентированную в6нутреннюю программу информационной безопасности в финансовой организации, (2) обязанность уведомлять потребителей о передаче их информации в некоторых ситуациях, (3) норму о пассивном согласии (opt-out), при соблюдении которой согласие потребителя на передачу сведений предполагается, пока потребитель не ответит на запрос отказом. Известны рекомендации Экспертного совета по финансовым институтам (FFIEC).

Финансовая организация, рассматривающая передачу данных из неамериканской юрисдикции в США, должна учитывать, что записи, содержащие финансовую информацию (financial records), подлежат учету и контролю со стороны широкого круга американских регулирующих и правоохранительных органов.

В законодательстве США имеется перечень случаев, при которых сведения могут передаваться без уведомления:

(1) Финансовая организация может раскрывать непубличную личную информацию потребителей в соответствии с требованиями федеральных или законов штатов, правилами и другими применимыми правовыми нормами.

(2) Финансовое учреждение может раскрывать непубличную личную информацию потребителей для ответа на запрос в рамках гражданского, уголовного расследования, а также по запросам суда или федеральных, государственных или местных органов власти и других целей, предусмотренных законом.

(3) Финансовое учреждение может раскрывать непубличную личную информацию потребителей для защиты или предотвращения фактического или потенциального мошенничества, несанкционированных транзакций и иных запрещенных законом действий.

(4) В той мере, в какой это разрешено или требуется в соответствии с нормами закона и в соответствии с Законом о праве на финансовую неприкосновенность 1978 года (RFPA), финансовое учреждение может раскрывать непубличную личную информацию правоохранительным органам для расследования по вопросам, касающимся общественной безопасности.

GLBA не запрещает передачу финансовой информации, относящейся к конкретному лицу, в адрес аффилированных компаний. Однако Закон о добросовестном предоставлении кредитной информации (FCRA) указывает, что такая передача аффилированным компаниям *в*

College of Law [Site]. – URL: http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Waggoner.pdf (accessed: 31.07.2018).

целях маркетинга должна раскрываться потребителям согласно установленной процедуре: (1) факт передачи должен быть четко и явно раскрыт потребителю в письменной форме или, если потребитель согласен, в электронном виде в кратком уведомлении, (2) потребителю должна быть предоставлена разумная возможность и разумный и простой способ отказаться от передачи этой информации, (3) потребитель не должен отказаться от такой передачи (opt-out).

Кроме того передача сведений может осуществляться в адрес третьих лиц (не аффилированных компаний) также в рамках процедуры opt-out[287]. Кроме того, финансовая организация не имеет права раскрывать, кроме агентства по предоставлению отчетности, номер счета или код доступа от счета кредитной карты, депозитного счета и т.д. любому не аффилированному с финансовой организацией лицу для использования в телемаркетинге, прямом маркетинге или другом виде маркетинга, осуществляемого посредством электронной почты.

Согласие opt-out не применимо к третьим лицам (не аффилированным компаниям), если (1) между ним и финансовой организацией заключен контракт о признании и хранении данной информации как конфиденциальной, т.е. третье лицо не может использовать такую информацию для раскрытия ее иным лицам[288] *или* если (2) третье не аффилированное лицо исполняет функцию финансовой организации от ее имени.

Наконец, требования к уведомлению и opt-out также не применимы к поставщикам услуг (обслуживающим компаниям) и к проектам совместного маркетинга, если (1) третье не аффилированное лицо исполняет функцию финансовой организации от ее имени и если (2) финансовая организация раскрывает сведения о потребителе этим третьим лицам, поскольку это необходимо для осуществления, администрирования или принудительного исполнения транзакции, на осуществление которой потребитель дал разрешение.

Субъект данных (потребитель) не имеет права требовать изменения, удаления, доступа, добавления персональных данных, хранимых в финансовой организации.[289]

GLBA в разделе 501(b) указал на необходимость принятия мер информационной безопасности для защиты финансовой информации потребителей. Во исполнение данной

---

[287] 15 U.S.C. §6802 (b) [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/uscode/text/15/6802 (accessed: 09.08.2018).

[288] A Legal Guide To Privacy And Data Security [Electronic resource] // Minnesota.gov portal [Site]. – URL: https://mn.gov/deed/assets/legal-guide-to-privacy-and-data-security_tcm1045-133708.pdf (accessed: 31.07.2018).

[289] 15 U.S.C. §§ 6801–6809 [Electronic resource] // Legal Information Institute [Site] – URL: https://www.notarylearningcenter.com/pdf/GrammLeachBliley.pdf (accessed: 09.08.2018).

нормы Федеральной торговой комиссией были приняты Правила о мерах безопасности (Safeguards Rule)[290]. Согласно 16 CFR 314.3 финансовой организацией должны быть приняты стандарты защиты информации о потребителях, в частности должна быть разработана программа информационной безопасности для целей обеспечения безопасности и конфиденциальности информации о потребителях, для целей защиты информации от любых ожидаемых угроз, а также от несанкционированного доступа, который может привести к существенному ущербу потребителей. Программа информационной безопасности должна периодически пересматриваться.

К мерам информационной безопасности относятся следующие процедуры, например[291]: (1) проверка анкет перед наймом сотрудников, которые будут иметь доступ к информации о потребителях, (2) подписание каждым новым сотрудником соглашения о конфиденциальности, (3) предоставление доступа к информации о пользователях только тем сотрудникам, у которых есть должностные обязанности с взаимодействием с такой информацией, (4) использование всеми сотрудниками «сильных» паролей, которые должны периодически меняться, (5) разработка политик для надлежащего использования и защиты ноутбуков, сотовых телефонов или других мобильных устройств, (6) обучение сотрудников основам информационной безопасности, (7) шифрование конфиденциальной информации о потребителях при передаче через общедоступные сети связи и т.д.

Сингапур

Банковская тайна в Сингапуре охраняется, в первую очередь, Законом о банках (Banking Act), который вводит такие понятия как «банк в Сингапуре», «потребитель», «информация о потребителе» и т.д. Закон охватывает все банки, учрежденные в Сингапуре, а также отделения зарубежных банков, находящихся в Сингапуре; оба типа банков обязаны получить установленную законом лицензию. Данный нормативно-правовой акт не содержит понятия банковской тайны.

[290]Federal Trade Commission 16 CFR Part 314 Standards for Safeguarding Customer Information; Final Rule – May 23, 2002 [Electronic resource] // Federal Trade Commission [Site]. – URL: https://www.ftc.gov/sites/default/files/documents/federal_register_notices/standards-safeguarding-customer-information-16-cfr-part-314/020523standardsforsafeguardingcustomerinformation.pdf (accessed: 31.07.2018).

[291]Financial Institutions and Customer Information: Complying with the Safeguards Rule [Electronic resource] // Federal Trade Commission [Site]. – URL: https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying (accessed: 31.07.2018).

Так как Сингапур относится к семье общего права, для него характерно явление прецедента как одного из видов нормотворчества, поэтому, во многом, статутное право не закрепляет принципов формирования состава сведений, относимых к понятию банковской тайны. Та или иная информация понимается в качестве относящейся к банковской тайне, исходя из конкретного рассматриваемого случая, а критерием формирования является отнесение признаков той или иной информации под конкретное нормативно-правовое регулирование.

На сегодняшний день вышеназванный Закон о банках содержит определение «информация о потребителе», под которой понимаются номера банковских счетов потребителя, сведения о суммах на счетах и сейфах (депозитах). В деле *PSA Corp Ltd. V Korea Exchange Bank* было указано, что информация должна пониматься расширительно, понятие должно включать в себя информацию в документах банка, а также всю относящуюся к счету и самому потребителю информацию. Также было отмечено, что при невозможности идентификации потребителя такая информация может быть передана (раскрыта), так как не содержит персональных данных. Например, в деле *Teo Wai Cheong v. Credit Industriel et Commercial* сказано, что записи телефонных разговоров с клиентами банка возможно передавать (раскрывать) третьим лицам, если вместо имен клиентов в информации о звонке будут обозначены обезличенные идентификаторы «A», «B», «C» и т.д.

Ввиду особенностей правового регулирования Сингапура, сведения, составляющие банковскую тайну, могут одновременно охраняться как иные виды тайн или иметь статус информации ограниченного доступа по иным основаниям, в том числе: сведения о денежных переводах одновременно охраняются как тайна связи; сведения о вкладах, счетах, операциях по счету и иная подобная информация как тайна частной жизни; сведения о клиенте и его корреспонденте как персональные данные, кроме того банковская и налоговая тайна, ввиду схожих между собой предметов регулирования, пересекаются во многих случаях.

Как указано выше, некоторые сведения составляющие банковскую тайну могут одновременно охраняться как иные виды тайн, включая тайну частной жизни, тайну связи.

Защита прав субъектов банковской тайны обеспечивается наличием юридической ответственности за неправомерное разглашение (передачу) финансовой информации, относимой к конкретному субъекту, за нарушение процедур уведомления потребителей и сбора согласий и т.д.

За нарушение банковской тайны предусмотрены следующие виды ответственности.

Банк, не соблюдающий ст. 47 Закона о банках, может быть привлечен к гражданской (материальной) ответственности). Кроме того, предусмотрена уголовная ответственность за разглашение информации для должностных лиц, например, в 2011 году бывший менеджер был привлечен к уголовной ответственности за разглашение банковской информации клиентов и был приговорен к 18 неделям тюремного заключения[292].

Фактический состав не закреплён исчерпывающим образом, однако, как было отмечено ранее, в деле *PSA Corp Ltd. V Korea Exchange Bank* указан критерий отнесения той или иной и информации к охраняемой в рамках банковской тайны.

Закон о банках (Banking Act) указывает, что банковская тайна не является абсолютной, раскрытие информации и ее передача возможна при определенных условиях, перечисленных в Приложении 3 к вышеназванному закону. Кроме того, раскрытие информации о пользователях возможно на основании одного из восьми законодательных актов, к примеру, Уголовно-процессуального кодекса, для целей расследования и подачи заявления касательно подозрения в совершении преступления. Раскрытию подлежит, при определенных условиях, информация об имени потребителя, личности, задолженности, дате прекращения оказания банковских услуг потребителю.

Приложение 3 Закона о банках разделяет два вида раскрытия информации: (1) дальнейшее раскрытие такой информации возможно и (2) любое дальнейшее раскрытие информации невозможно[293]. Например, строгие ограничения вводятся на передачу информации от банка своим аффилированным организациям, учрежденным не в Сингапуре. Подчас отсутствие согласия потребителя ведет к тому, что конечный получатель такой информации, например, аффилированное лицо банка, не имеет права ее в дальнейшем передавать иным третьим лицам.

По умолчанию раскрытие информации может быть совершено с согласия физического лица (потребителя). Законодательство Сингапура прямо указывает, что договор об оказании банковских услуг не может быть одновременно согласием на обработку персональных данных, а в 1984 году было введено дополнительное требование об обязательном *письменном* согласии, которое должно быть приложено банком для подписания в виде отдельного

[292]Jail for relationship manager who sold details of bank clients [Electronic resource] // Caveat Emptor Singapore [Site]. – URL: http://caveat-emptor-singapore.blogspot.com/2011/03/jail-for-relationship-manager-who-sold.html (accessed: 31.07.2018).

[293]Third Schedule Section 47 Disclosure of information Part I / Further Disclosure Not Prohibited [Electronic resource] // Singapore Statutes Online [Site]. – URL: /https://sso.agc.gov.sg/Act/BA1970?ProvIds=Sc3-#Sc3- (accessed: 31.07.2018).

документа перед оказанием банковских услуг. Таким образом, без *письменного* согласия потребителя передача его информации не может происходить, если только такое раскрытие информации не подпадает под исключения.

Нерешенным вопросом для законодательства Сингапура является порядок уведомления физических лиц о произведенном раскрытии (передаче) их информации.

В законодательстве Сингапура имеется перечень случаев, при которых сведения могут передаваться без согласия клиента банка, данные случаи определены достаточно подробно в Приложении 3 к Закону о банках:

- выдача завещания и проведение процедур в рамках наследственного права;
- в случае банкротства клиента для лиц, которые имеют права запрашивать такую информацию;
- в случае судебного разбирательства (перечень лиц и случаев ограничен);
- если раскрытие информации необходимо для соблюдения поручения и т.д.

Закон о банках предусматривает, что субъект персональных данных дает письменное согласие, а в случае смерти лица – его законный представитель (representative)[294]. Стоит отметить, что несмотря на буквальное толкование, юристы Сингапура трактуют норму расширительно, включая возможность передачи.[295]

Нормативно-правовым актом, регламентирующим противодействие отмыванию преступных доходов является Закон о коррупции, наркоторговле и иных тяжких преступлениях (CDSA). Согласно закону информация может быть раскрыта на основании судебного запроса в рамках проведения расследования. Корме того, закон налагает ответственность на граждан, а также на финансовые учреждения, сообщать о нарушениях закона, а также о всех подозрительных транзакциях, которые могут свидетельствовать о преступных схемах. Согласно закону финансовые организации обязаны хранить финансовую информацию, а также информацию, подпадающую под банковскую тайну, в течение пяти лет.

Закон об Управлении денежно-кредитного обращения (Monetary Authority of Singapore Act) предусматривает необходимость проведения комплексной юридической оценки клиента, хранение всех записей, содержащих информацию клиента, а также сообщения

[294] Banking Act – Revised March 31, 2008 [Electronic resource] // Singapore Statutes Online [Site]. – URL: https://sso.agc.gov.sg/Act/BA1970#Sc3- (accessed: 31.07.2018).

[295] Booysen S., Neo D. Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres Around the World. - Cambridge University Press, 2017. – PP. 278-287.

государственным органам всей подозрительной информации о транзакциях от всех финансовых организаций Сингапура.

Как было указано ранее, обязательно письменное согласие клиента банка для последующей передачи третьим лицам.

К финансовым организациям предъявляются общие требования об информационной безопасности.

Южная Корея

К деятельности финансовых учреждений применяются требования, содержащиеся в законе «О кредитной информации», Законе «О банках», Законе «О страховании бизнеса», Законе «Об электронных транзакциях», иных законах, а также актах Комиссии по Финансовым Услугам.[296] Правила об охране информации, которая может охраняться как банковская тайна, в целом сводятся к общим правилам, отмеченным выше. Регулирование финансовых транзакций в Корее содержится в Законе «Об электронных финансовых транзакциях», а также в международных договорах Кореи.

Для целей настоящего исследования необходимо отдельно рассмотреть вопрос охраны кредитной информации, поскольку данный вопрос детально урегулирован в законодательстве Южной Кореи.

Порядок и условия передачи сведений, составляющих тайну, третьим лицам, а также аффилированным лицам и аудиторам. В Корее достаточно подробно урегулирована деятельность компаний, собирающих кредитную информацию. При сборе такой информации, компании должны чётко определить цель, ради которой осуществляется поиск и сбор информации, при этом поиск и сбор должен производиться только с использованием обоснованных и законных мер, необходимых для применения в контексте обозначенных целей. Кредитные организации в большинстве случаев не могут осуществлять сбор информации с ограниченным доступом (национальная безопасность, коммерческая тайна, результаты научно-технической деятельности, информация о политических убеждениях).

Изъятия из режима охраны в социальных, государственных, экономических

[296] Kwang Bae Park, Ju Bong Jang The Privacy, Data Protection, and Cybersecurity Law Review – Edition 4 – December, 2017 [Electronic resource] // The Law Reviews [Site]. – URL: https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151290/korea (accessed: 31.07.2018).

целях. Государственные органы обладают правом на доступ к финансовым данным частного сектора в двух случаях:

1. Государственные органы запрашивают у компаний, осуществляющих сбор кредитной информации;
2. Государство осуществляет самостоятельный сбор финансовой информации в рамках администрирования государственной программы.

1. **Государственные органы запрашивают у компаний, осуществляющих сбор кредитной информации**

По общему правилу, информация о предоставленных кредитах и гарантиях может быть раскрыта третьим лицам только по согласию субъекта такой информации. В общем исключения из этого правила сводятся к следующим ситуациям:

- Имеется решение (приказ) суда о раскрытии информации;
- В случае крайней необходимости, когда речь идёт о спасении человеческой жизни.

Кроме того, компания, осуществляющая сбор информации о кредитных историях, обязана предоставить такую информацию, когда это предусмотрено налоговым законодательством.(статья 23(7) Закона «О защите кредитной информации»). В соответствии с Законом «О кредитной информации», когда глава публичного института осуществляет письменный запрос для целей, предусмотренных в специальных законах, компания обязана предоставить кредитную информацию.

Государство может получать отдельную финансовую информацию в рамках наблюдения таких компаний Комиссией по Финансовым Услугам. Комиссия уполномочена инспектировать состояние бизнес процессов и финансовое положение компаний, осуществляющих сбор кредитной информации, и требовать информацию, необходимую для осуществления своей деятельности.

2. **Государство осуществляет самостоятельный сбор финансовой информации в рамках администрирования государственной программы.**

Сбор информации в рамках борьбы с отмыванием денежных средств. В соответствии с Законом «О Сообщении и Использовании Специальной Финансовой Информации о Транзакциях», государственные органы имеют доступ к информации финансовых организаций в рамках деятельности по борьбе с отмыванием денежных средств. Финансовые организации обязаны докладывать Специальному Уполномоченному Органу

Финансовой Разведки о любых транзакциях, превышающих 5 000 долларов США (или эквивалента в иностранной валюте) или 10 000 корейских вон, когда у финансовой организации есть основания полагать , что транзакция производится в связи с деятельностью по отмыванию денежных средств, террористической деятельностью или другим преступлением. Также финансовые организации обязаны сообщать информацию об оплате или получении в течение 30 дней наличными суммы, составляющей более 20 000 корейских вон.

Сбор информации в рамках финансовой деятельности государственных организаций. Некоторая финансовая информация находится в распоряжении государственных органов в связи с осуществлением финансовой деятельности (например, Кредитный Гарантийный Фонд Кореи, Технологическая Финансовая Корпорация Кореи).

Израиль

Банковская тайна это обязанность банка по неразглашению информации о клиентах банка третьим лицам без разрешения клиентов. Банковская тайна не является абсолютной: в ряде случаев раскрытие информации допустимо.[297]

Для банковской тайны целесообразно перечислить отдельно перечень нормативных актов, из которых вытекает принцип соблюдения банковской тайны.

1. Основополагающие принципы, закрепившие право каждого лица на тайну личной жизни.

2. Закон о Соблюдении тайны личной жизни 1981 (5741-1981). Особое значение здесь будет иметь часть «В» данного акта, регулирующая вопросы охраны тайны личной жизни информации, содержащейся в базах данных, поскольку в банках данные часто хранятся именно в форме баз данных.

3. В отношении ряда вопросов банковская тайна регулируется законом «Об инвестиционном консультировании», 5755–1995. В соответствии с этим законом, банк обязан сохранять конфиденциальность информации, которую клиенты передали банку, включая документы, переданные банку, их содержимое и иные другие детали актов, в отношении которых банк осуществляет консультирование.

[297] Ruth Plato-Shinar Bank Secrecy in Israel [Electronic resource] // Social Science Research Network [Site]. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427586 (accessed: 08.08.2018).

4. Закон «Об агентах», поскольку банк выступает по отношению к клиенту в качестве агента.

5. Закон «О запрете отмывания денежных средств» содержит обязанность сохранения конфиденциальности на лице, в распоряжении которого попала информация в связи с исполнением обязанностей, возложенных на исполнителей финансовых услуг. Нарушение такой обязанности является основанием для привлечения к уголовной ответственности.

6. Закон «О данных кредитных услуг», 5762–2002 регулирует вопросы, связанные с продажей юридическими лицами данных о кредитных историях при наличии специальной лицензии. Данный закон призван найти баланс между правом на тайну личной жизни, с одной стороны, и коммерческими целями.[298]

Понятие. Понятие «банковская тайна» толкуется широко. Банковская тайна применяется к любым делам и транзакциям клиента вне зависимости от того, связаны ли такие транзакции с частными вопросами клиента или с коммерческими (business). Банковской тайной охраняются, в том числе, имя, адрес, клиента, сам факт наличия банковского аккаунта у клиента. Также не имеет значения, была ли информация получена напрямую от клиента либо от стороннего источника, была ли информация получена до создания аккаунта в банке либо в связи с созданием такого аккаунта либо после закрытия аккаунта. Обязанность по сохранению конфиденциальности не имеет временных ограничений (в том числе, сохраняется после закрытия аккаунта, смерти клиента, ликвидации корпорации).

Обязанность по сохранению конфиденциальности возникает не только перед клиентами банка, но и перед третьими лицами.

В рамках рассмотрения иных видов тайн, резонно рассмотреть следующие виды тайны: коммерческая тайна.

Механизм правовой защиты субъектов состоит из следующих элементов:

(1) Раскрытие информации по общему правилу осуществляется только с согласия субъекта тайны;

(2) Круг субъектов, который может иметь доступ к тайне без согласия субъекта тайны, ограничен;

(3) Случаи, когда допускается разглашение сведений, составляющих тайну

[298] Know Your Customer: Quick Reference Guide [Electronic resource] / Pwc / January, 2013. // PWC [Site]. – URL: https://www.pwc.com/gx/en/financial-services/assets/pwc-kyc-anti-money-laundering-guide-2013.pdf (accessed: 08.08.2018).

коммуникации, ограничены;

(4) Ответственность за неправомерное разглашение сведений, составляющих тайну.

Юридическая ответственность. Уголовная ответственность может наступать в соответствии с Уголовным Кодексом (статья 496):

Лицо, разгласившее информацию, которая стала ему известна в связи с осуществлением его профессиональной деятельности, составляет уголовное правонарушение. Компенсация за такое правонарушение может достигать US $50,000. Ответственность по данной статье наступает вне зависимости от «типов» клиентов или типов дел, однако, ответственность будет наступать только в случае, если информация была имено Предоставлена человеку, а не попала в его распоряжение каким-либо иным способом (например, случайно).

Порядок и условия передачи сведений, составляющих тайну связи, третьим лицам, а также аффилированным лицам и аудиторам. В целом исключения из соблюдения конфиденциальности банковской тайны базируются на принципах раскрытия, имплементированных в английском праве, и сводятся к следующему.

(1) Раскрытие информации обязательно в соответствии с законом;

В этом случае нераскрытие информации будет приводить к нарушению закона.

В рамках данного вида раскрытия, можно выделить следующие основные виды:

a) Раскрытие информации органам власти (полиции, налоговой службе, контроллеру банков, органам безопасности, органам, осуществляющим борьбу с отмыванием денег);
b) По решению суда: когда банк не является стороной в деле;
c) Раскрытие информации, когда банк является стороной по делу.

Тут необходимо упомянуть дело **Sals vs. Sals,** которым был установлен прецедент о том, что в случае если получение информации от банка осуществляется в соответствии с судебным приказом, позиция третьей стороны выслушивается в обязательном порядке. Суд также должен применить тест пропорциональности и соотнести необходимость разглашения информации и последствия её неразглашения, а также установить, что без разглашения информации дело не будет разрешено справедливым образом.

(2) Раскрытие тайны обеспечено общественными интересами;

(3) Интересом банка является необходимость в раскрытии информации;

Данное положение необходимо понимать узко: например, банк выступает в качестве истца по делу о взыскании долга и раскрытие информации необходимо для доказывания его позиции по делу.

(4) Раскрытие происходит с согласия клиента.

В качестве дела, иллюстрирующего необходимость раскрытия банком информации, можно привести дело **Tefahot Mort gage Bank Ltd. vs. Tsabach.** В данном деле покупатели квартир получили кредит от банка на покупку квартиры, принадлежащей другому клиенту банка. В момент оформления кредита банк не раскрыл информацию о том, что клиенты находились в сложной материальной ситуации. В итоге, продавец разорился и покупатели не получили квартиру, которую они должны были приобрести по договору. Верховный Суд вынес решение о том, что в данном случае банк должен был поставить покупателей в известность о том, что в данном случае имеется конфликт интересов и не должен был предоставлять кредит без получения согласия со стороны приобретателей. Поскольку банк не осуществил таких действий, банк обязали выплачивать убытки, которые по его вине возникли у приобретателей квартиры.

Объединенные Арабские Эмираты

В законодательстве ОАЭ не содержится понятия банковской тайны. Однако это является обычной банковской практикой. В том числе некоторые принципы сформулированы в документах, опубликованных Центральным банком ОАЭ. В частности, в Постановлении о финансовых организация №112/2018[299] в п.4 дается понятие конфиденциальных данных, согласно которому конфиденциальные данные – это банковский счет или иная информация, относящаяся к клиенту или сотруднику финансовой организации, который может быть идентифицирован или может быть идентифицирован либо с помощью конфиденциальных данных или с помощью конфиденциальных данных в сочетании с другой информации, которая доступна или может быть доступна для лица, организации.

[299] Finance Companies Regulation (Central Bank of the UAE) Circular No. 112/2018 of 24.04.2018 [Electronic resource] // Central Bank of Arabian Emirates [Site]. – URL: https://centralbank.ae/en/pdf/notices/FinanceCompaniesRegulation.pdf (accessed: 10.08.2018).

В отсутствие понятия банковской тайны, а также широкого определения конфиденциальных данных, сформулированного выше, принцип формирования состава сведений, составляющих банковскую тайну, можно назвать открытым.

Состав сведений, составляющих банковскую тайну, законодательно не определен.

В процессе анализа сведения ограниченного доступа не выявлены.

Поскольку в ОАЭ отсутствует законодательство о персональных данных, разграничить сведения, составляющие банковскую тайну и сведения, составляющие персональные данные, не представляется возможным. Однако в ОАЭ есть несколько свободных экономических зон, на территории которых действуют свое законодательство.

Прежде всего, Закон о персональных данных №1 от 2007 г. (далее – Закон о ПД)[300] действует только на территории и в рамках деятельности свободной экономической зоны – Международного финансового центра Дубай (DIFC). Согласно положениям данного Закона персональные данные – это любые данные относящиеся к идентифицируемому физическому лицу. Понятие конфиденциальных данных, сформулированное Центральным банком, шире, чем понятие, содержащее в Законе о ПД DIFC. Таким образом, данные понятия соотносятся лишь частично. Следовательно, часть сведений, составляющих банковскую тайну, будут являться конфиденциальной информацией, а часть персональными данными.

Механизм правовой защиты прав субъектов банковской тайны заключается в наличии юридической ответственности, за разглашение банковской тайны. Помимо этого, в той части, в которой сведения, составляющие банковскую тайну, являются персональными данными по Закону о ПД DIFC, у субъекта имеются механизмы защиты, предусмотренные в Законе о ПД DIFC. Более подробно см. указанные механизмы защиты в разделе Врачебная тайна в ОАЭ.

Юридическая ответственность наступает на основании ст.378, 379 Уголовного кодекса ОАЭ. Более подробно см. раздел Врачебная тайна в ОАЭ.

В Конституции ОАЭ отсутствуют положения, связанные с защитой тайны личной жизни (за исключением ст.31 о свободе почтовой переписки, передачи телеграфных сообщений и прочих средств связи). В связи с этим выявить соотношение конституционных прав не представляется возможным.

[300] Data Protection Law [Electronic resource] //: DIFC Law No. 2 of 2007. // Dubai International Financial Centre [Site]. – URL: https://www.difc.ae/files/3615/1739/8803/Data_Protection_Law_DIFC_Law_No._1_of_2007.pdf (accessed: 09.08.2018).

Говоря о трансграничной передаче необходимо отметить, что положения об этом содержатся в Основах регулирования хранимых данных и электронных платежных систем[301]. Согласно пп. «d» п. 6.1. провайдер электронных платежных систем обязуется хранить данные всех клиентов и данные о транзакциях только на территории ОАЭ (за исключением свободных экономических зон) в течение 5 лет с даты осуществления транзакции.

Помимо этого в Законе о ПД DIFC предусмотрены требования о передаче персональных данных за предела DIFC. В частности, согласно ст. 11 передача допускается, если обеспечивается адекватный уровень защиты персональных данных, и соответствующие нормативные требования применяются к получателю данных. В Постановлении о персональных данных[302] содержится перечень допустимых юрисдикций. На сегодня туда включены: страны ЕС, а также Уругвай, Канада, Аргентина, Андорра, Гернси, о. Мэн, Фарерские острова. Россия не включена в перечень.

В случае, если государство не включено в указанный перечень, до передача за пределы DIFC допускается при наличии одного из нескольких установленных в ст.12 Закона о ПД DIFC оснований. Например, при наличии письменного согласия; наличия разрешения Комиссара по персональным данным и при этом контролер данных будет применять адекватные меры защиты в отношении таких персональных данных; если это необходимо для выполнения договор между субъектом персональных данных и контролером данных; это предусмотрено законом.

Порядок передачи персональных данных предусмотрен в Законе о ПД DIFC и содержит общие требования к обработке персональных данных (ст.9). Например, с письменного согласия субъекта; когда это необходимо для исполнения договора, стороной которого является субъект; на основании требований закона.

Случаи, условия, порядок передачи сведений, составляющих тайну связи, без согласия субъектов описаны выше.

---

[301] Regulatory Framework For Stored Values and Electronic Payment Systems dated of 01.01.2017 [Electronic resource] // Central Bank of The United Arab Emirates [Site]. – URL: https://www.centralbank.ae/en/pdf/notices/Regulatory-Framework-For-Stored-Values-And-Electronic-Payment-Systems-En.pdf (accessed: 10.08.2018).

[302] Data Protection Regulation (DPR) [Electronic resource] / DIFC Consolidated Version No. 3 (in force on 31.01.2018). // Dubai International Financial Centre [Site]. – URL: https://www.difc.ae/files/4515/1745/7405/Data_Protection_Regulations.pdf (accessed: 09.08.2018).

Изъятия из режима тайны связи в целях обеспечения возможности обработки накопленных данных для достижения социальных, государственных, экономических целей не установлены.

По вопросу о случаях и порядке раскрытия сведений, составляющих тайну связи, в том числе, в форме открытых данных, и принципа раскрытия данных по умолчанию в деятельности органов государственного управления см. Врачебная тайна в ОАЭ.

Возможность доступа третьих лиц к тайне связи с согласия субъекта раскрыта выше. Возможность администрирования согласий субъектов тайны связи на обработку сведений, составляющих тайну связи, и их передачу третьим лицам (в т.ч. наличие права субъекта определять порядок использования таких сведений, делегирования права на выдачу согласий, отзыва согласий на их сбор, обработку и/или передачу и т.д.), а также специальных норм (при их наличии) по идентификации субъектов тайны связи (в т.ч. их законных представителей) в целом не предусмотрена.

1.4. Налоговая тайна

Российская Федерация

Понятие налоговой тайны определяется в Налоговом кодексе РФ (ст. 102 НК РФ). Налоговую тайну составляют любые полученные налоговым органом, органами внутренних дел, следственными органами, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, плательщике страховых взносов, за исключением сведений, отдельно поименованных в п. 1 ст. 102 НК РФ.

В российском законодательстве принципы формирования сведений, составляющих налоговую тайну, не определены. Тем не менее, можно сформулировать следующие принципы на основании системного толкования применимых НПА и судебной практики:

(1) основной принцип - перечень сведений, составляющих налоговую тайну, определяется путем исключения из сведений информации, которая налоговой тайной не является. Такой перечень является закрытым;

(2) сведения, составляющие налоговую тайну, являются таковыми вне зависимости от формы (документ, электронный документ, видеозапись, фотография, иное);

(3) налоговая тайна определяется через исчерпывающий перечень субъектов,

обладающих в силу закона правом обращения к налоговым органам за предоставлением сведений, составляющих налоговую тайну, в указанных в законе целях;

(4) перечень исключений из налоговой тайны направлен на защиту конституционного строя РФ (п.п. 1, 3, 5, 8 п. 1 ст. 120 НК РФ), защиту прав потенциальных контрагентов (п.п. 2, 7, 9, 10, 11, 12, 13 п. 1 ст. 102 НК РФ), формирование учета , исполнение международных договоров (п.п. 4 п. 1 ст. 102 НК РФ), а также включает сведения о государственной регистрации юридических лиц (п.п. 2, 6, 12, 13 п. 1 ст. 102 НК РФ).

К сведениям, составляющим налоговую тайну, относятся любые полученные налоговым органом, органами внутренних дел, следственными органами, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, плательщике страховых взносов, за исключением следующих сведений, перечисленных в п. 1 ст. 102 НК РФ НК РФ:

(1) являющихся общедоступными, в том числе ставших таковыми с согласия их обладателя - налогоплательщика (плательщика страховых взносов);

(2) об идентификационном номере налогоплательщика;

(3) о нарушениях законодательства о налогах и сборах (в том числе суммах недоимки и задолженности по пеням и штрафам при их наличии) и мерах ответственности за эти нарушения;

(4) предоставляемых налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является Российская Федерация, о взаимном сотрудничестве между налоговыми (таможенными) или правоохранительными органами (в части сведений, предоставленных этим органам), в том числе в рамках международного автоматического обмена информацией;

(5) предоставляемых избирательным комиссиям в соответствии с законодательством о выборах по результатам проверок налоговым органом сведений о размере и об источниках доходов кандидата и его супруга, а также об имуществе, принадлежащем кандидату и его супругу на праве собственности;

(6) предоставляемых в Государственную информационную систему о государственных и муниципальных платежах, предусмотренную Федеральным

законом от 27 июля 2010 года N 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

(7) о специальных налоговых режимах, применяемых налогоплательщиками, а также об участии налогоплательщика в консолидированной группе налогоплательщиков;

(8) предоставляемых органам местного самоуправления (органам государственной власти городов федерального значения Москвы, Санкт-Петербурга и Севастополя) в целях осуществления контроля за полнотой и достоверностью информации, представленной плательщиками местных сборов, для расчета сборов, а также о суммах недоимки по таким сборам;

(9) о среднесписочной численности работников организации за календарный год, предшествующий году размещения указанных сведений в информационно-телекоммуникационной сети «Интернет»;

(10) об уплаченных организацией в календарном году, предшествующем году размещения указанных сведений в информационно-телекоммуникационной сети «Интернет», суммах налогов и сборов (по каждому налогу и сбору) без учета сумм налогов (сборов), уплаченных в связи с ввозом товаров на таможенную территорию Евразийского экономического союза, сумм налогов, уплаченных налоговым агентом, о суммах страховых взносов;

(11) о суммах доходов и расходов по данным бухгалтерской (финансовой) отчетности организации за год, предшествующий году размещения указанных сведений в информационно-телекоммуникационной сети «Интернет»;

(12) о постановке на учет в налоговых органах иностранных организаций в соответствии с п. 4.6 ст. 83 НК РФ;

(13) о постановке на учет в налоговых органах физических лиц в соответствии с п. 7.3 ст. 83 НК РФ (речь идет о лицах, не являющихся ИП и оказывающих без привлечения наемных работников услуги физическим лицам для личных, домашних и (или) иных подобных нужд).

Кроме этого, установлено отдельное регулирование для сведений, содержащихся в специальной декларации, представленной в соответствии с Федеральным законом «О добровольном декларировании физическими лицами активов и счетов (вкладов) в банках и о внесении изменений в отдельные законодательные акты Российской Федерации», (и (или) прилагаемых к ней документах и (или) сведениях). Такие сведения признаются налоговой

тайной без исключений, установленных п.п. 1-3 и 5-8 п. 1 ст. 102 НК РФ (п. 8 ст. 102 НК РФ).

Указано, что содержание данных налогового учета (в том числе данных первичных документов) является налоговой тайной (ст. 313 НК РФ).

Сведения, составляющие налоговую тайну, могут одновременно относиться к иным видам сведений ограниченного доступа, например:

(1) сведения, составляющие налоговую тайну, могут содержать персональные данные (например, сведения, содержащиеся в Личном кабинете налогоплательщика);

(2) сведения, составляющие банковскую тайну, становятся налоговой тайной после передачи их субъектам налоговой тайны (налоговый орган и иные субъекты);

(3) при запросе информации, которая составляет профессиональную тайну (адвокатская, аудиторская, иная), налоговый орган обязан обеспечить её конфиденциальность;

(4) так как доступ к сведениям, содержащим налоговую тайну, ограничен органами государственной власти, то данные сведения являются также служебной тайной.

Кроме того, к разглашению налоговой тайны относится, в частности, использование или передача другому лицу информации, составляющей коммерческую тайну (секрет производства), ставшей известной должностному лицу налогового органа, органа внутренних дел, следственного органа, органа государственного внебюджетного фонда или таможенного органа, привлеченному специалисту или эксперту при исполнении ими своих обязанностей (п. 2 ст. 102 НК РФ).

Защита прав налогоплательщиков (плательщиков страховых взносов) в отношении налоговой тайны обеспечивается наличием юридической ответственности разных видов за нарушение режима налоговой тайны: как за нарушение режима хранения такой информации и доступа к ней, так и за разглашение налоговой тайны.

За нарушение налоговой тайны предусмотрены следующие виды ответственности:

(1) Уголовная ответственность (ст. 183 УК РФ).

- Отдельно выделяется ответственность за собирание сведений, составляющих налоговую тайну путем похищения документов, подкупа или угроз, а равно иным незаконным способом – наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет, либо лишением свободы на тот

же срок.

- Незаконные разглашение или использование сведений, составляющих налоговую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе (ч. 2) – наказываются штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до трех лет, либо лишением свободы на тот же срок.
- В случае, если деяния, установленные ч. 2 данной статьи, причинили крупный ущерб (превышающий два миллиона двести пятьдесят тысяч рублей) или были совершены из корыстной заинтересованности, то они наказываются штрафом в размере до одного миллиона пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.
- В случае, если деяния, установленные ч. 2 или ч. 3 данной статьи, повлекли тяжкие последствия, то они наказываются принудительными работами на срок до пяти лет либо лишением свободы на срок до семи лет.
- При этом в случае специальных деклараций: разглашение соответствующих сведений и утрата представленных специальных деклараций и (или) прилагаемых к ним документов и (или) сведений являются основанием для привлечения к уголовной ответственности за незаконное разглашение сведений, составляющих налоговую тайну (п.п. 2 п. 8 ст. 102 НК РФ).

(2) Гражданско-правовая имущественная ответственность за причинение вреда налогоплательщику или его имуществу с возмещением в полном объеме убытков, включая упущенную выгоду, за счет средств федерального бюджета на основании ст. ст. 35 и 103 НК РФ.

(3) Дисциплинарная ответственность в виде увольнения гражданского служащего соответствующего органа в случае разглашения налоговой тайны (п.п. 5 п. 1 ст. 57 закона от 27.07.2004 N 79-ФЗ «О государственной гражданской службе Российской

Федерации»).

Согласно применимым НПА, судебной практике, а также разъяснениям Минфина (ФНС, УФНС), сведения, относящиеся к налоговой тайне, включают в том числе:

(1) сведения, содержащиеся в специальной декларации (и (или) прилагаемых к ней документах и (или) сведениях) (п. 8 ст. 102 НК РФ);

(2) материалы налогового контроля (п. 13 «Обзора судебной практики по вопросам, связанным с участием уполномоченных органов в делах о банкротстве и применяемых в этих делах процедурах банкротства» (утв. Президиумом Верховного Суда РФ 20.12.2016));

(3) сведения, полученные налоговым органом, содержащиеся в первичных документах налогоплательщика (ст. 313 НК РФ);

(4) сведения о наличии либо отсутствии денежных средств на банковском счете налогоплательщика (Письмо УФНС России по г. Москве от 31.12.2008 N 09-17/122410);

(5) сведения о зарегистрированной налогоплательщиком кассовой технике, с применением которой осуществляется реализация товаров, работ, услуг (Письмо УФНС России по г. Москве от 20.06.2008 N 22-12/059038);

(6) сведения о подтверждении налогового статуса (резидентства) гражданина (Письмо ФНС России от 02.12.2015 N ЗН-3-17/4568);

(7) сведения, содержащиеся в Личном кабинете налогоплательщика (Письмо ФНС России от 09.11.2015 N ОА-19-17/276);

(8) запросы всех лиц, за исключением случаев, указанных в статье 102 Кодекса и иных федеральных законах (Письмо Минфина России от 13.02.2015 N 03-02-08/6483);

(9) сведения о доходах налогоплательщика – физического лица (Письмо ФНС РФ от 20.10.2011 N ПА-3-12/3437).

Относительно порядка и условий передачи сведений, составляющих налоговую тайну, можно отметить следующее:

(1) Не является разглашением налоговой тайны предоставление налоговым органом ответственному участнику консолидированной группы налогоплательщиков сведений об участниках этой группы, составляющих налоговую тайну (п. 2.1 ст. 102 НК РФ).

(2) В соответствии с п.п. 1 п. 1 ст. 102 НК РФ налогоплательщик (плательщик

страховых взносов) может выразить согласие на признание сведений (их части), составляющих налоговую тайну, общедоступными.

(3) Сведения, полученные при осуществлении лицами их профессиональной деятельности (в частности, адвоката, аудитора), относятся к профессиональной тайне этих лиц. Как таковая передача им сведений, составляющих налоговую тайну, не осуществляется (см. судебную практику, №1).

(4) Порядок доступа к конфиденциальной информации налоговых органов установлен в Приказе МНС РФ от 03.03.2003 N БГ-3-28/96 «Об утверждении Порядка доступа к конфиденциальной информации налоговых органов». В частности, не допускается предоставление налоговыми органами баз, банков данных, архивов, списков налогоплательщиков и работников налоговых органов, содержащих конфиденциальную информацию, за исключением случаев, предусмотренных федеральным законом, или соглашением об информационном обмене между пользователем и Министерством Российской Федерации по налогам и сборам, заключенным в соответствии с федеральным законом.

(5) В Приказе МВД России от 11.01.2012 N 17 «Об утверждении Перечня должностных лиц системы МВД России, пользующихся правом доступа к сведениям, составляющим налоговую тайну» установлен перечень должностных лиц системы МВД РФ, пользующихся таким правом доступа.

(6) УПК РФ определяет следующие условия доступа следователей к различным сведениям, составляющим налоговую тайну:

- только суд, в том числе в ходе досудебного производства, правомочен принимать решения о производстве выемки предметов и документов, содержащих налоговую тайну (п. 7 ч. 2 ст. 29 УПК РФ);
- если в материалах уголовного дела содержатся сведения, составляющие государственную или иную охраняемую федеральным законом тайну, то у присяжных заседателей отбирается подписка о ее неразглашении (ч. 24 ст. 328 УПК РФ).

(7) В случае необходимости получения сведений, составляющих налоговую тайну в отношении лиц, не участвующих в третейском разбирательстве, Третейский суд с местом арбитража на территории Российской Федерации (за исключением третейского суда в рамках арбитража для разрешения конкретного спора) в случае

возникновения необходимости получения доказательств, требующихся для разрешения спора, вправе обратиться в арбитражный суд субъекта Российской Федерации (районный суд), на территории которого находятся истребуемые доказательства, с запросом о содействии в получении этих доказательств (ст. 74.1 АПК РФ, ст. 63.1 ГПК РФ).

(8) Ст. 9 Федерального закона от 07.08.2001 N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» устанавливает, что предоставление по запросу уполномоченного органа информации и документов органами и организациями, указанными в части первой данной статьи, и Центральным банком Российской Федерации в целях и порядке, которые предусмотрены настоящим этим ФЗ, не является нарушением налоговой тайны.

(9) В п. 1 ст. 13 закона от 15.12.2001 N 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации» указано, что страховщик имеет право, в частности, на получение от налогового органа информации о налогоплательщиках, составляющую налоговую тайну.

(10) Представление источниками формирования кредитной истории информации, определенной статьей 4 данного закона, в бюро кредитных историй в соответствии с настоящей статьей не является нарушением служебной, банковской, налоговой или коммерческой тайны (Федеральный закон от 30.12.2004 N 218-ФЗ (ред. от 31.12.2017) «О кредитных историях»).

Не относятся к налоговой тайне сведения, предоставляемые налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является Российская Федерация, о взаимном сотрудничестве между налоговыми (таможенными) или правоохранительными органами (в части сведений, предоставленных этим органам), в том числе в рамках международного автоматического обмена информацией (п.п. 4 п. 1 ст. 102 НК РФ).

Если законом установлено право запроса и получения сведений, составляющих налоговую тайну, третьим лицом, то согласие на это налогоплательщиков (плательщиков страховых взносов) (не субъектов) не требуется. Субъектом налоговой тайны является налоговый орган, орган внутренних дел, следственный орган, орган государственного внебюджетного фонда и таможенный орган (их должностные лица, привлекаемые ими

специалисты, эксперты).

В настоящее время таких изъятий нет. Тем не менее, в юридических научных кругах такие изъятия обсуждаются. Так, в статье Вайпана В. А. утверждается, что «Развитие цифровой экономики возможно потребует пересмотра принципов защиты различных видов тайны. Это обусловлено необходимостью уточнения порядка передачи третьим лицам сведений, составляющих банковскую тайну, тайну связи, врачебную тайну и т.п., с согласия профессиональных субъектов в целях обеспечения возможности обработки накопленных данных для достижения социальных, государственных и экономических целей»[303].

Относительно случаев и порядка раскрытия сведений, составляющих налоговую тайну, в том числе в форме открытых данных, и принцип раскрытия данных по умолчанию в деятельности органов государственного управления необходимо отметить следующее:

(1) Раскрытие соответствующих сведений допускается только на основании закона и только полномочным лицам (см. п. 3.2.11).

(2) В соответствии с п.п. 1 п. 1 ст. 102 НК РФ налогоплательщик (плательщик страховых взносов) может выразить согласие на признание сведений (их части), составляющих налоговую тайну, общедоступными. В таком случае данные сведения перестают быть налоговой тайной.

(3) Законодатель последовательно расширяет перечень исключений из налоговой тайны. Так, например, Федеральным законом от 01.05.2016 N 134-ФЗ были введены п.п. 10 и п.п. 11 п. 1 ст. 102 НК РФ, которые предполагают раскрытие в сети «Интернет» информации об уплаченных организацией налогов и сборов, а также о суммах доходов и расходов по данным бухгалтерской (финансовой) отчетности.

(4) Относительно принципа раскрытия данных по умолчанию (Open data by default). Открытые данные – информация, размещенная в сети «Интернет» в виде систематизированных данных, организованных в формате, обеспечивающем ее автоматическую обработку без предварительного изменения человеком, в целях неоднократного, свободного и бесплатного использования (п. 1 «Методических рекомендаций по публикации открытых данных государственными органами и органами местного самоуправления, а также технические требования к публикации

[303] Вайпан В.А. Основы правового регулирования цифровой экономики // Право и экономика. – 2017. – № 11. – С. 5-18

открытых данных. Версия 3.0» (утв. протоколом заседания Правительственной комиссии по координации деятельности Открытого Правительства от 29.05.2014 N 4). К налоговой тайне в силу её специфики это не относится.

Возможность доступа третьих лиц к налоговой тайне с согласия субъекта тайны, администрирования согласий субъектов налоговой тайны на обработку сведений, составляющих налоговую тайну, и/или их передачу третьим лицам (в т.ч. наличие права субъекта определять порядок использования таких сведений, делегирования права на выдачу согласий, отзыва согласий на их сбор, обработку и/или передачу и т.д.), а также специальных норм (при их наличии) по идентификации субъектов налоговой тайны (в т.ч. их законных представителей) может быть прокомментирована следующим образом:

(1) Как указано выше, субъект налоговой тайны – соответствующий орган (должностное лицо, привлекаемые эксперт, специалист) (подробнее см. п. 3.2.11). Возможность доступа третьих лиц, не обладающих полномочиями на такой доступ, к налоговой тайне с согласия налогоплательщика, не регулируется законодательно. Делегирование права на выдачу сведений не предполагается (за исключением случаев, предусмотренных законом; например, предоставление сведений на основании ст. 9 Федерального закона от 07.08.2001 N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» не является нарушением налоговой тайны). Порядок использования таких сведений определяется конкретными обязанностями запрашивающего с учетом положений о налоговой тайне. Например, проведение правоохранительным органом ОРМ и запрос им сведений, составляющих налоговую тайну, не предполагает в дальнейшем права на раскрытие этой информации, не предполагает права на передачу этой информации иному лицу (за исключениями, установленными федеральным законами).

(2) Подзаконные акты регулирования соответствующих отношений:
- Приказ ФНС России от 13.01.2012 N ММВ-7-4/6@ «Об утверждении Концепции информационной безопасности Федеральной налоговой службы»;
- Приказ ФНС России от 25.02.2014 N ММВ-7-6/66@ (ред. от 19.06.2018) «Об утверждении Концепции системы управления информационной безопасностью ФНС России»;
- Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении

требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- 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»;
- Приказ МНС РФ от 03.03.2003 N БГ-3-28/96 «Об утверждении Порядка доступа к конфиденциальной информации налоговых органов»;
- Приказ ФНС России от 15.11.2016 N ММВ-7-17/615@ «Об утверждении формы, формата согласия налогоплательщика (плательщика страховых взносов) на признание сведений, составляющих налоговую тайну, общедоступными, порядка заполнения формы, а также порядка его представления в налоговые органы»;
- Постановление Правительства РФ от 10.07.2013 N 584 (ред. от 30.06.2018) «Об использовании федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (вместе с «Правилами использования федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»);

3) Относительно идентификации и аутентификации субъектов налоговой тайны, запрашивающих лиц, налогоплательщиков (плательщиков сборов).

1. Субъекты налоговой тайны (должностные лица).

В качестве средств идентификации/аутентификации выступают цифровые сертификаты (п. 6.3.2 Приказа ФНС России от 13.01.2012 N ММВ-7-4/6@). Рабочая станция (АРМ) Удостоверяющего центра, предназначенная для формирования закрытых ключей и сертификатов пользователей информационных систем налоговых органов, должна размещаться на автономной платформе, обеспечивать работу в автономном режиме и исключать возможность несанкционированного физического соединения с

информационными системами налоговых органов. Формируемые цифровые сертификаты должны соответствовать формату, определенному рекомендациями и стандартами (RFC 5280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile», RFC 4491 «Using the GOST R 34.10-94, GOST R».

2. Запрашивающие лица.

Запрос о предоставлении конфиденциальной информации (далее именуется - запрос) оформляется и направляется в письменном виде на бланках установленной формы фельдсвязью, почтовыми отправлениями, курьерами, нарочными или в электронном виде по телекоммуникационным каналам связи с реквизитами, позволяющими идентифицировать факт обращения пользователя в налоговый орган. Подпись должностного лица, имеющего право направлять запросы в налоговые органы, подтверждается печатью канцелярии пользователя. При направлении запросов по телекоммуникационным каналам связи подпись должностного лица подтверждается электронной цифровой подписью (п. 4, 5 Приказа МНС РФ от 03.03.2003 N БГ-3-28/96).

3. Налогоплательщик (плательщик сборов), о выражении согласия на признание сведений, составляющих налоговую тайну, общедоступными.

Согласие может быть представлено в налоговые органы в письменной форме лично или по телекоммуникационным каналам связи с применением усиленной квалифицированной электронной подписи или через личный кабинет налогоплательщика в соответствии со статьей 11.2 НК РФ в электронной форме (п. 2 Приложения 4 Приказа ФНС России от 15.11.2016 N ММВ-7-17/615@). При представлении Согласия в письменной форме налогоплательщик (плательщик страховых взносов) может представить его в налоговый орган лично либо через своего представителя (п. 2 Приложения 4 Приказа ФНС России от 15.11.2016 N ММВ-7-17/615@).

В части возможности, случаев и объемов предоставления кредитными учреждениями конфиденциальных данных, полученных или сформированных при выполнении требований административного законодательства, например, о противодействии отмыванию преступных доходов, правоохранительным органам и иным органам власти, не указанным в таком административном законодательстве, например, в силу общих полномочий указанных органов власти; критерии оценки соответствующих запросов на предмет законности, обоснованности, конкретности, пропорциональности, отметим следующее.

Ст. 9 закона 07.08.2001 N 115-ФЗ «О противодействии легализации (отмыванию)

доходов, полученных преступным путем, и финансированию терроризма» устанавливает, что предоставление по запросу уполномоченного органа информации и документов органами и организациями, указанными в части первой данной статьи, и Центральным банком Российской Федерации в целях и порядке, которые предусмотрены настоящим федеральным законом, не является нарушением налоговой тайны.

К органам и организациям, указанным в части первой данной статьи относятся: органы государственной власти Российской Федерации, Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования, государственные корпорации и иные организации, созданные Российской Федерацией на основании федеральных законов, организации, созданные для выполнения задач, поставленных перед федеральными государственными органами, органы государственной власти субъектов Российской Федерации, органы местного самоуправления.

Банк России не является кредитным учреждением, не может получать сведения, составляющие налоговую тайну (за исключением случая, когда налогоплательщик (плательщик страховых взносов) сам дал на это согласие, см. п. 5.2 Письма Банка России N 01-40-7/7949, ФНС России N ММВ-20-2/150@ от 02.10.2017 «О представлении информации по пунктам 5 и 10 приложения N 1 к Соглашению об информационном взаимодействии между Центральным банком Российской Федерации и Федеральной налоговой службой»). Кредитное учреждение также не может получать сведения, составляющие налоговую тайну.

К вопросу относительно прав и обязанностей специальных категорий лиц (агентов, посредников, подрядчиков, в т.ч. юридических лиц, обслуживающих программно-аппаратные и/или аппаратные комплексы, на которых обрабатываются сведения, составляющие налоговую тайну, управляющих компаний, в т.ч. управляющих компаний особых экономических зон, территорий опережающего развития, и проч.) в части доступа к сведениям, составляющих налоговую тайну, а также случаев такого доступа, заметим, что таким специальным категориям лиц доступ к сведениям, составляющим налоговую тайну, не предоставляется.

Тем не менее, в Приказе ФНС России от 13.01.2012 N ММВ-7-4/6@ указано, что для объектов информатизации налоговых органов основными актуальными источниками угроз безопасности информации для всех или части (информационных ресурсов (ИР) являются (п. 5.3.1):

(1) (…) поставщики программно-технических средств, расходных материалов, услуг, в том числе провайдеры телематических услуг (антропогенные, внешние);

(2) подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования ИС налоговых органов и его ремонт (антропогенные, внешние);

(3) работники налоговых органов, являющиеся легальными участниками процессов обработки информации и действующие вне рамок предоставленных полномочий (антропогенные, внутренние);

(4) работники налоговых органов, являющиеся легальными участниками процессов обработки информации и действующие в рамках предоставленных полномочий (антропогенные, внутренние).

Обзор законодательных требований по информационной безопасности при сборе, обработке, передаче, хранении сведений, составляющих налоговую тайну, включая требования к надежности систем обработки и хранения данных:

(1) О подзаконных НПА, принятых на основе законов, регулирующих соответствующие требования, см. п. 3.2.14. Кроме того, в соответствии ч. 5 ст. 16 закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» требования о защите информации, содержащейся в государственных ИС, устанавливаются ФСБ и ФСТЭК. Поэтому необходимо также рассмотреть Приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных система».

Согласно Приказу ФНС России от 13.01.2012 N ММВ-7-4/6@ «Об утверждении Концепции информационной безопасности Федеральной налоговой службы», предусматриваются требования к системе защиты информации, системе обеспечения безопасности информации, виртуальным технологиям, средствам криптографической защиты информации, задачам защиты информации на различных уровнях, встроенным функциям защиты общесистемного программного обеспечения и специальным техническим средствам защиты информации.

Заслуживает внимания репрезентативная ***судебная практика Российской Федерации и ЕСПЧ*** по вопросам обработки и защиты информации, составляющей соответствующие виды тайн. В частности, можно отметить следующие судебные решения.

Определение Конституционного Суда РФ от 30.09.2004 N 317-О. Специальный

правовой статус сведений, составляющих налоговую тайну, закреплен статьей 102 НК РФ исходя из интересов налогоплательщиков и с учетом соблюдения принципа баланса публичных и частных интересов в указанной сфере, поскольку в процессе осуществления налоговыми органами Российской Федерации своих функций, установленных Налоговым кодексом Российской Федерации и иными федеральными законами, в их распоряжении оказывается значительный объем информации об имущественном состоянии каждого налогоплательщика, распространение которой может причинить ущерб как интересам отдельных граждан, частная жизнь которых является неприкосновенной и охраняется законом, так и юридических лиц, чьи коммерческие и иные интересы могут быть нарушены в случае произвольного распространения в конкурентной или криминальной среде значимой для бизнеса конфиденциальной информации. Поэтому федеральный законодатель предусмотрел ограниченный режим доступа к такой информации путем установления исчерпывающего перечня субъектов, обладающих в силу закона правом обращения к налоговым органам за предоставлением сведений, составляющих налоговую тайну, в указанных в законе целях. Суд определил, что адвокат не включен законодателем в число лиц, имеющих доступ к сведениям, составляющим налоговую тайну.

Постановление Арбитражного суда Восточно-Сибирского округа от 28.07.2017 N Ф02-3705/2017 по делу N А19-22283/2016. Налоговый орган не обязан сообщать контрагенту соответствующего лица, документы (информация) о сделках которого запрошена, причины, по которым он посчитал необходимым направить требование в порядке, установленном статьей 93.1 Кодекса; иной вывод привел бы к незаконному разглашению налоговой тайны.

Постановление ФАС Восточно-Сибирского округа от 10.09.2010 по делу N А33-17361/2009 и Постановление ФАС Уральского округа от 31.10.2011 N Ф09-6378/11 по делу N А50П-341/2011. Отказ инспекции в ознакомлении налогоплательщика с материалами выездной налоговой проверки, мотивированный тем обстоятельством, что запрашиваемые документы содержат налоговую тайну, является нарушением права налогоплательщика на участие в рассмотрении материалов налоговой проверки.

Постановление ФАС Восточно-Сибирского округа от 26.08.2009 по делу N А78-7102/08. Не могут относиться к налоговой тайне сведения, которые по своей природе не могут быть конфиденциальными (например, наименование налогоплательщика-организации, имя индивидуального предпринимателя, под которыми они выступают в гражданском обороте).

Постановление Арбитражного суда Московского округа от 17.04.2018 N Ф05-4142/2018 по делу N А40-186267/2017 и Постановление Арбитражного суда Северо-Западного округа от 23.04.2018 N Ф07-3829/2018 по делу N А56-54459/2017. Режим банковской тайны не является препятствием для использования соответствующих сведений налоговыми органами, поскольку согласно статье 102 НК РФ полученные сведения о налогоплательщике составляют налоговую тайну, не подлежат разглашению, имеют специальный режим хранения и доступа. Представление банком документов по запросу инспекции не является нарушением банковской тайны, так как сведения передаются государственному органу, также сохраняющему тайну в отношении представленных сведений.

Постановление ФАС Северо-Западного округа от 11.02.2014 N Ф07-10138/2013 по делу N А05-3725/2013. Если сотрудники органов внутренних дел выделены управлением для проведения выездной проверки общества на основании мотивированного запроса налогового органа, то данные лица имеют право быть субъектами налоговой тайны и несут соответствующие обязанности и ответственность за разглашение сведений, составляющих налоговую тайну.

Постановление Арбитражного суда Уральского округа от 17.08.2016 N Ф09-8075/16 по делу N А50-17096/2015. Установленные Банком России правила не предусматривают получение сведений об уплате работодателями заемщиков налоговых платежей (НДФЛ). Коммерческий банк, исходя из ст. 102 НК РФ не имеет возможности получить самостоятельно сведения, отнесенные к налоговой тайне.

Европейский союз

Германия

Все международные конвенции об избежании двойного налогообложения и соглашения об обмене налоговой информацией, подписанные Германией, содержат положения о режиме тайны в отношении всей полученной и передаваемой информации[304].

[304] Глобальный Форум по прозрачности и обмену информацией для целей налогообложения Экспертные обзоры: Германия (Global Forum on Transparency and Exchange of Information for Tax Purposes Peer Reviews: Germany), с. 69

Кроме этого, специальные положения о налоговой тайне предусмотрены локальным законодательством Германии, в частности, разделом 30 Налогового кодекса[305]. Установлено, что государственные должностные лица обязаны соблюдать налоговую тайну. Нарушением налоговой тайны считается разглашение или использование информации, которая стала им известна, без авторизованного согласия, а также разглашение или использование коммерческой тайны, которая стала известна в ходе налоговых проверок, налоговых споров, в уголовном производстве по налоговым преступлениям.

Приводится перечень лиц, которые приравниваются к государственным должностным лицам в отношении соблюдения режима налоговой тайны (например, приглашенные эксперты).

Установлен закрытый перечень условий, при которых допускается раскрытие информации, относящейся к налоговой тайне (п.4 раздела 30 Налогового кодекса):

(1) если раскрытие информации служит осуществлению административных процедур, например, проведению налоговой проверки

(2) если это прямо разрешено законом

(3) если заинтересованные лица дают свое согласие,

(4) если информация служит для осуществления уголовного производства по преступлению, не являющемуся налоговым преступлением (при определенных условиях)

(5) существует заинтересованность общества в раскрытии такой информации; в частности, когда речь идет о преступлениях и умышленных тяжких преступлениях против жизни и здоровья или против государства и его институтов, экономические преступления в зависимости от размера причиненного ущерба, которые могут существенно нарушить экономический порядок или существенно подорвать общую уверенность в добросовестности деловых отношений или упорядоченном функционировании органов власти и государственных учреждений; а также в ряде других случаев.

Отдельно предусмотрено, что не считается нарушением налоговой тайны, если при использовании должностным лицом электронной почты аккредитованным поставщиком

[305] Налоговый кодекс Федеративной Республики Германия [Электронный ресурс] // Bundesministerium der Justiz und für Verbraucherschutz [Сайт]. – URL: https://www.gesetze-im-internet.de/englisch_ao/englisch_ao.html#p0175 (дата обращения: 30.07.2018).

услуг осуществляется временная автоматическая расшифровка информации для проверки на наличие вредоносных программ и с целью передачи данных адресату почтового сообщения (п.7 раздела 30 Налогового кодекса).

За нарушение налоговой тайны ст. 355 Уголовного кодекса Федеративной Республики Германия предусмотрена уголовная ответственность (лишение свободы на срок до двух лет или штраф).

Относительно технических мер предотвращения утечки информации, составляющей налоговую тайну. В Федеральном Центральном Налоговом Управлении Германии (BZSt) внедрена ИТ-система для автоматического обмена информацией, в которой все запросы хранятся в электронном виде, а информация передается через защищенную электронную почту. Таким образом, внутри Федерального Центрального Налогового Управления не хранятся печатные копии запросов, а местные и региональные органы власти не имеют доступ в ИТ-систему Управления[306].

Испания

Вопросы, связанные с налоговой тайной, содержатся в законе Испании «Об общем налогообложении» (Ley 58/2003, de 17 de diciembre, General Tributaria)[307]. Определение понятия налоговой тайны как таковое не закреплено в законодательстве Испании, но сущность этого института может быть выведена из анализа статьи 95 Закона.

Все сведения, полученные налоговым органом в ходе выполнения должностных обязанностей, являются конфиденциальными, могут использоваться только для целей исполнения налоговыми органами своих функций, не подлежат раскрытию, за исключением случаев, установленных законом. К исключениям относятся.

(1) сотрудничество с судом и прокуратурой по преступлениям, которые предполагают уголовное преследование;
(2) сотрудничество с другими налоговыми органами с целью соблюдения налоговых обязательств в рамках их компетенций;

[306] Глобальный Форум по прозрачности и обмену информацией для целей налогообложения Экспертные обзоры: Германия (Global Forum on Transparency and Exchange of Information for Tax Purposes Peer Reviews: Germany).

[307] Закон Испании «Об общем налогообложении» [Электронный ресурс] // Agencia Estatal Boletin Oficial del Estado [Сайт]. – URL: http://www.boe.es/buscar/pdf/2003/BOE-A-2003-23186-consolidado.pdf (дата обращения: 30.07.2018).

(3) сотрудничество с органами социального обеспечения в борьбе с мошенничеством в области социального страхования, а также для определения взносов лиц в Национальную Систему Здравоохранения;
(4) сотрудничество с государственными органами в борьбе с налоговыми преступлениями в области получения помощи или субсидий из государственных средств или средств Европейского Союза;
(5) сотрудничество с Парламентскими комиссиями по расследованию в установленном законом порядке;
(6) при защите прав и интересов несовершеннолетних и инвалидов в судах или прокуратуре;
(7) сотрудничество со Счетной Платой при осуществлении функции контроля за налоговым органом;
(8) сотрудничество с судами для вынесения судебных решений при условии, что иные способы сбора информации полностью исчерпаны;
(9) сотрудничество в области противодействия отмыванию денег и финансированию терроризма с соответствующими государственными органами;
(10) сотрудничество с иными государственными органами (при условии согласия налогоплательщика на раскрытие им сведений);
(11) сотрудничество с органом, осуществляющим аудит сектора государственного управления (IGAE);
(12) сотрудничество с органом по управлению активами для отслеживания активов, изъятых или конфискованных в уголовном процессе;
(13) если правилами ЕС установлено, что такие сведения являются публичными;
(14) в соответствии с международными договорами, одной из сторон которых является

Предоставление сведений, составляющих налоговую тайну, должно производиться предпочтительно с помощью компьютерных средств или средств электронной связи.

Ответственность за незаконное раскрытие налоговой тайны установлена в статьях 197 и 198 Уголовного Кодекса Испании[308].

[308] Уголовный кодекс Испании [Электронный ресурс] // Agencia Estatal Boletin Oficial del Estado [Сайт]. – URL: https://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf (дата обращения: 30.07.2018).

Незаконное раскрытие налоговой тайны сотрудником налогового органа называется лишением свободы от одного до четырех лет и штрафом от 18 до 24 месяцев (день штрафа от 2 до 400 евро – ст. 50 Кодекса) с запретом занимать должности государственной службы от 6 до 12 лет.

Эстония

Законодательство Эстонии содержит достаточно подробное регулирование режима конфиденциальности налоговой тайны (раздел 4 «Налоговая тайна» Закона «О налогообложении»[309]). В § 26 Закона определяется понятие налоговой тайны, к которой относится вся информация, получаемая должностными лицами налоговых органов во время выполнения должностных обязанностей. Разглашение сведений, составляющих налоговую тайну, допускается только с письменного разрешения налогоплательщика или в случаях, предусмотренных § 27-30 настоящего Закона: информация относится к публичной (например, название, идентификационный номер налогоплательщика); информация об объеме налоговой задолженности и период, когда такая задолженность возникла; информация о преступлениях, если публичная заинтересованность в обнародовании такой информации перевешивает заинтересованность в ее неразглашении, а обнародование информации не влияет на установление истины в уголовном или административном производстве.

С точки зрения раскрытия налоговой тайны третьим лицам, не признается таким раскрытием передача налоговым органом по государственным налогам сведений, необходимых для проверки правильности исчисления и уплаты местного налога в налоговый орган по местным налогам. Отдельно установлен перечень ситуаций, когда налоговый орган вправе разглашать сведения, составляющие налоговую тайну (§ 29 Закона). В частности, это ситуации разглашения информации, относящейся к налоговой тайне, следователям и прокурорам в целях предупреждения и выявления преступлений, в суды для подготовки и рассмотрения уголовных, гражданских и административных дел, судебным приставам, если информация необходима для совершения исполнительных действий, и т.д., всего 42 пункта.

Кроме этого, налоговый и таможенный департамент может раскрывать информацию, подлежащую налоговой тайне, без согласия или без уведомления облагаемого налогом лица

[309] Закон «О налогообложении» Эстонской республики [Электронный ресурс] // Riigi Teataja [Сайт]. – URL: https://www.riigiteataja.ee/en/eli/523012015008/consolide (дата обращения: 30.07.2018).

или третьего лица: 1) компетентному органу иностранного государства в порядке, установленном договором; 2) органам Европейского Союза и его государств-членов, компетентным обмениваться информацией, касающейся налогооблагаемых лиц, в порядке, установленном законодательством Европейского Союза.

Круг лиц, которые могут иметь доступ к налоговой тайне включает в себя не только должностных лиц налогового органа, но и сотрудников, которые занимаются обслуживанием и развитием информационно-коммуникационных систем налогового органа, а также лиц, осуществляющих проверку деятельности налогового органа. Должностные лица и служащие, получающие доступ к налоговой тайне, обязаны сохранять конфиденциальность любой информации, которая стала им известна, и после прекращения службы или трудовых отношений.

Закон «О налогообложении» Эстонии не содержит мер ответственности за нарушение налоговой тайны. Такие меры предусмотрены законом «О публичной информации», а за их соблюдением следит специальный орган - инспекция по защите данных[310]. В частности, § 16 закона «Об общественной информации» установлено, что к информации, предназначенной для внутреннего использования, относятся сведения, собранные о лице в процессе налогообложения, за исключением сведений о налоговой задолженности. В § 54.1 Закона указано, что намеренное раскрытие или разглашение информации, предназначенной для внутреннего использования, или несоблюдение предписания инспекции по защите данных наказывается штрафом в размере до 300 штрафных единиц (около 1 200 евро).

Великобритания

Основные положения по защите налоговой тайны Великобритании предусмотрены в Законе «Об уполномоченных по налоговым и таможенным сборам» (раздел 18 «Конфиденциальность» и раздел 19 «Неправомерное раскрытие»)[311].

Интересно, что вопросы налоговой тайны в Великобритании регулярно получают широкий общественный резонанс. Так, в статье «Верховный Суд постановил, что Государственное управление Великобритании по налоговым и таможенным сборам

[310] Public Information Act of November 15, 2000 (as revised June 14, 2017) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/514112013001/consolide (accessed: 30.07.2018).

[311] Commissioners for Revenue and Customs Act 2005 [Electronic resource] // Legislation.gov.uk [Site]. – URL: https://www.legislation.gov.uk/ukpga/2005/11/pdfs/ukpga_20050011_en.pdf (accessed: 30.07.2018).

нарушило конфиденциальность»[312] по мотивам нашумевшего судебного разбирательства о нарушении налоговой тайны в отношении говорится, что члены Парламента Великобритании неоднократно вступали в конфликты с Управлением Великобритании по налоговым и таможенным сборам (далее – Управление) в связи с отказом последних раскрывать детали урегулирования расчетов по налоговым платежам с крупными налогоплательщиками. По мнению одного из членов Парламента, «конфиденциальность в пользу налогоплательщиков разрушает уверенность в целостности системы»[313].

Устанавливается, что должностные лица Управления не вправе разглашать любую информацию, полученную ими в связи с выполнением должностных обязанностей.

Сведения, относящиеся к налоговой тайне, определяются как вся информация, полученная Управлением, за исключением ряда случаев. Не является разглашением налоговой тайны разглашение информации, если оно:

- было совершено с согласия лица, к которому относится такая информация;
- было совершено для функционирования Управления и одновременно не противоречит ограничениям, налагаемым уполномоченными должностными лицами Управления;
- соответствует требованиям раскрытия информации в общественных интересах и интересах органов прокуратуры;
- было произведено для целей гражданского или уголовного судопроизводства;
- а также в ряде других специфических случаев.

Нарушением налоговой тайны является такое раскрытие информации, при котором лицо, к которому относится эта информация, прямо указано при разглашении или может быть определено путем умозаключений. Лицо, виновное в разглашении налоговой тайны, наказывается лишением свободы на срок до двух лет и к штрафу, размер которого не ограничен и определяется судом исходя из причиненного ущерба (раздел 19 Закона).

[312] Vanessa Houlder, Jane Croft Supreme Court rules HMRC breached confidentiality [Electronic resource] / October 19, 2016. // Financial Times [Site]. – URL: https://www.ft.com/content/3db314c4-95f4-11e6-a80e-bcd69f323a8b (accessed: 30.07.2018).

[313] Ibid.

Соединенные Штаты Америки

Налоговое законодательство США закреплено в главе 26 Кодекса внутренних доходов США (U.S. Code: Title 26 - Internal Revenue Code)[314].

Определение понятия налоговой тайны как таковое не закреплено в законодательстве США, тем не менее, понимание сущности этого института возможно через анализ иных терминов и анализ положений законодательства. Терминология отлична от законодательства о налогах в России, поэтому там, где невозможно подобрать достаточно точный перевод, мы используем описание термина.

А. Конфиденциальность налоговой декларации и раскрытие информации, содержащейся в налоговой декларации (26 U.S. Code § 6103 - Confidentiality and disclosure of returns and return information)[315]

Общий принцип – запрет на раскрытие информации, содержащей налоговую тайну, соответствующими должностными лицами Федерации или Штатов (а также иными лицами, которые могут иметь доступ к такой информации), за исключением случаев, установленных законом.

1) Основные термины и определения[316].

1. Термин “return” включает в себя налоговую декларацию, информационную декларацию, декларацию об авансовых платежах, требование о возмещении, дополнения к этим документам (вложения, списки, иное), которые подаются в налоговый орган (далее – налоговая декларация, декларация).

2. Термин “return information” включает в себя:

(1) идентификационные данные налогоплательщика;

(2) информацию о характере, источнике или объеме его доходов, платежей, выручки, вычетов, льгот, кредитов, активов, пассивов налоговых обязательств, налоговых платежей и др.;

[314] U.S. Code: Title 26 - Internal Revenue Code [Electronic resource] // Cornell Law School [Site]. – URL: https://www.law.cornell.edu/uscode/text/26 (accessed: 30.07.2018).

[315] U.S. Code § 6103 - Confidentiality and disclosure of returns and return information [Electronic resource] // Cornell Law School [Site]. – URL: https://www.law.cornell.edu/uscode/text/26/6103 (accessed: 30.07.2018).

[316] Ibid.

(3) иную информацию, полученная налоговым органом в отношении налоговой декларации или в отношении существования или возможного существования ответственности (штрафы, пени, иное) какого-либо лица;

(4) разъяснения налоговых органов или материалы письменного запроса для разъяснения, которые не открыты для общественности в соответствии с разделом 6110 (по общему правилу – открыты, за исключением сведений, относящихся к: именам, адресам, подобному; иным тайнам (государственная, коммерческая, другие); пояснения специального отдела при налоговой службе США, который дает разъяснения действующего законодательства;

(5) информацию о соглашении о применяемой налогоплательщиком методологии трансфертного ценообразования;

(6) информацию о соглашении об ответственности в отношении любого налога;

Таким образом, несмотря на перечисление конкретных примеров сведений, составляющих налоговую тайну, перечень является открытым.

2) Исключения из налоговой тайны также установлены в разделе 6103. Ниже рассмотрим только случаи, представляющие интерес по теме исследования или представляющие интерес вообще (например, при отсутствии такого института в России). Информация может раскрываться налоговым органом:

(1) уполномоченному представителю налогоплательщика;

(2) государственным аудиторам государственных доходов и программ в той мере, в которой это необходимо для применения налоговых законов;

(3) раскрытие информации лицам, имеющим материальный интерес:

- любой член товарищества имеет право на получение информации в отношении декларации товарищества за период, охватывающий момент, когда он был членом товарищества;
- к информации в декларации корпорации или её дочернего предприятия может иметь доступ:
  - любое лицо, назначенное членом Совета Директоров;
  - любой сотрудник такой корпорации по письменному запросу, подписанному главным должностным лицом и заверенному сотрудником налогового органа;

– любой добросовестный акционер, владеющий 1 или более процентами акций такой корпорации.

(4) раскрытие информации Комитетам Конгресса (если речь об информации, прямо или косвенно указывающей на конкретного налогоплательщика, то рассмотрение этой информации на заседании возможно либо в случае согласия такого налогоплательщика, либо на закрытом заседании);

(5) любая информация о любом налогоплательщике может раскрываться Президенту США при условии указания причины запроса;

(6) раскрытие информации (фирменное наименование; характер, основания контракта) подрядчиком по сбору неактивной дебиторской задолженности (например, если истекла треть срока давности взыскания) в тех ситуациях, которые были одобрены налоговым органом, лицу, с которого предполагается взыскание такой задолженности;

(7) информация может быть раскрыта в соответствии с положениями, предписанными Секретарем налогового органа, любому лицу в той мере, в какой это необходимо в связи с обработкой, хранением, передачей и воспроизведением такой информации, программированием, обслуживанием, ремонтом, тестированием и приобретением оборудования, а также в связи с предоставлением иных услуг для целей налогового администрирования.

Перейдем к рассмотрению ответственности за незаконное разглашение информации, составляющей налоговую тайну.

B. Ответственность за незаконное разглашение сведений, составляющих налоговую тайну – раздел 7213 главы 26 Кодекса США Несанкционированное раскрытие информации, раздел 7431 главы 26 Кодекса США Гражданский ущерб за несанкционированную проверку или раскрытие информации о налоговой декларации (26 U.S. Code § 7213 - Unauthorized disclosure of information, 26 U.S. Code § 7431 - Civil damages for unauthorized inspection or disclosure of returns and return information)[317][318]

[317] 26 U.S. Code § 7213 - Unauthorized disclosure of information [Electronic resource] // Cornell Law School [Site]. – URL: https://www.law.cornell.edu/uscode/text/26/7213 (accessed: 30.07.2018).

[318] 26 U.S. Code § 7431 - Civil damages for unauthorized inspection or disclosure of returns and return information [Electronic resource] // Cornell Law School [Site]. – URL: https://www.law.cornell.edu/uscode/text/26/7431 (accessed: 30.07.2018).

Незаконное раскрытие информации (return и return information) сотрудниками (в том числе бывшими) соответствующих органов, иными лицами, указанными в разделе 6103, незаконное получение такой информации лицами, получившими такую информацию в с помощью предложения материальной выгоды, незаконное раскрытие информации акционерами, получившими её на основании положениями 6103(e)(1)(D)(iii) (добросовестный акционер с более, чем 1% акций), является уголовным преступлением и наказывается штрафом в сумме, не превышающей 5000 долларов США, или лишением свободы на срок до пяти лет, или штрафом и лишением свободы, с возмещением всех судебных расходов. Кроме того, если такое лицо является государственным служащим США (Федерации), то оно должно быть уволено с должности.

Незаконное раскрытие (умышленно или по легкомыслию) информации лицом, занимающимся предпринимательской деятельностью в сфере для предоставления услуг по подготовке, заполнению декларации, наказывается штрафом в сумме, не превышающей долларов США, или лишением свободы на срок до одного года, или штрафом и лишением свободы, с возмещением всех судебных расходов, а также с увольнением с должности.

Незаконное раскрытие информации о программном обеспечении (исходный код и исполняемый код), наказывается штрафом в сумме, не превышающей 5000 долларов США, или лишением свободы на срок до пяти лет, или штрафом и лишением свободы, с возмещением всех судебных расходов.

Налогоплательщик также может подать гражданский иск за разглашение налоговой тайны. Сумма иска: 1000 долларов США за каждый акт раскрытия информации или убытков, понесенных истцом в результате раскрытия тайны. Если же раскрытие тайны произошло в результате умысла или грубой халатности, то сумма иска составит сумму штрафа и убытков.

С. Краткие сведения о требованиях налоговых органов США к информационной безопасности[319]

Меры, принимаемые для защиты информации:

(1) создание специальных зон физического хранения информации и специальных средств защиты (охрана, сейфы и т.д.);

[319] IRS Publication No. 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information (Rev. 3/99) [Electronic resource] // IRS [Site]. – URL: https://www.irs.gov/pub/irs-utl/p1075.pdf (accessed: 30.07.2018).

(2) полное шифрование диска (технология защиты информации, переводящая данные на диске в нечитаемый код, который нелегальный пользователь не сможет легко расшифровать), содержащего охраняемую информацию;

(3) постоянное обучение сотрудников в направлениях защиты информации (например, подготовка к непредвиденным обстоятельствам, раскрытие информации, реагирование на происшествия, ролевое обучение). Ежегодно проводится повторная сертификация сотрудника;

(4) периодическая (не реже одного раза в 18 или 36 месяцев) проверка, проводимая Службой Внутренних Доходов США, в отношении получателей информации относительно соблюдения требований по информационной безопасности;

получатели информации обязаны предоставлять отчеты установленной формы в Службу Внутренних Доходов США по поводу реализации мер по информационной безопасности.

Япония

Впервые концепция налоговой прозрачности и открытости появилась в Японском законодательстве в 2010 году. Принятый закон был направлен на упрощение налоговых правил и привлечение нарушителей к ответственности.

Соблюдение налоговой тайны в Японии гарантируется главой 38 Конституции. Причем соблюдение налоговой тайны обязательно для всех, государственных лиц и налоговых инспекторов, поскольку налоговая тайна должна быть сохранена, даже если во время проверки были обнаружены налоговые нарушения.

Так, в 2014 году во время выборов мэра города Яхио-Сити действующий мэр намеренно распространил информацию о налоговых нарушениях своего оппонента. За нарушение налоговой тайны действующему мэру было предъявлено обвинение и назначен домашний арест.

До сегодняшнего дня случав похищения конфиденциальных налоговых сведений из единого хранилища данных зафиксировано не было. Однако в случае если налоговая тайна будет нарушена, потерпевший может обратиться в Комиссию по защите персональных данных. Если тайна была нарушена должностным лицом, потерпевший может подать иск для возмещения причиненного ущерба.

Что касается трансграничных случаев нарушения налоговой тайны, то в судебных инстанциях США был рассмотрен гражданский иск о возмещении убытков, который включал утечку неправильной информации, предоставленной должностным лицом налоговой службы Японии.

Сингапур

Понятие налоговой тайны (официальной тайны) в Сингапуре установлено в п. 6 части 2 Закона о подоходном налоге (Income Tax Act (Chapter 134))[320]. При этом, налоговым законодательством Сингапура прямо установлено, что обязанность предоставить информацию в соответствии с международными соглашениями имеет приоритет над обязанностью соблюдать налоговую тайну.

Законодательно закреплена обязанность должностного лица, которое рассматривает и обрабатывает все документы, информацию, налоговые декларации и приложения к ним, относящиеся к доходу любого лица, должно обращаться с такой информацией как с тайной. Лицо, которое передает или пытается передать такую тайную информацию, разрешает иному лицу иметь доступ к этой информации, за исключением случаев, установленных законом, виновно в совершении правонарушения. Таким образом, к налоговой тайне относится всё, что не исключено законом. Рассмотрим исключения.

(1) никто из лиц, обладающих налоговой тайной, не обязан разглашать в суде конфиденциальную информацию, за исключением случаев, когда это необходимо для целей реализации данного закона или в целях возбуждения дела о правонарушении в соответствии с данным законом;
(2) в случае реализации международных договоров, одной из сторон которых является Сингапур;
(3) предоставление информации при аудите государственных средств;
(4) предоставление информации в целях исполнения обязанностей налоговым органам по прочим налогам (Контролеру налога на имущество, Контролеру налога на товары и услуги, Комиссару по государственным (в том числе таможенным) пошлинам);

[320] Income Tax Act (Chapter 134) [Electronic resource] // Singapore Statutes Online [Site]. – URL: https://sso.agc.gov.sg/Act/ITA1947#pr6- (accessed: 30.07.2018).

(5) предоставление информации в Резервный Фонд (речь о пенсионных накоплениях, медицинских накоплениях);

(6) предоставление информации в службу статистики;

(7) предоставление информации Комиссару полиции или Директору Департамента по коммерческим вопросам, если такая информация может потребоваться для расследования или судебного преследования лица за преступления, связанные с коррупцией, незаконным оборотом наркотиков, другими серьезными преступлениями;

(8) при согласии лица, информация о котором является конфиденциальной, возможно предоставление информации любому иному государственному должностному лицу.

Ответственность за разглашение налоговой тайны установлена в разделе 94 части 20 Закона о подоходном налоге Сингапура.

Разглашение налоговой тайны наказывается штрафом не превышающем 1000 сингапурских долларов, а в случае неуплаты - лишением свободы на срок не более 6 месяцев.

Южная Корея

Южная Корея подписала широкий перечень двусторонних соглашений по обмену информацией по налоговым вопросам (с 86 юрисдикциями на 2012 г.).

Для Национальной налоговой службы Республики Корея установлены законодательные барьеры (законы о налоговой тайне) на обмен информацией с другими учреждениями, включая правоохранительные органы или другие компетентные органы[321].

Определен порядок доступа к информации компетентных органов. Указано, что некоторая основная информация о корпорациях находится в открытом доступе, например регистрационный номер и количество акционеров в публичных компаниях. Регулирующие, налоговые, надзорные и правоохранительные органы обладают целым рядом предусмотренных законом полномочий по получению информации о собственности и контроле юридических лиц как из общедоступных источников, так и с помощью различных

[321] Отчет «Борьба с отмыванием денег и борьба с финансированием терроризма. Южная Корея» [Электронный ресурс] // Financial Action Task Force (FATF) [Site]. – URL: http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Korea.pdf (дата обращения: 30.07.2018).

других мер. Однако объем информации о бенефициарной собственности ограничивается тем, что регистрируется в корпоративных реестрах акционеров.

В соответствии с законом «О корпоративном налогообложении» юридические лица обязаны уплачивать налоги и подавать налоговые декларации в Национальную налоговую службу Республики Корея. Информация, содержащаяся в налоговых декларациях, может позволять установить бенефициарного собственника юридического лица. Однако информация в этих декларации и другая информация, имеющаяся у Национальной налоговой службы, является налоговой тайной и может быть передана только правоохранительным органам и другими государственными органами только по решению суда или в соответствии с конкретным расследованием уклонения от уплаты налогов.

Если рассматривать соотношение в Южной Корее налоговой тайны и других видов тайн, например, профессиональной тайны, примечательно, что информация, которую, например получает сертифицированный бухгалтер в рамках своей профессиональной деятельности, может быть раскрыта налоговым и прочим органам[322].

Израиль

Рассмотрим регулирование налоговой тайны на примере закона «Порядок налогообложения подоходным налогом»[323]. Сохранять конфиденциальность в отношении налоговой тайны обязаны должностные лица, имеющие доступ к налоговой тайне, которая может содержаться в декларациях физических лиц, приложениях к декларациям и прочих документах. Интересно, что не считается нарушением раскрытие данных налоговой декларации или доходов лица его супругу/супруге за то время, которое они были женаты (п. 231 Закона).

Ответственность за разглашение налоговой тайны предусмотрена, если должностное лицо сообщает или пытается сообщить информацию о доходах лица или любое содержание налоговых деклараций и прочих полученных сведений. Такое нарушение наказывается лишением свободы сроком на шесть месяцев или штрафом. Не считается нарушением

[322] Глобальный Форум по прозрачности и обмену информацией для целей налогообложения Экспертные обзоры: Республика Корея (Global Forum on Transparency and Exchange of Information for Tax Purposes Peer Reviews: Republic of Korea).

[323] Закон Государства Израиль «Порядок налогообложения подоходным налогом» [Электронный ресурс] // International Center for Not-For-Profit Law [Сайт]. – URL: http://www.icnl.org/research/library/files/Israel/Ordinance.pdf (дата обращения: 30.07.2018).

налоговой тайны раскрытие информации государственному институту страхования (п.п. 234-235 Закона).

На 2014 г. Израиль заключил 54 двусторонних соглашения об обмене налоговой информацией. Все соглашения содержат положения о соблюдении конфиденциальности в отношении получаемых и направляемых сведений[324].

Объединенные Арабские Эмираты

В ОАЭ вопросы налоговой тайны регулируются Федеральным законом «О налоговых процедурах» (Federal Law No. (7) of 2017 on Tax Procedures), принятым относительно недавно.[325]

В статье 41 Закона описаны положения о тайне профессиональной информации. Само понятие «налоговая тайна» в законе не определяется специально, но указано, что сотрудники (в том числе бывшие) налоговых органов не должны разглашать информацию, которую они получили, или к которой они имели доступ в связи с исполнением профессиональных обязанностей, за исключением случаев, предусмотренных Исполнительным регламентом к данному закону[326]. При этом раскрытие такой информации в любом случае может быть произведено только в соответствии с основными положениями Закона.

Исключения, которые не являются разглашением налоговой тайны перечислены в статье 24 Исполнительного регламента[327]. К таким исключениям относятся:

1. Раскрытие информации по решению судебного органа для целей гражданского или уголовного делопроизводства.

2. Раскрытие информации другому государственному органу после заключения соглашения (меморандума) о раскрытии информации (в котором оговаривается такое

[324] Глобальный Форум по прозрачности и обмену информацией для целей налогообложения Экспертные обзоры: Израиль (Global Forum on Transparency and Exchange of Information for Tax Purposes Peer Reviews: Israel).

[325] Federal Law of the United Arab Emirates No. (7) of 2017 on Tax Procedures [Electronic resource] // Federal Tax Authority [Site]. – URL: https://www.tax.gov.ae/pdf/Federal-Law-No-7-of-2017-on-Tax-Procedures.pdf (accessed: 30.07.2018).

[326] Cabinet Decision No. (36) of 2017 on the Executive Regulation of Federal Law No. (7) of 2017 on Tax Procedures [Electronic resource] // Federal Tax Authority [Site]. – URL: https://www.tax.gov.ae/pdf/Cabinet-Decision-36-of-2017-on-Executive-Regulation-on-Tax-Procedures.pdf (accessed: 30.07.2018).

[327] Ibid.

раскрытие, использование информации, механизмы контроля, безопасности) между руководством налогового органа и соответствующим государственным органом.

3. Раскрытие информации в соответствии с международными договорами.

4. Раскрытие информации самому лицу, в отношении которого налоговый орган получил информацию, или его налоговому агенту.

5. Раскрытие сведений другому специализированному органу при условии, что оно сделано в месте и в соответствии с условиями конфиденциальности (то есть специализированный орган будет охранять эти сведения в соответствии со своими положениями об охране тайн).

Ответственность за незаконное раскрытие конфиденциальной информации установлена в статье 379 Уголовного Кодекса ОАЭ. Незаконное раскрытие налоговой тайны будет наказываться лишением свободы на срок не менее одного года и не более пяти лет и (или) минимальным штрафом в размере двадцати тысяч дирхамов (примерно 4600 евро)[328].

1.5. Отдельные особенности регулирования оборота и защиты информации в мире

ЕС и GDPR

Особенность правового регулирования в Европейском Союзе (далее - «ЕС») обусловлена тем обстоятельством, что европейское право является, по сути, некой самостоятельной правовой системой, находящейся одновременно на стыке национального права государств-членов ЕС и международного права. Европейского право обладает свойством прямого действия, а значит, применяется непосредственно и является обязательным на всей территории ЕС и относительно всех субъектов права. Однако это не исключает того факта, что многие положения подлежат дополнительной детализации на уровне государств - участников ЕС. В этой связи в настоящем разделе будут проанализированы не только директивы и регламенты ЕС, но и применимые международные договоры, также будет приведены некоторые кейсы ЕСПЧ, разъясняющие отдельные положения таких международных договоров. Анализ законодательства отдельных государств

[328] The Penal Code of United Arab Emirates [Electronic resource] // Abu Dhabi Judicial Department [Site]. – URL: https://www.adjd.gov.ae/sites/Authoring/AR/ELibrary%20Books/E-Library/PDFs/Penal%20Code.pdf (accessed: 30.07.2018).

ЕС приведен в разделах, посвященных Германии, Эстонии и Испании.

Базовые положения о защите определенных видов информации содержатся в международных договорах, касающихся прав человека, в частности, Европейской конвенции о защите прав человека и основных свобод[329], а также Хартии Европейского союза об основных правах[330]. В частности, статьей 8 Европейской конвенции и статьей 7 Хартии равным образом установлено, что каждый человек имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции. Статья 8 Хартии закрепляет право каждого человека на защиту относящихся к нему данных личного характера. Обработка подобных данных должна производиться в четко определенных целях, с согласия заинтересованного лица либо при наличии других правомерных оснований, предусмотренных законом. Говоря об обработке данных, следует отметить и Конвенцию Совета Европы о защите частных лиц в отношении автоматизированной обработки данных личного характера № 108, принятую в 1981 г (далее – «Конвенция 108»)[331]. В ней определен ряд главных принципов, в дальнейшем положенных в основу многих законов об охране персональных данных и неприкосновенности личной жизни. Конвенция также защищает физических лиц от вторжения в их личную жизнь со стороны государственных органов и администрации частных организаций.

Данные положения получили развитие в установлении режима обработки персональных данных и, в частности, принятии Европейским Парламентом и Советом Европейского союза 27 апреля 2016 года Общего регламента о защите персональных данных[332] (далее - «GDPR»), на сегодняшний день являющегося основополагающим актом ЕС в сфере защиты персональных данных физических лиц.

Принятие GDPR представляет собой одно из самых значительных изменений в законодательстве о защите персональных данных в ЕС за последние 20 лет. GDPR заменил

---

[329] Конвенция о защите прав человека и основных свобод [Электронный ресурс]: заключена – в г. Риме 04.11.1950 (с изм. от 13.05.2004). – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 30.07.2018).

[330] Хартия Европейского союза об основных правах [Электронный ресурс]: принята в г. Страсбурге 12.12.2007. – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 30.07.2018).

[331] Конвенция о защите физических лиц при автоматизированной обработке персональных данных [Электронный ресурс]: заключена в г. Страсбурге 28.01.1981 (с изм. от 08.11.2001). – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 30.07.2018).

[332] 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) [Электронный ресурс]: регламент Европейского парламента и Совета Европейского Союза. – № 2016/679 – 27.04.2016. – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 30.07.2018).

собой действующую с 1995 года Директиву 95/46/ЕС «О защите прав физических лиц применительно к обработке персональных данных и о свободном движении таких данных» (далее – «Директива 95/46/ЕС») [333]. Следует отметить, что GDPR в отличие от Директивы 95/46/ЕС обладает прямым действием на территории всех государств-членов ЕС. Согласно ч. 2 ст. 99 GDPR, он стал обязательным для применения с 25 мая 2018 года. Для подготовки к новым требованиям компаниям было предоставлено чуть более двух лет. Трудно переоценить значение, которое имеет настоящий документ для порядка обработки данных граждан ЕС в любой сфере жизнедеятельности, а потому на протяжении нашего отчета мы будем к нему неоднократно обращаться. Кроме того, полагаем возможным во всех случаях заменять в нормативных документах ссылку на Директиву 95/46/ЕС ссылкой на GDPR.

Прежде чем перейти к описанию правового режима отдельных видов данных, отметим некоторые важные моменты применительно к актуальным тенденциям в отношении оборота данных в ЕС. Построение и развитие экономики данных является частью Стратегии единого цифрового рынка[334]. Основной задачей является создание возможности максимально эффективно использовать цифровые данные в целях экономического развития и укрепления благосостояния общества. Для реализации поставленной задачи Европейская Комиссия намерена стимулировать повторное использование или пере-использование (*re-use*) различных видов данных, а также обеспечить свободное распространение и передачу информации на территории ЕС в рамках единого цифрового рынка. В рамках обозначенного направления Комиссия разработала ряд мер, включающих пересмотр действующих нормативных актов в сфере использования данных государственного сектора, данных исследований, а также разработку директивы, регулирующей оборот данных, не являющихся персональными[335]. Данная директива совместно с GDPR должна обеспечить единообразный и сбалансированный подход к свободному распространению всех и любых данных в рамках ЕС. Это, в частности, предполагает снижение уровня локализации данных (уменьшение

[333] О защите физических лиц при обработке персональных данных и о свободном обращении таких данных [Электронный ресурс]: директива Европейского парламента и Совета Европейского Союза – № 95/46/ЕС – 24 октября 1955 г. – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 30.07.2018).

[334] Building a European data economy [Electronic resource] // European Commission [Site]. – URL: https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy (accessed: 30.07.2018).

[335] Proposal for a regulation of the European parliament and of the Council on a framework for the free flow of non-personal data in the European Union – September 13, 2017 – [Electronic resource] // European Commission [Site]. – URL: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-framework-free-flow-non-personal-data (accessed: 30.07.2018).

количества соответствующих требований в зависимости от типа данных), трансграничную передачу данных для целей государственного контроля и надзора, упрощение процедур перехода от одного провайдера облачных сервисов к другому для профессиональных пользователей, а также обеспечение необходимого уровня информационной безопасности.

Второе важное направление связано с использованием данных государственного сектора. Как отмечено Европейской Комиссией в ЕС аккумулируется большое количество данных государственного сектора (*public sector information* или *PSI*) или государственной информации, которая может и должна использоваться повторно[336]. Такая информация включает в себя любую информацию, которая создается, собирается государственными органами или за их счет, например, географические данные, статистика, погодные сведения, сведения исследований, финансируемых государством и т.д. Повторное использование или пере-использование (*re-use*) таких данных может принести существенную пользу интересам общества и экономике в целом.

Так, согласно проведенным исследованиям на сегодняшний день рынок открытых данных ЕС (*EU open data market*) имеет существенный экономический потенциал. В частности, по оценкам специалистов совокупная экономическая стоимость таких данных должна вырасти с 52 миллиардов евро в 2018 до 194 миллиардов евро в 2030 году. Использование PSI преимущественно направлено на стимулирование экономического развития и инноваций, разрешение социальных задач в таких сферах как здравоохранение и транспортное обслуживание, развитие новых технологий, таких как искусственный интеллект, которым требуется большое количество данных для обработки, расширение участия граждан в политической и социальной сферах, повышение прозрачности деятельности государственных органов.

Использование государственной информации регулируется Директивой О2003/98/ЕС «О пере-использовании государственной информации»[337], которая была пересмотрена в 2013 году. Положения данной Директивы не применяются к документам, которые являются интеллектуальной собственностью третьих лиц, документам, содержание которых охраняется в соответствии со специальным правовым режимом, например, таким как: защита

[336] Open data [Electronic resource] // European Commission [Site]. – URL: https://ec.europa.eu/digital-single-market/en/open-data (accessed: 30.07.2018).

[337] On the re-use of public sector information – the European parliament and of the Council Directive – № 2003/98/EC – 17 November 2003 – [Electronic resource] // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:02003L0098-20130717 (accessed: 30.07.2018).

национальной безопасности, конфиденциальность статистических данных, коммерческая или служебная тайна, в целях защиты персональных данных и т.д. Документы и информация, которые охватываются настоящей Директивой, в том числе, документы публичных библиотек, музеев и архивов, могут быть предоставлены соответствующим государственным органом лицу по запросу в существующем формате или в машиночитаемой форме. На сегодняшний день реализован *The European Union Open Data Portal*, где размещены данные различные данные государственных органов и учреждений ЕС[338], включая географические, геополитические и финансовые данные, статистические данные, результаты голосований, нормативные акты, сведения о правонарушениях, здоровье, окружающей среде, транспортном обслуживании и научных исследованиях.

В настоящее время подготовлен проект новой Директивы[339] в целях устранения существующих барьеров, препятствующих эффективному использованию PSI. В частности, в качестве таких барьеров были названы следующие обстоятельства:

1. данные, генерируемые коммунальными и транспортными службами, имеющие большой потенциал для использования, не подпадают под действие существующей Директивы, несмотря на тот факт, что деятельность таких служб преимущественно финансируется за государственный счет. Указанное справедливо и в отношении данных исследований, финансируемых государством;
2. крайне редко предоставляется доступ в режиме реального времени к динамическим данным (*dynamic data*), имеющим на сегодняшний день наибольшую коммерческую ценность;
3. необоснованно завышенный размер платы за предоставление данных, что препятствует использованию данных малыми и средними предприятиями (*SMEs*).

Проект новой директивы направлен на устранение существующих барьеров посредством увеличение доступности PSI, расширение их состава, снижения стоимости за предоставление данных, поощрение использования динамических данных и т.д.

---

[338] EU Open Data Portal [Electronic resource]– URL: http://data.europa.eu/euodp/en/home (accessed: 30.07.2018).

[339] Proposal for a directive of the European parliament and of the Council on the re-use of public sector information (recast) – April 25, 2018 – [Electronic resource] // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0234:FIN (accessed: 30.07.2018).

Регулирование коммерческой тайны в ЕС

Регулированию данного вида тайн посвящена Директива N 2016/943 Европейского Парламента и Совета ЕС о защите конфиденциальных ноу-хау и деловой информации (коммерческой тайны) от незаконного приобретения, использования и раскрытия (далее – «Директива 2016/943»)[340]. Государства-члены ЕС должны были до 9 июня 2018 г. привести свое национальное законодательство в соответствие с положениями Директивы 2016/943. При этом они вправе предусмотреть дополнительные способы защиты коммерческой тайны.

Как отмечено в преамбуле, «коммерческая тайна играет важную роль в деле защиты обмена знаниями между субъектами предпринимательской деятельности, включающими в себя, в частности, малые и средние предприятия (*SMEs*), а также исследовательские учреждения в пределах и за рамками внутреннего рынка, в области исследований, разработок и инноваций. Коммерческая тайна является одной из наиболее общераспространенных форм защиты бизнесом результатов интеллектуальной деятельности и инновационного ноу-хау, однако в то же время коммерческая тайна является наименее защищенной с помощью средств имеющейся правовой базы Союза от незаконного приобретения, использования или раскрытия третьими лицами»[341].

Определение коммерческой тайны содержится в ст. 2, в частности, коммерческая тайна обозначает информацию, отвечающую всем нижеперечисленным требованиям:

(a) она является секретной в том смысле, что она полностью или в части не является общеизвестной или общедоступной для круга лиц, обычно имеющих дело с такого рода информацией;

(b) она обладает коммерческой ценностью, т.к. не доступна третьим лицам;

(c) владельцем информации были предприняты необходимые меры для сохранения ее в тайне.

В преамбуле Директивы 2016/943 отмечено, что такое определение коммерческой тайны охватывает ноу-хау, деловую информацию и техническую информацию, в случае если такая информация соответствует установленным требованиям, и у ее владелец вправе

[340] О защите конфиденциальных ноу-хау и деловой информации (коммерческой тайны) от незаконного приобретения, использования и раскрытия [Электронный ресурс]: директива Европейского парламента и Совета Европейского Союза. – № 2016/943 – 08.06.2016. – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 30.07.2018).

[341] О защите конфиденциальных ноу-хау и деловой информации (коммерческой тайны) от незаконного приобретения, использования и раскрытия / Там же.

сохранить ее в секрете. Виды информации, которые могут составлять коммерческую тайну, не могут быть ограничены. «Под определение коммерческой тайны не подпадает обычная информация и опыт, полученный сотрудниками в ходе обычного выполнения ими их трудовых обязанностей, а также из определения исключается общеизвестная информация или информация, к которой имеется свободный доступ лиц, в кругу которых принято иметь дело с такого рода информацией. Примечательно, что ни на информацию, охраняемую в качестве коммерческой тайны, ни на ноу-хау не устанавливается никаких исключительных прав.»[342] Таким образом, должна сохраняться возможность для самостоятельного выявления одних и тех же ноу-хау или информации.

Использование или разглашение коммерческой тайны может осуществляться исключительно с согласия ее обладателя. Нарушителем, а значит и ответчиком, может быть любое лицо, которое приобрело информацию, составляющую коммерческую тайну, незаконно, в частности путем несанкционированного доступа, присвоения, копирования документов, предметов, материалов, веществ или электронных файлов, или нарушило соглашение о конфиденциальности, или нарушило договорное или любое другое обязательство по ограничению использования коммерческой тайны (пп. 2, 3 ст. 4 директивы 2016/943). Обязательство по сохранению конфиденциальности информации накладывается на всех участников судебного разбирательства по вопросу незаконного приобретения, использования или раскрытия коммерческой тайны.

Приобретение, использование и раскрытие коммерческой тайны в случаях, разрешенных законодательством, должно расцениваться как правомерное. В частности, это относится к приобретению и раскрытию коммерческой тайны в контексте осуществления прав представителей работников на получение информации, консультаций, в ходе коллективной защиты прав работников и работодателей, а также приобретение или раскрытие коммерческой тайны при проведении обязательного аудита.

Государства-члены ЕС обязаны обеспечить, чтобы за раскрытие коммерческой тайны и иные правонарушения компетентные судебные органы могли применить к нарушившей стороне «одну или более из нижеуказанных мер:

(a) прекращение или, в зависимости от ситуации, запрет использования или раскрытия

[342] О защите конфиденциальных ноу-хау и деловой информации (коммерческой тайны) от незаконного приобретения, использования и раскрытия / Там же.

коммерческой тайны;

(b) запрет на производство, предложение, размещение на рынке или использование контрафактных товаров или импорт, экспорт или хранение контрафактных товаров для указанных целей;

(c) принятие в отношении контрафактных товаров надлежащих корректировочных мер (изъятие с рынка контрафактных товаров, лишение контрафактных товаров их контрафактных качеств, уничтожение контрафактных товаров);

(d) уничтожение полностью или частично любого документа, объекта, материала, вещества или электронного файла, содержащего или воплощающего собой коммерческую тайну, или, если применимо, передача заявителю полностью или частично любых из указанных документов, объектов, материалов, веществ или электронных файлов.»[343]

Вместо указанных мер суды должны при определенных условиях иметь право взыскать денежную компенсацию (если лицо добросовестно приобрело коммерческую тайну, но только позднее узнало, что информация была получена из источников, использующих соответствующую коммерческую тайну незаконно), либо возместить владельцу коммерческой тайны ущерб в размере, равном действительному ущербу, причиненному в результате незаконного приобретения, использования или раскрытия коммерческой тайны.

На примере Эстонии общие подходы ЕС конкретизируются следующим образом. Положения, регулирующие коммерческую тайну, содержатся в Законе о конкуренции[344], Коммерческом кодексе[345], Трудовом кодексе[346] и Уголовном кодексе. Сведения, составляющие коммерческую тайну, такие как: техническая и финансовая информация, относящаяся к ноу-хау, секретам производства и процессов, источникам поставок, объемам закупок и продаж, рыночной доле, клиентам и дистрибьюторам, маркетинговым планам, ценовой политике и структурированию, перечислены в статье 63 Закона о конкуренции. В дополнение к этому Верховный суд ранее пояснял, что при определении того, что охраняется коммерческой тайной, применяется определение, используемое в Соглашении по торговым

[343] О защите конфиденциальных ноу-хау и деловой информации (коммерческой тайны) от незаконного приобретения, использования и раскрытия / Там же.

[344] Competition Act of June 05, 2001 (as revised December 06, 2017) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/527122017001/consolide (accessed: 30.07.2018).

[345] Commercial Code of February 15, 1995 (as revised October 26, 2017) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/519122017001/consolide (accessed: 30.07.2018).

[346] Employment Contracts Act of December 17, 2008 (as revised June 06, 2018) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/529062018003/consolide (accessed: 30.07.2018).

аспектам интеллектуальной собственности или ТРИПС.

Как было указано в соответствующем разделе настоящего отчета, на уровне ЕС была утверждена Директива 2016/943, посвящённая регулированию вопросов коммерческой тайны. Как было отмечено в преамбуле, между законодательством государств-членов ЕС имеются существенные различия в отношении вопросов защиты коммерческой тайны от незаконного приобретения, использования и раскрытия со стороны третьих лиц. Существующие различия между формами правовой защиты коммерческой тайны, предусмотренными в государствах-членах ЕС, свидетельствуют о том, что коммерческая тайна не обладает эквивалентным уровнем защиты на территории всего Евросоюза, что, в свою очередь, ведет к фрагментации внутреннего рынка в данной области и к ослаблению общего сдерживающего воздействия применимых правил. Все это послужило основой для принятия Директивы 2016/943, которая позволит сблизить соответствующее законодательство государств-членов ЕС, чтобы обеспечить наличие достаточного и единообразного для всех государств уровня гражданско-правового возмещения вреда, причиненного владельцу коммерческой тайны на внутреннем рынке, в случае незаконного приобретения, использования или раскрытия коммерческой тайны.

Как было отмечено ранее, государства-члены ЕС должны были до 9 июня 2018 г. привести свое национальное законодательство в соответствие с положениями Директивы 2016/943, однако, согласно публичным источникам, Эстония до настоящего момента данное требование не выполнила. Проект Закона о предотвращении недобросовестной конкуренции и защите коммерческой тайны (*Unfair Competition Prevention and Trade Secret Protection Act*) находится в разработке.

Платформа "Open Data" в Эстонии

Эстония является одной из передовых стран по части развития информационных технологий в государственном секторе, большинство государственных сервисов переведены в режим онлайн. В основе цифрового взаимодействия лежит принцип «*once-only*», в соответствии с которым государство не должно запрашивать одну и ту же информацию у граждан дважды. Например, если данные об адресе родственников были предоставлены в службу переписи населения, то фонд медицинского страхования не должен запрашивать их повторно. Дальнейшее развитие и расширение сфер использования данных и аналитики

(включая *Big data*) в целях развития публичных сервисов и полноценного использования данных для усовершенствования процедуры принятия решений были озвучены в качестве основных направлений в Таллинской декларации по электронному правительству[347].

Законом о публичной информации (*Public Information Act*)[348] закреплена возможность, так называемого, повторного использования публичных данных, что означает публичное использование данных (*open data*), не ограниченное законом и в установленном порядке физическими или юридическими лицами для коммерческих и некоммерческих целей, отличных от тех, для которых данные были первоначально собраны. При этом должны быть обеспечены неприкосновенность частной жизни и защита авторских прав, национальной безопасности, коммерческой тайны и иной информации ограниченного доступа. Если информация, раскрываемая в соответствии с законом, содержит персональные данные и раскрытие такой информации представляет собой существенную угрозу неприкосновенности частной жизни, то публичное использование такой информации может быть ограничено. Если же публичное раскрытие такой информации нарушит неприкосновенность частной жизни, то информация не должна быть раскрыта полностью или может быть раскрыта в части или таким образом, чтобы это не привело к существенному нарушению неприкосновенности частной жизни.

В целях реализации указанного закона в Эстонии создана платформа *Open data portal*[349], аккумулирующая публичные базы данных, созданные различными государственными и муниципальными органами власти. *Open data portal* позволяет владельцам данных регистрироваться и размещать на платформе собранную информацию, а заинтересованным лицам и гражданам – искать, скачивать опубликованные данные и использовать для дальнейшей обработки. Данная платформа была разработана в целях стимулирования экономического развития, повышения прозрачности, снижения количества информационных запросов и, как следствие, уменьшение нагрузки на государственный сектор, стимулирование создания и управления открытыми сервисами в частном и государственном секторах, переход к новым технологиям, использующим связанные данные,

[347] Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU on 6 October 2017 [Electronic resource] // EU2017.EE [Site]. – URL: https://www.eu2017.ee/node/4551.html (accessed: 08.08.2018).

[348] Public Information Act of November 15, 2000 (as revised June 14, 2017) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/514112013001/consolide (accessed: 30.07.2018).

[349] About open data portal of Estonia [Electronic resource] // Open data portal of Estonia [Site]. – URL: https://opendata.riik.ee/en/about (accessed: 30.07.2018).

большие данные (*Big data*) и Интернет вещей (*Internet of Things*).

Открытые данные, размещаемые на платформе, представляют собой исходные данные (*raw data*), которые по усмотрению владельца раскрываются посредством предоставления онлайн доступа любому лицу в машиночитаемом виде и без всяких ограничений на использование и дальнейшее распространение. В частности, на платформе размещаются базы данных, созданные различными государственными и муниципальными органами власти, публичное использование которых не запрещается законом напрямую, и которые содержат иные данные, кроме персональных. Если же база данных содержит, как персональные, так и не персональные данные, в таком случае публикуются только последние. Также могут быть опубликованы данные третьих лиц, если они представляют общественный интерес. Опубликованные данные не должны позволять идентифицировать конкретных людей, за исключением тех случаев, когда такие данные уже были ранее раскрыты (например, имена гражданских служащих, работающих в министерствах).

Данные могут быть представлены в форме собрания договоров, положений, метаданных, файлов бюджетов и статистики, баз или реестров, представленных в машиночитаемой форме или вэб-сервисов, которые позволяют искать информацию в таких базах или реестрах. С технической точки зрения это могут быть сборники текстовых файлов или подборки данных в машиночитаемой форме.

Данные могут использоваться в самых различных целях, например, для анализа тенденций в определенных сферах жизнедеятельности, сравнения данных различных органов, для создания различных сервисов и приложений, включая коммерческое использование.

Некоторое время назад была анонсирована инициатива *Advancing the Use of Open Data* по дальнейшему продвижению использования открытых данных. Проект разработан добровольной общественной ассоциацией *Open Knowledge Estonia*, выступающей за свободный доступ к информации и являющейся частью глобальной сети *Open Knowledge network*[350] совместно с Министерством экономических дел и связей. Целью инициативы является систематическое развитие использования открытых данных в Эстонии, увеличение степени осведомленности населения об открытых данных и их пользователях, усиление взаимодействия между владельцами данных и пользователями, развитие инновационных

[350] Open Knowledge International [Electronic resource] // Open data portal of Estonia [Site]. – URL: https://okfn.org/ (accessed: 30.07.2018).

сервисов на основе данных.

«Предполагаемое» согласие в штате Калифорния, США

Предполагаемое согласие, или opt-out, на сегодняшний день достаточно распространено в Соединенных Штатах Америки. Принятый 28 июня 2018 года Закон Калифорнии о личной информации клиентов (“CCPA”), вступающий в силу 1 января 2020 года, не является первым нормативно-правовым актом, который предоставил право субъектам персональных данных (клиентам) на отказ от использования организацией или раскрытия их персональных данных. Другие федеральные законы, включая Закон Грамма-Лича-Блили (“GLBA”) и Закон о борьбе со спамом (“CAN-SPAM Act”) содержат право на opt-out[351].

Нормы CCPA защищают как всех резидентов Калифорнии, так и, в целом, информацию, относимую к ним. Хотя нормативно-правовой акт оперирует словом клиент (consumer), в §1798.140(g) Гражданского кодекса Калифорнии (“Cal. Civ. Code”) имеется норма-дефиниция, где под клиентом понимается «физическое лицо, являющееся резидентом Калифорнии, как определено в ст. 17014 раздела 18 Административного кодекса Калифорнии…». Соответственно, под действие закона подпадают не только клиенты в узком смысле слова, но и работники, пациенты, арендаторы, студенты, родители, дети и т.д[352].

В отличие от других разделов Гражданского кодекса штата Калифорния и иных законов о конфиденциальности упомянутый кодекс в §1798.140 (o) (1) широко определяет термин «личная информация» как «любую информацию, которая ... относится к ... конкретному потребителю или к домохозяйству». Данные должны быть защищены, даже если (1) они не относятся к конкретному человеку (поскольку «домашние хозяйства» также входят в субъектов личной информации), и даже если (2) информация о физическом лице не содержит его полного имени. Например, ежегодное потребление воды или энергии домохозяйства, расписание работы сотрудника, адрес интернет-протокола, история просмотра веб-страниц и «история покупок» будут регулироваться как личная информация, даже если с ней не связаны имена субъектов.

[351] The Practical Guide to the California Consumer Privacy Act: Part 5 The Right to Opt-Out of Information Selling [Electronic resource]: Lexology [Site]. - URL: https://www.lexology.com/library/detail.aspx?g=0d9dd1cc-dbd6-4e83-8c08-9aaaacccc6d6 (accessed: 02.10.2018)
[352] Analysis: The California Consumer Privacy Act of 2018 [Electronic resource]: IAPP [Site]. - URL: https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/ (accessed: 02.10.2018)

Для того, чтобы соответствовать CCPA организациям, необходимо:

1. Проверить существующие на сайте политики (уведомления) о конфиденциальности и убедиться, что они отвечают новым требованиям CCPA.
2. Предоставить ясную и заметную ссылку «Не продавайте мою личную информацию» на домашней странице организации, которая будет направлять пользователей на веб-страницу, позволяющую резидентам или их представителям отказаться от продажи личной информации (Гражданский Кодекс Калифорнии §1798.135 (a) (1)).
3. Установить необходимые, соответствующие требованиям CCPA способы подачи субъектами персональных данных запросов об отказе (opt-out) в вашу организацию.
4. Разработать соответствующую политику для идентификации лиц, делающих запросы об отказе (opt-out).
5. Разработать методику, представляющую из себя стандартные сообщения, которые могут быть направлены лицам в ответ на запросы (“play book”).
6. Обучить сотрудников, как необходимо отвечать на запросы (opt-out).
7. Убедиться, что применяемые политики и методики облегчают исполнение запросов в течение периода времени, установленного CCPA[353].

Таким образом, opt-out необходимо рассматривать как одну из форм получения согласия, максимально удобную для организаций, хотя и требующую определенных усилий и регламентации внутренних бизнес-процессов со их стороны для защиты субъектов персональных данных. Однако стоит отметить, что не все ученые согласны с тем, что данный метод является обоснованным для применения на практике. Ученые университета Пенсильвании в 2009 году провели исследование[354] о таргетированной рекламе, и в частности об отношении американцев к opt-out в связи с ней. Они цитируют опросы, проведенные Союзом потребителей, свидетельствующие о том, что 72% американцев не хотят быть таргетированы. При этом они обращают внимание на то, что, например, технология cookies не является достаточно простой (не всегда компании, даже после opt-out пользователя, перестают его отслеживать, ученые указывают, что таргетирование прекращается, но трекинг

[353] The Practical Guide to the California Consumer Privacy Act: Part 5 The Right to Opt-Out of Information Selling [Electronic resource]: Lexology [Site]. - URL: https://www.lexology.com/library/detail.aspx?g=0d9dd1cc-dbd6-4e83-8c08-9aaaacccc6d6 (accessed: 02.10.2018)

[354] J. Turow, J. King, C.J. Hoofnagle, A. Bleakley and M. Hennessy, ‘Americans Reject Tailored Advertising’. Annenberg: University of Pennsylvania, 2009.

пользователей - нет). Кроме того, многие сайты предлагают лишь согласиться с передачей cookies, иначе сайты не смогут работать в нормальном режиме в браузере пользователя, что ставит пользователя сайта в неудобное положение, когда он должен вручную удалять cookies.

Законодательство о критической информационной инфраструктуре РФ

Дополнительно стоит упомянуть специальные требования информационно безопасности в отношении обеспечения защиты критической информационной инфраструктуры.

Критической информационной инфраструктурой (далее – «КИИ») признаны информационные системы, сети и автоматизированные системы управления, которые:

(а) функционируют в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности

и при этом

(б) принадлежат субъектам КИИ, в качестве которых рассматриваются не только государственные органы и учреждения, но и российские юридические лица и (или) индивидуальные предприниматели, которым принадлежат указанные объекты КИИ либо которые обеспечивают взаимодействие указанных систем или сетей.

Из этого следует, в частности, что владельцами (пользователями) КИИ могут быть только российские юридические лица и индивидуальные предприниматели.

Законодательство устанавливает принципы обеспечения безопасности КИИ: законность, непрерывность и комплексность обеспечения безопасности, приоритет предотвращения компьютерных атак (что особенно актуально в свете мировых событий 2017 года в области кибербезопасности).

Основными источниками, в которых содержатся требования к информационной безопасности, являются:

- **Федеральный закон от 26.07.2017 № 187-ФЗ** «О безопасности критической информационной инфраструктуры Российской Федерации» УК РФ Статья 274.1 – до 8 лет лишения свободы;
- **Постановление Правительства РФ от 08.02.2018 № 127** «Об утверждении Правил

категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;

- **Приказ ФСТЭК России от 21.12.2017 N 235** «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (Зарегистрировано в Минюсте России 22.02.2018 N 50118);
- **Приказ ФСТЭК России от 06.12.2017 N 227** «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» (Зарегистрировано в Минюсте России 08.02.2018 N 49966);
- **Указ Президента РФ от 22.12.2017 N 620** «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Личная информация, тайна связи, врачебная и банковская тайны в Японии

Общий обзор. В Японии четкое разделение различных видов тайн, как это предусмотрено, например, российским законодательством, не предусмотрено (за исключением секретов производства и тайны связи). В частности, законодательство Японии не содержит четких правил, определяющих содержание, порядок раскрытия медицинской тайны, тайны связи и т.д., не содержит положений, которые были бы направлены на обеспечение конфиденциальности банковской информации. Законодательство не содержит системных правил использования (в том числе предоставления третьим лицам) сведений, составляющих различные виды тайны. Правовые режимы охраны информации ограниченного доступа, отличаются не только по отраслевому признаку, но и по субъекту использования. Для коммерческих организаций и публично-правовых образований установлены различные правила использования персональной информации физических лиц.

Условно систему права Японии в области защиты информации можно представить следующим образом.

1. Закон Японии о защите персональной информации (Act on the Protection of Personal

Information No. 57 of 2003, APPI[355]), который является основным источником регулирования использования **коммерческими организациями и предпринимателями** любых видов тайн, включающих персональную информацию физических лиц. К таким тайнам относятся: тайна личной жизни, тайна связи, медицинская тайна. Частично Закон регулирует и сведения, составляющие банковскую и профессиональную тайну.

2. Отраслевое законодательство, которое, как правило, содержит положения о недопустимости разглашения соответствующей информации, позволяет определить круг охраняемой информации и предусматривает некоторые меры ответственности за нарушение конфиденциальности. Например, Закон Японии о телекоммуникационном бизнесе (Telecommunication Business Law No. 25, 1984[356]), Закон Японии о медицинской помощи (Medical Care Act No. 205 of July 30, 1948[357]).
3. Положения (т.н. Guidelines) министерств/ведомств (имеющих компетенцию в отраслях использования персональной информации), которые толкуют Закон Японии об использовании персональной информации. Таких положений более 40[358].
4. Закон Японии № 58, регулирующий использование персональной **информации государственными органами** (Act on the Protection of Personal Information Held by Administrative Organs No. 58 of 2003[359]), .
5. Закон Японии о доступе к информации государственных органов или Закон № 42 (Act on Access to Information Held by Administrative Organs No. 42 of 1999[360]).

---

[355] Act on the Protection of Personal Information No. 57 of 2003 [Electronic resource] // Personal Protection Commission of Japan [Site]. – URL: https://www.ppc.go.jp/files/pdf/280222_amendedlaw.pdf (accessed: 08.08.2018).

[356]Telecommunication Business Law No. 25, 1984 [Electronic resource] // Ministry of Internal Affairs and Communications [Site]. – URL: http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/2001TBL.pdf (accessed: 08.08.2018).

[357] Medical Care Act No. 205 of July 30, 1948 [Electronic resource] // Japanese Law Translation [Site]. – URL: http://www.japaneselawtranslation.go.jp/law/detail/?id=2199&vm=04&re=02 (accessed: 08.08.2018).

[358] The Privacy, Data Protection and Cybersecurity Law Review, Edition 4. Privacy Law Review [Electronic resource] // The Law Reviews [Site]. – URL: https://thelawreviews.co.uk/edition/1001106/the-privacy-data-protection-and-cybersecurity-law-review-edition-4 (accessed: 08.08.2018).

[359] Act on the Protection of Personal Information Held by Administrative Organs No. 58 of 2003 [Electronic resource] // Japanese Law Translation [Site]. – URL: http://www.japaneselawtranslation.go.jp/law/detail_main?re=&vm=02&id=131 (accessed: 08.08.2018).

[360] Act on Access to Information Held by Administrative Organs No. 42 of 1999 [Electronic resource]: Japanese Law Translation // Japanese Law Translation [Site]. – URL: http://www.japaneselawtranslation.go.jp/law/detail_main?id=99&vm=2&re= (accessed: 08.08.2018).

6. Базовые законы Японии, такие как Конституция Японии, Уголовный кодекс Японии, Гражданский кодекс Японии, процессуальные кодексы.

В этой связи, в отличие от юрисдикций, по которым прослеживается четкое разделение видов тайн и/или правового режима использования информации, составляющей разные виды тайн (см., например, раздел настоящего Отчета по Российской Федерации), результаты исследования в части анализа законодательства Японии по вопросам, изложенным в Техническом задании, будут, главным образом, разделены по видам субъектов, обрабатывающих информацию конфиденциального характера.

Некоторые специальные правила оборота и использования тех или иных видов конфиденциальной информации, сформулированные в отраслевом законодательстве, рекомендациях государственных органов и/или судебной практике, такие правила будут указаны отдельно.

При этом, поскольку сведения, составляющие тайну личной жизни, медицинскую тайну и тайну связи, имеют прямое отношение к персональной информации физических лиц, а защита таких сведений носит публично-частный характер, они будут рассматриваться отдельно.

Банковская и коммерческая тайны будут рассмотрены отдельно в связи со следующим:

- Банковская тайна имеет пересечение с названными выше видами тайн и регулируется Законом о персональной информации только в части клиентской информации физических лиц . В других случаях банковская тайна имеет иной правовой режим.
- Коммерческая тайна, по своему содержанию и характеру отличается от медицинской тайны, банковской тайны, тайны связи, тайны личной жизни и имеет свое регулирование. Также, большинство вопросов Технического задания (касающиеся предоставления третьим лица, администрирования согласий и т.п.) для данного вида тайны неприменимы.

Тайна связи, тайна личной жизни, медицинская тайна. Закон Японии о защите персональной информации содержит довольно широкое определение **персональной информации**. Персональная информация - это информация о живом физическом лице,

подпадающая под одну из следующих категорий:

- информация, которая содержит имя, дату рождения или иное описание и т.д., изложенные, зафиксированные или иным образом выраженные посредством голоса, движений или иными средствами в документе, изображении или электронной записи (т.е. записи, которая хранится в электромагнитной форме, под электромагнитной формой понимается такая форма, которая недоступна для восприятия человеческими чувствами), с помощью которой может быть определено конкретное лицо или которое можно соотнести с такой информацией и идентифицировать;
- информация, которая содержит идентифицирующий код. Под идентифицирующим кодом понимаются любые номера, символы и т.д., которые предусмотрены Кабинетом министров Японии, включая: (а) символы, буквы, номера или иные коды, которые позволяют идентифицировать лицо и которые были конвертированы в машиночитаемый код для обработки компьютерами; (б) такие символы, буквы, номера или иные коды, которые присвоены для оказания услуг лицу или продажи лицу товаров, или которые содержатся или зафиксированы в электромагнитной форме в документе, выданном физическому лицу, для целей идентификации конкретного пользователя или покупателя, или получателя помощью генерации и присвоения таких кодов такому пользователю, покупателю или получателю.

Стоит отметить, что используется термин «персональная информация», а не «персональные данные», которые в Законе Японии о защите персональной информации имеет другое значение.

Важно, что любой документ или иной носитель, который содержит соответствующую информацию, автоматически подпадает под понятие «персональная информация» (ст. 2(1), ст. 2(2) Закона Японии о защите персональной информации).

Отдельно выделяется чувствительная информация (special-care required personal information), которая включает медицинскую историю, которая по своему содержанию тождественна медицинской тайне (ст. 2(3) Закона Японии о защите персональной информации).

Тайна связи. Закон о телекоммуникационном бизнесе (содержит запрет на цензуру и просмотр сообщений (ст. 3) и предусматривает, что конфиденциальность коммуникаций не

должна нарушаться (ст.(1) Закона о телекоммуникационном бизнесе).

Конституция Японии[361] также гарантирует тайну связи (ст. 21 Конституции Японии).

Таким образом, конфиденциальный характер устанавливается и в отношении самих сообщений, даже если они не содержат персональной информации.

Согласно Отчету об использовании анонимной информации, подготовленному Японским ведомством в сфере защиты персональной информации (The PPC Secretariat Report on Anonymously Processed Information[362]) адреса электронной почты, номера телефонов отнесены к информации, которая может идентифицировать персональную информацию. В Японии существует концепция т. н. «связующих кодов» («codes linking»). Отчет предусматривает, что создания обезличенной информации связующие коды (в том числе такие как), которые могут быть использованы для идентификации лица, должны быть удалены (п. 4.1.3 Отчета). Дополнительно Отчет предусматривает, что идентификационный номер устройства относится к т.н. highly constant ID (п. 4.5.1.2).

Медицинская тайна. Отдельные законы и до вступления в силу Закона Японии о персональных данных устанавливали запрет на раскрытие медицинскими работниками информации, ставшей им известной в ходе осуществления профессиональных обязанностей (без уточнения состава таких сведений), и ответственность за нарушение этой обязанности[363]. Между тем, на данный момент основным источником регулирования вопросов использования сведений, составляющих медицинскую тайну, является Закон Японии о персональной информации, который предусматривает, что к чувствительной информации (special care-required information) относится медицинская история (ст. 2(3) Закона Японии о персональной информации)[364]. Согласно Правилам соблюдения Закона о персональной информации (Enforcement Rules for the Act on the Protection of Personal Information dated May

[361] The Constitution of Japan [Electronic resource]: Promulgated on November 3, 1946. Came into effect on May 3, 1947 // Official Website of the Prime Minister and His Cabinet [Site] – URL: https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html (accessed: 08.08.2018).

[362] The PPC Secretariat Report on Anonymously Processed Information [Electronic resource]: Personal Information Protection Commission of Japan // Personal Information Protection Commission of Japan [Site]. – URL: https://www.ppc.go.jp/en/legal/ (accessed: 08.08.2018).

[363] Act on public Health Nurses, Midwives, and Nurses Review [Electronic resource]: adopted in Japan on 30 Jul.1948 // Japanese Law Translation [Site]. – URL: http://www.japaneselawtranslation.go.jp/law/detail/?id=2075&vm=04&re=02 (accessed: 08.08.2018).

[364] Yuichiro Tsuji. Medical Privacy Issues in Ageing Japan // Australian Journal of Asian Law – 2017. - No.1. – P. 1-18.

30, 2017[365]) к такой информации, втом числе относятся: сведения о физических недостатках или психических расстройствах, которые подробно перечислены в Законе о благополучии лиц с физическими недостатками Act for the Welfare of Persons with Physical Disabilities, Act No. 283 of 1949), Законе о благополучии лиц с психическими расстройствами (Act for the Welfare of Persons with Intellectual Disabilities, Act No. 37 of 1960), Законе о благополучии лиц с умственными расстройствами (Act for the Welfare of Persons with Mental Disabilities, Act No. 123 of 1950).

Тайна личной жизни. Право на неприкосновенность частной жизни и тайну личной жизни выводится из ст. 13 Конституции Японии, согласно которой право на жизнь, свободу и стремление к счастью должны быть основными принципами в законодательство и публичных делах. Прямо именно право на тайну личной жизни Конституция Японии не закрепляет. Судебная практика так толкует ст. 13 Конституции, что право на свободу означает и право на сохранение конфиденциальности личной информации (см. Решение Верховного суда Японии № 1187 от 24 декабря 1969 г., Keishu Vol.23, No. 12[366]).

Закон Японии о защите персональной информации, не содержит исчерпывающего состава сведений, которые относятся к персональной информации, понятие является описательным. При этом отраслевое законодательство, как правило, также не раскрывает содержания конфиденциальной информации, а лишь устанавливает запрет на незаконное разглашение.

В этой связи ориентироваться следует на Положения, судебную практику и толкование, которое дается в толковании Японского ведомства, уполномоченного в сфере защиты персональной информации (Personal Protection Commission of Japan[367]). Как отмечают авторы состав сведений оставляющих персональную информацию, является определимым, а не определенным[368].

Тем не менее, можно следующие виды информации можно однозначно отнести к различным видам тайн:

---

[365] Enforcement Rules for the Act on the Protection of Personal Information dated May 30, 2017 [Electronic resource] // Personal Information Protection Commission of Japan [Site]. – URL: https://www.ppc.go.jp/files/pdf/PPC_rules.pdf (accessed: 08.08.2018).

[366] Supreme Court of Japan [Electronic resource] // Supreme Court of Japan [Site]. – URL: http://www.courts.go.jp/app/hanrei_en/detail?id=34 (accessed: 08.08.2018).

[367] Personal Protection Commission of Japan [Electronic resource] // Personal Informatuion Protection Comission of Japan [Site]. – URL: https://www.ppc.go.jp/en/ (accessed: 08.08.2018).

[368] Yuichiro Tsuji. Medical Privacy Issues in Ageing Japan // Australian Journal of Asian Law – 2017. - No.1. – PP. 1-18.

(1) Содержание любых сообщений, метаданные, которые содержат персональную информацию отправителя и/или получателя, приложенные к сообщениям документы, которые содержат персональную информацию любых лиц, электронные сообщения, явно адресованные конкретному лицу или исходящие от него; при этом прямо указывается, что книги и иные подобные товары, различные рекламные материалы, инструкции и иные подобные документы, не адресованные конкретному лицу, к корреспонденции не относятся (тайна связи)[369];

(2) Сведения, составляющие медицинскую тайну, четко не определены[370].

В Японии не разграничиваются различные виды тайн, персональные данные и иные виды конфиденциальной информации, как предусмотрено российским законодательством. Широкое понятие «персональная информация» по своему содержанию может включать различные сведения, обычно относимые в российском законодательстве к тем или иным видам тайн. Стоит отметить, что при этом данные, содержательно между собой не отличающиеся могут иметь различные правовые режимы использования. Так, использование персональной информации, публично-правовыми организациями имеет свое регулирование, использование анонимной и псевдонимной информации (далее - анонимной) – свое регулирование. При этом **специальный правовой режим использования анонимной информации установлен для предоставления больших возможностей коммерциализации и использования Big Data**.

В целом, различные виды тайн на законодательном уровне между собой четко не разграничиваются. Между тем, стоит отметить, что многие виды сведений ограниченного характера представляют собой профессиональную тайну. Отраслевое законодательство, например, Закон Японии о телекоммуникационном бизнесе или Закон Японии о медицинских работниках (Act No. 203 On Public Health Nurses, Midwives, and Nurses of July 30, 1948[371]) запрещают разглашать те или иные сведения именно в качестве одной из профессиональных обязанностей. В названном выше деле (2007(Kyo)23) Верховный суд Японии рассматривал сведения клиента банка в качестве разновидности профессиональной тайны.

---

[369] What falls under the category of correspondence? [Electronic resource] // Japan Post [Site]. – URL: https://www.post.japanpost.jp/service/about_shinsyo_en.html (accessed: 08.08.2018).

[370] Yuichiro Tsuji. Medical Privacy Issues in Ageing Japan // Australian Journal of Asian Law – 2017. - No.1. – P. 1-18.

[371] Act on public Health Nurses, Midwives, and Nurses Review [Electronic resource]: adopted in Japan on 30 Jul.1948 // Japanese Law Translation [Site]. – URL: http://www.japaneselawtranslation.go.jp/law/detail/?id=2075&vm=04&re=02 (accessed: 08.08.2018).

Механизм правовой защиты субъектов состоит из следующих элементов:

(1) Права субъектов персональной информации на требования об уточнении, удалении, предоставление информации об обрабатываемых данных (ст. 28-32).

(2) Обязанность обработчика персональной информации реагировать на жалобы субъектов персональной информации о ненадлежащей обработке (ст. 35 Закона Японии о персональной информации).

(3) Некоторые отраслевые законы предусматривают специальные процедуры обращения к операторам данных с жалобами на нарушение прав, в том числе конфиденциальности информации (см., например, ст. 27 Закона Японии о телекоммуникационном бизнесе).

(4) Специальные требования в отношении обеспечения безопасности обрабатываемой персональной информации. Такие требования содержатся в Законе Японии о персональной информации, специальном законодательстве (см., например) и Положениях министерств и ведомств (см., например, Положение Министерства внутренних дел Японии «О защите персональной информации в телекоммуникационном бизнесе»[372]).

(5) На Правительство Японии, отраслевые министерства и ведомства возложена обязанность по обеспечению надлежащей обработки персональной информации в тех отраслях, в которых они имеют компетенцию (часть 2 Закона Японии о защите персональной информации).

(6) Возможность обращения в суд за защитой права на тайну связи с гражданско-правовым иском (ГК Японии).

(7) В случае незаконного распространения персональной информации или иной охраняемой законом информации в сети Интернет субъект, чьи права нарушены, вправе обратиться к информационному посреднику с требованием предоставить персональные данные пользователя услуг, который распространил соответствующую информацию (ст. 4 Закона об ограничении ответсвенности посредников).

Закон Японии о персональной информации предусматривает ответственность в

[372] Guideline of the Ministry on Internal Affairs On Protection of Personal Information in Telecommunication Business. [Electronic resource] // The Ministry of Internal Affairs and Communications [Site]. – URL: http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/others/110214_1.pdf (accessed: 08.08.2018).

отношении работников операторов персональной информации, которые незаконно использовали персональную информацию для своих личных целей или для целей третьих лиц в виде лишения свободы сроком до 1 года или штрафа в размере до 500 000 йен (примерно 280 000 рублей). Также закон предусматривает различные виды ответственности за несоблюдение требований Регулятора. Наконец, ответственность в отношении должностных лиц Регулятора (ст.ст. 82-86 Закона Японии о персональной информации).

УК Японии[373] отдельно предусматривает уголовную ответственность:

- За вскрытие без достаточных оснований запечатанного письма (ст. 133);
- За разглашение профессиональной тайны медицинскими работниками, прокурором, адвокатом (ст. 134);

Такие уголовные дела являются в Японии делами частного обвинения (ст. 135).

В соответствии с ГК Японии лицо, чье право нарушено, вправе требовать возмещения убытков (ст.ст. 709-710).

Отраслевое законодательство может также предусматривать дополнительные меры ответственности. Например, такие меры ответственности предусмотрены в отношении лиц, осуществляющих телекоммуникационный бизнес (ст. 179 Закона о телекоммуникационном бизнесе). Ответственность предусмотрена и в отношении медицинских работников (см., например, Закон о медицинских работниках). Некоторые из таких норм дублируют положения УК Японии.

Общие правила о порядке и условиях передачи сведений третьим лицам. Как и российское законодательство, Закон Японии о персональной информации разрешает предоставлять доступ к персональной информации с согласия субъекта персональной информации, а также без согласия в случаях, предусмотренных законодательством Японии, для защиты жизни, здоровья и при этом сложно получить согласие субъекта, для некоторых публичных целей (поддержание общественного здоровья, воспитание детей и т.д.), ст. 28 Закона о персональной информации. Оператор обязан предоставлять субъекту (или делать легко доступной) информацию о передаче его персональной информации третьим лицам, в том числе информацию о целях использования, категориях данных, методе предоставления (ст. 23(2), (3) Закона Японии о персональной информации). Оператор персональной информации обязан вести реестр третьих лиц, которым предоставляется персональная

[373] The Penal Code of Japan [Electronic resource] // Japanese Law Translation [Site]. – URL: http://www.japaneselawtranslation.go.jp/law/detail/?id=1960&re=02&vm=04 (accessed 08.08.2018).

информация (ст. 25 Закона Японии о персональной информации). При этом предоставление третьим лицам должно осуществляться в рамках завяленной цели обработки персональной информации (ст.15 Закона Японии о персональной информации) либо должно быть получено дополнительное согласие на использование в иных целях.

В соответствии с Законом о персональной информации, ст. 23 (5) следующие лица не считаются третьими лицами и, соответственно, на них не распространяются требования о получении согласия и иные подобные условия (ведение реестра, информирование субъекта и т.д.):

(1) Лица, которым оператор персональной информации доверил обработку персональной информации полностью или частично в оправданном объеме для достижения цели обработки.
(2) Лица, которые являются правопреемниками оператора персональной информации и будут использовать персональную информацию для тех целей, для которых их использовал оператор.
(3) Определенное лицо, которое использует персональную информацию совместно с оператором («совместный пользователь», joint user), о чем субъект персональной информации был заранее уведомлен или он легко мог узнать о существовании такого специального лица, целях, объемах и иных деталях обработки специальным лицом. Как видно из публичных политик обработки персональной информации некоторых японских компаний, такими «совестными пользователями», как правило, являются аффилированные лица[374].

По общему правилу, трансграничная передача персональной информации может осуществляться только с согласия субъекта персональной информации, за исключением следующих случаев:

(1) Когда согласие не требуется в соответствии со ст. 23 Закона Японии о персональной информации;
(2) Иностранное лицо, которому передается информация, устанавливает систему обработки и защиты персональной информации, соответствующую стандартам, предусмотренным Регулятором в отношении иностранных компаний, которые

[374]Statement on Personal Information Protection (Privacy Policy) [Electronic resource] // Bank of America Merrill Lynch [Site]. – URL: http://www.japan.ml.com/privacy/mljs_privacy_e3.asp (accessed: 08.08.2018).

эквивалентны тем стандартам, которые предусмотрены Законом Японии о персональной информации в отношении операторов персональной информации.

(3) Иностранное лицо, которому передается информация, находится на территории государства, которое устанавливает систему обработки и защиты персональной информации, соответствующую стандартам, предусмотренным Регулятором в отношении иностранных компаний, которые эквивалентны тем стандартам, которые предусмотрены Законом Японии о персональной информации в отношении операторов персональной информации.

В общем виде случаи передачи персональной информации третьим лицам без согласия таких лиц предусмотрены в ст. 23 Закона о персональной информации. В частности, к таким случаям относятся следующие:

(1) В целях защиты жизни и здоровья субъекта и когда получить согласие субъекта сложно.

(2) В целях поддержания общественного здоровья, воспитания детей и при этом сложно получить согласие субъекта персональной информации.

(3) Для целей сотрудничества с центральным или местным государственным органом или лицом, которому соответствующие органы делегировали исполнение своих полномочий, и при этом получение согласия у субъекта может помешать исполнению обязанностей соответствующих органов власти.

Специальные правила:

(1) Отдельные, более строгие правила доступа предусмотрены для сведений, составляющих тайну связи. В Японии принят и действует отдельный закон, который регулирует порядок прослушивания телефонных переговоров и перехвата сообщений в целях уголовного преследования (Law on Communications Interception During Criminal Investigation)[375]. Процедурные требования к порядку получения доступа к переговорам/сообщениям предусмотрены УПК Японии. В частности, такая мера допускается только в отношении определенных видов преступлений, по

[375] Yohei Suda. The Japanese Law on Communications Interception During Criminal Investigations: Translator's Introduction [Electronic resource] // School of Law. University of Washington [Site]. – URL: https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/778/10PacRimLPolyJ067.pdf?sequence=1&isAllowed=y (accessed: 08.08.2018).

судебному решению и т. д.[376]

(2) Некоторые случаи раскрытия сведений, составляющих медицинскую тайну, также предусмотрены отраслевым законодательством. Например, предоставление в полицию информации о мертворожденном (ст.41. Закона о медицинских работниках.

По общему правилу персональная информация пользователей телекоммуникационных услуг не может предоставляться третьим лицам без их согласия. Однако согласие не требуется в том случае, если такая информация необходима для целей исполнения публично-правовыми образованиями их полномочий и получение согласия у субъекта может помешать исполнению таких полномочий (положения Министерства Внутренних Дел Японии об обработке персональной информации в сфере телекоммуникаций от 2017 г.). Таким образом, сформулировано общее правило, а конкретные изъятия могут быть, как предусмотрены, так и не предусмотрены в специальных законах.

В отличие, от законодательства России, Закон Японии о персональной информации не содержит подробных правил относительно требований к формам согласий на обработку персональной информации.

Согласно Законодательству Японии работодатель вправе установить контроль в отношении коммуникаций работника, связанных с исполнением трудовых обязанностей. Вместе с тем, могут возникнуть вопросы относительно нарушения личных прав работника. В этой связи японские юристы рекомендуют установить внутренние правила, запрещающие использовать рабочие почту и телефон для личных целей[377].

Специальные правила о Big Data. Для создания благоприятных условий использования информации (включая большие данные) в коммерческих целях, в 2017 г. в Закон Японии об использовании персональной информации были внесены изменения, предусматривающие порядок использования обезличенной информации[378].

Обезличенные данные могут использоваться и предоставляться третьим лицам не для

---

[376] Hiromi Hayashi, Akiro International Comparative Legal Guides. Telecoms, Media & Internet, 2018. Japan [Electronic resource] // The International Comparative Legal Guide [Site]. – URL: https://iclg.com/practice-areas/telecoms-media-and-internet-laws-and-regulations/japan#chaptercontent4 (accessed: 08.08.2018)

[377] Hiromi Hayashi, Rina Shimada. Data Protection 2018/Japan [Electronic resource]: International Comparative Legal Guides [Site]. – URL: https://iclg.com/practice-areas/data-protection-laws-and-regulations/japan#chaptercontent1 (accessed: 08.08.2018).

[378] The Privacy, Data Protection and Cybersecurity Law Review, Edition 4. Privacy Law Review [Electronic resource] // The Law Reviews [Site]. – URL: https://thelawreviews.co.uk/edition/1001106/the-privacy-data-protection-and-cybersecurity-law-review-edition-4 (accessed: 08.08.2018).

тех целей, для которых изначально получена и обрабатывается персональная информация. Для этого не требуется получать дополнительное согласие Единственным условием предоставления обезличенной информации третьим лицам является публичное раскрытие категорий предоставляемой персональной информации (ст. 37 Закона Японии о персональной информации).

Правила соблюдения Закона Японии о персональной информации (Enforcement Rules for the Act on Protection of Personal Information) содержат подробные требования:

(1) К стандартам и методам создания обезличенной информации (не любая деперсонифицированная информация считается обезличенной по законодательству Японии, ст. 19 Правил);

(2) К сведениям, которые должны быть публично раскрыты при создании обезличенной информации (ст. 20 Правил);

(3) К сведениям, которые должны быть публично раскрыты при предоставлении обезличенной информации третьим лицам (ст. 21 Правил).

Отдельного внимания заслуживает Отчет об использовании анонимной информации, подготовленный Японским ведомством в сфере защиты персональной информации, который детально разъясняет порядок создания и использования обезличенной информации.

Отчет прямо предусматривает, что система использования обезличенной информации создана специально для создания условий и возможности использования (в том чсиле обмена) информации в иных целях, чем те, для которых эти сведения изначально были получены. По мнению законодателя, наличие такой системы является предпосылкой для развития бизнеса, предоставления новых услуг (п. 3.1 Отчета).

Далее в Отчете приводится понятие анонимной информации и раскрывается каждый элемент этого определения (например, п. 3.2.2 What Does the Phrase «Not to be Able to Restore Information» Mean, п. 3.5 What Does it Mean to Produce Anonymously Processed information). Согласно Отчету ***статистическая информация*** не относится ни к персональной информации, ни к обезличенной информации (п. 3.4.1). Также отчет предусматривает различные методы анонимизации в отношении персональной информации разного рода, подробно описывая их (п. 4.3»).

Оператор, обрабатывающий обезличенную информацию обязан предпринять специальные меры безопасности, направленные на недопущение раскрытия метода обезличивания (п. 3.3 Отчета).

Лицо, которое получает обезличенную информацию, не вправе предпринимать действия, направленные на персонификацию информации.

Интересно, что Отчет приводит конкретные примеры использования обезличенной информации и графические алгоритмы использования (п. 7.1 Отчета). Например, ритейлеры могут предоставить историю покупок в обезличенном виде другим компаниям, которые, в свою очередь, могут использовать эту информацию для целей анализа поведения покупателей, выявления определенных трендов и предложения новых сервисов/услуг и т.д.

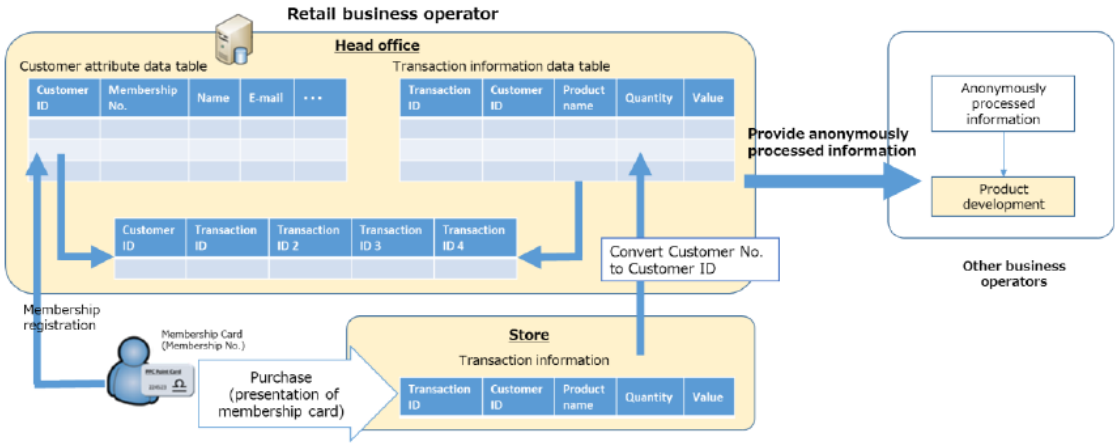

Рис. 3. Алгоритм использования обезличенной информации.

Банковская тайна. В Японии на законодательном уровне обязательство банков по сохранению конфиденциальности информации клиентов не закреплено, равно как не закреплено понятие и содержание банковской тайны[379]. Тем не менее, фактически такое обязательство за банками признается, что подтверждается судебной практикой и положениями некоторых законов (например, Закона о персональной информации, Законом о банковской деятельности). Впервые обязанность банков по сохранению конфиденциальности информации была подтверждена решением Верховного суда Японии[380] (подробнее см. в подборке репрезентативной судебной практики).

Поскольку круг сведений, которые составляют банковскую тайну, в Законодательстве не определен, суды в каждом конкретном деле оценивают, относятся те или иные сведения к

[379] Banking Regulation 2018 Japan [Electronic resource] // Global Legal Insights [Site]. – URL: https://www.globallegalinsights.com/practice-areas/banking-and-finance-laws-and-regulations/japan (accessed: 25.07.2018).

[380] Case number 2007(Kyo) 23 dated 11 Dec. 2007 [Electronic resource] // Supreme Court of Japan [Site]. - URL: http://www.courts.go.jp/app/hanrei_en/search (accessed: 08.08.2018).

банковской тайне и были ли законные основания для разглашения[381]. Так, Верховный суд Японии относил следующие сведения к конфиденциальной информации: сведения о транзакциях клиента[382]; внутренний документ банка, на основании которого банк принимает решение о выдаче кредита (такой документ содержит идентифицирующую информацию заемщика, размер кредита, процентную ставку по нему, цели использования кредита, сведения о гарантийном обязательстве, финансовом состоянии клиента иные подобные сведения)[383], результат аналитической деятельности банка по оценке финансового состояния клиента и прогнозам на будущее[384].Верховный суд Японии не признавал конфиденциальными такие внутренние документы банка, которые не содержат информации о клиентах[385].

В отличие от других видов тайн, специальной ответственности за нарушение банковской тайны Законодательством не предусмотрено. В этой связи единственной мерой ответственности является возмещение убытков в соответствии с ГК Японии. Также банк/сотрудник банка может быть привлечен к ответственности в соответствии с Законом Японии о персональной информации (см. выше).

Сведения, составляющие банковскую тайну, могут быть предоставлены третьим лицам[386]:

(1) **На основании согласия клиента.** Такое согласие может быть в устной, письменной или иной форме. При этом в отношении клиентов юридических лиц действует т.н. принцип opt-out, согласно которому согласие считается полученным, если банк проинформировал клиента о предоставлении информации третьим лицам и предоставил клиенту возможность отказаться от раскрытия..

Положения Агентства по финансам (the Financial Services Agency of Japan) «О защите персональной информации в финансовом секторе» (Guidelines for Personal Information

[381] Booysen S., Neo D. Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres Around the World. - Cambridge University Press, 2017. – PP. 252-278

[382] Case number: 2006 (Kyo) 21 dated 27 Oct. 2006 [Electronic resource] // Supreme Court of Japan [Site]. – URL: http://www.courts.go.jp/app/hanrei_en/search (accessed: 08.08.2018).

[383] Case number 1999 (Kyo) 2 dated 12 Nov. 1999 [Electronic resource] // Supreme Court of Japan [Site]. – URL: http://www.courts.go.jp/app/hanrei_en/detail?id=459 (accessed: 08.08.2018).

[384] Case number: 2008 (Kyo) 18 dated 25 Nov. 2008 [Electronic resource] // Supreme Court of Japan [Site]. – URL: http://www.courts.go.jp/app/hanrei_en/search (accessed: 08.08.2018).

[385] Supreme Court of Japan [Electronic resource] // Supreme Court of Japan [Site]. – URL: http://www.courts.go.jp/app/hanrei_en/detail?id=34 (accessed: 08.08.2018).

[386] Booysen S., Neo D. Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres Around the World. - Cambridge University Press, 2017. – PP. 252-278

Protection in the Financial Filed)[387] предусматривают детальные правила предоставления банковской тайны, относящейся к физическим лица. Такие требования относятся к следующему:

- **Форме согласия.** Согласие предпочтительно получать в форме документа (в том числе электронного). При этом, если для целей получения согласия используется форма документа/шаблон или иной заранее заготовленный документ, оператор должен убедиться в том, что субъекту персональной информации понятны содержание и условия согласия (такие условия должны быть четко отделены от иных условий и т.д.). Либо желательно получать согласие в форме документа, на основании которого можно установить намерение клиента предоставить согласие (в качестве примера приводится документ с полями для метки). При этом согласие должно включать следующее: названия третьих лиц, которым предоставляются сведения, цели использования сведений третьими лицами, состав передаваемых сведений.
- **Администрированию согласий на предоставление сведений кредитным организациям, входящим в группу лиц.** Суть требований заключается в том, что при предоставлении информации группе лиц субъект персональной информации, должен быть об этом проинформирован (посредством перечисления, сайтов таких лицом или иным образом).
- **Совместному использованию.** Как было предусмотрено ранее, Закон о персональной информации разрешает т.н. совместное использование персональной информации в определенных случаях. Такие «сопользователи» третьими лицами не признаются и в отношении них не требуется получение согласий. Тем не менее, Положения Агентства по финансам расширяют требование Закона о персональной информации, о том, что такое совместное использование заранее должно быть очевидно для субъекта. В частности, Положения предусматривают обязательство о письменном уведомлении клиента о совместном использовании.

(2) В случаях, предусмотренных законом (включая случаи предоставления

[387] Legislation and Guidelines of the Financial Services Agency [Electronic resource] // Financial Services Agency [Site]. – URL: https://www.fsa.go.jp/en/refer/legislation/index.html (accessed: 08.08.2018).

персональной информации, которые предусмотрены выше). Как правило, это изъятия из банковской тайны, предусмотренные для целей уголовного, гражданского судопроизводства и иных подобных целей (предоставление отчетов Агентству по финансам, налоговым органам)[388].

(3) Для защиты банком своих собственных интересов. Однако оснвоания и пределы пределы предрставленяи информации в Законодательстве прямо не определены.

Сведения, составляющие банковскую тайну и персональную информацию пересекаются в части информации, относящейся к клиентам банка- физическим лицам.

Некоторые требования информационной безопасности в отношении банков

Законодательство и подзаконные акты Японии содержат довольно жесткие требования относительно обеспечения банками безопасности обрабатываемой информации. В частности, основные требования содержатся в следующих НПА:

- Приказ о введении в действие Закона о о банках (The Ordinance for Enforcement of the Banking Act[389]), согласно которому банки обязаны предпринимать разумные меры для недопущения утечки информации, разумные меры для надлежащей обработки персональной информации при делегировании обработки персональной информации работников или клиентов третьим лицам и т.д. (ст. 13-6-4 Приказа)
- Положения Агентства по финансовой службе для банков (Comprehensive Guidelines for Supervision of Major Banks).[390]
- Закон о финансовых организациях и финансовом обмене (Financial Instruments and Exchange Act dated June 14, 2006[391])
- В иных профильных НПА;
- Также банки ориентируются на требования, предъявляемые законодательством о защите персональной информации. Например, некоторые положения содержатся в Положении Агентства по финансам (ст. 10).

[388] Booysen S., Neo D. Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres Around the World. - Cambridge University Press, 2017. – 432 P.

[389] The Ordinance of the Ministry of Finance No. 10 of March 31, 1982 for Enforcement of the Banking Act. [Electronic resource] // Japanese Law Translation [Site]. – URL: http://www.japaneselawtranslation.go.jp/law/detail/?id=2691&vm=04&re=02 (accessed: 08.08.2018).

[390] Comprehensive Guidelines for Supervision of Major Banks [Electronic resource]: Financial Services Agency [Site]. – URL: https://www.fsa.go.jp/common/law/guide/gaigin.pdf. (accessed: 08.08.2018).

[391] Financial Instruments and Exchange Act dated June 14, 2006 [Electronic resource]: Financial Services Agency [Site]. – URL: https://www.fsa.go.jp/common/law/guide/gaigin.pdf (accessed: 08.08.2018).

Налоговая тайна. Впервые концепция налоговой прозрачности и открытости появилась в Японском законодательстве в 2010 году. Принятый закон был направлен на упрощение налоговых правил и привлечение нарушителей к ответственности.

Соблюдение налоговой тайны в Японии гарантируется главой 38 Конституции. Причем соблюдение налоговой тайны обязательно для всех, государственных лиц и налоговых инспекторов, поскольку налоговая тайна должна быть сохранена, даже если во время проверки были обнаружены налоговые нарушения.

Так, в 2014 году во время выборов мэра города Яхио-Сити действующий мэр намеренно распространил информацию о налоговых нарушениях своего оппонента. За нарушение налоговой тайны действующему мэру было предъявлено обвинение и назначен домашний арест.

До сегодняшнего дня случаев похищения конфиденциальных налоговых сведений из единого хранилища данных зафиксировано не было. Однако в случае если налоговая тайна будет нарушена, потерпевший может обратиться в Комиссию по защите персональных данных. Если тайна была нарушена должностным лицом, потерпевший может подать иск для возмещения причиненного ущерба.

Что касается трансграничных случаев нарушения налоговой тайны, то в судебных инстанциях США был рассмотрен гражданский иск о возмещении убытков, который включал утечку неправильной информации, предоставленной должностным лицом налоговой службы Японии.

Иные виды тайн

По своему характеру коммерческая тайна существенно отличается от таких видов тайн как, тайна связи, тайна личной жизни, банковская тайна, налоговая тайна. Главным образом, тем, что в ней отсутствует публично-правовой элемент: режим коммерческой тайны, как правило, устанавливается лицами, осуществляющими предпринимательскую деятельность, в отношении сведений, представляющих для них коммерческую ценность. А право следует из закона и обеспечивается принудительной силой государства.

Как следствие, вопросы Технического задания, относящиеся к порядку предоставления третьим лицам сведений, получению согласия у третьих лиц на распространение сведений, составляющих соответствующий вид тайны, во многом неприменимы к сведениям, в отношении которых установлен режим коммерческой тайны.

В Японии, в отличие от России, коммерческая тайна не регулируется как правовой

режим». При этом охраняются и признаются секреты производства (ноу хау), которые являются объектами.

Секрет производства определяется как бизнес или техническая информация, имеющая ценность для коммерческой деятельности, такой как производственная деятельность, определение маркетинговых стратегий, в отношении которой сохраняется конфиденциальность и которая не является общеизвестной (ст.4 Закона Японии о предотвращении недобросовестной конкуренции, Unfair Competition Prevention Act[392]).

В 2016 г. Закона Японии о предотвращении недобросовестной конкуренции были внесены существенные изменения в части ужесточения ответственности за нарушение прав на секреты производства393.

За нарушение прав на секреты производства предусмотрена уголовная и гражданская ответственность, в том числе:

(1) Уголовная ответственность в виде лишения свободы на срок до 10 лет и выплаты штрафа в размере до 10 000 000 йен (примерно 5 600 000 рублей), ст. 21 Закона Японии о предотвращении недобросовестной конкуренции.

(2) Гражданская ответственность в виде возмещения убытков (ст. 4) Закона Японии о предотвращении недобросовестной конкуренции.

Также доступны такие меры как уничтожение контрафактной продукции и .т.д

Использование конфиденциальной информации государственными органами

Как было отмечено выше, в Японии существует отдельное регулирование в отношении использования персональной информации государственными органами и иными публично-правовыми образованиями. В частности, использование регулируется Законом о защите персональной информации, обрабатываемой государственными органами (Закон №58), Законом о защите персональной информации, обрабатываемой государственными агентствами (Закон №59) и Законом о доступе к информации государственных органов (Закон №42), совместно именуемые в настоящем разделе «Законы».

Впервые возможность доступа к документам государственных органов была закреплена в Японии с принятием Закона о доступе к информации, обрабатываемой

[392] Unfair Competition Prevention Act [Electronic resource]: Japanese Law Translation [Site]. – URL: http://www.japaneselawtranslation.go.jp/law/detail_main?id=83&vm=2&re= (accessed: 08.08.2018).

[393] David Case. “We’re Not Gonna Take It!” Significant Changes to Japan’s Trade Secret Protection Law [Electronic resource] // Orrick Blogs [Site]. – URL: https://blogs.orrick.com/trade-secrets-watch/2016/04/18/were-not-gonna-take-it-significant-changes-to-japans-trade-secret-protection-law/ (accessed: 08.08.2018).

государственными органами и Закона о доступе к информации, обрабатываемой государственными агентствами . История принятию данных законов растянулась на несколько десятков лет. В частности, принятию этих законов предшествовало большое количество дискуссией, инициатив и т.д., начиная с 1970-х годов.

Впоследствии был принят Закон № 58, который направлен на защиту персональной информации, содержащуюся в документах, государственных органов.

Ниже приводятся ключевые положения, регулирующие порядок использования и доступа к персональной информации, которая обрабатывается государственными органами.

1. Сфера распространения Закона №58

Закон № 58 регулируют порядок использования персональной информации, то есть информации, которая относится к живому физическому лицу и позволяет определить конкретное лицо по имени, дате рождения, иным параметрам (в том числе информация, которая позволяет идентифицировать лицо на основании соотнесения с другой информацией) в составе т.н административных документов, «Обрабатываемая персональная информация» (Retained personal information) (ст. 2 Закона №58).

Под административным документом понимается документ, изображение или электронная запись, которые были подготовлены или получены работниками государственных органов в процессе исполнения своих должностных обязанностей, за исключение документов (таких как официальные газеты, журналы, книги), предназначенных для массовой продажи/распространения, или отнесенные Кабинетом министров Японии к историческим или культурным ценностям (ст. 1 Закона №42).

Ограничения и условия использования

(1) В отношении обработки и использования государственными органами персональной информации установлены следующие ограничения (ст. 3 Закона №58):

- По общему правилу, государственный орган должен обрабатывать персональную информацию только для целей исполнения должностных обязанностей, которые на него возложены;
- Государственный орган обязан определить цели использования персональной информации и использовать персональную информацию в соответствии с такими целями;
- Государственный орган не может произвольно менять цели использования, так чтобы цель использования существенно отличалась от изначально завяленной.

(2) Государственный орган обязан заранее уведомить субъекта персональной информации о целях использования его персональной информации за исключением некоторых случаев, прямо предусмотренных в законе (ст. 4 Закона №58).

(3) В случае, если государственный орган намеревается использовать персональную информацию в виде Информационного файла – систематизированной базы данных, содержащей персональную информацию, в которой поиск может осуществляться с помощью ЭВМ или с использованием отдельных идентифицирующих сведений, он должен сообщить об этом Министерству внутренних дел Японии (ст. 10 Закона №58).

2. Условия и порядок предоставления третьим лицам по Закону № 58

(1) По общему правилу, государственный орган может использовать сам или предоставлять третьим лицам Обрабатываемую персональную информацию только для определенных им заранее целей использования, если иное не предусмотрено законодательством.

(2) Закон № 58 предусматривает ряд исключений из данного правила, в том числе следующие исключения:

- Получено согласие субъекта персональной информации;
- Обрабатываемая персональная информация предоставляется другим государственным органам, государственным агентствам, публично-правовым образованиям при условия использования полученной информации исключительно для целей исполнения полномочий и обязанностей таких субъектов, которые определены в законодательстве и иных НПА;
- Для статистических целей или целей научного исследования и в иных специальных целях (ст. 8 Закона № 58).

(3) Закон № 58 подробно прописывает процедуру и порядок получения доступа к Обрабатываемой персональной информации субъектом такой персональной информации или законным представителем (глава 4 Закона № 58).

Закон № 58 определяет перечень информации, которая не подлежит раскрытию, т.н. «Non-disclosure information». Среди такой информации:

- Информация, которая содержит персональную информацию третьих лиц (за исключением информации, которая относится к предпринимательской деятельности лица, осуществляющего такую предпринимательскую деятельность);

- Информация, которая содержит информацию о юридическом лице (бизнесе) третьего лица, за исключением различных организаций с государственным участием;
- Информация, раскрытие которой может нанести вред национальной безопасности или международным отношениям с иностранным государством;
- Информация, раскрытие которой может нанести вред расследованию преступлений,
- Иная информация (полный перечень исключений предусмотрен ст. 14 Закона № 58).

(4) Закон не содержит норм, которые прямо регулируют условия и порядок трансграничной передачи Обрабатываемой персональной информации.

3. Некоторые положения Законов № 42 и № 57 относительно порядка предоставления административных документов государственных органов и организаций

(1) В отличие от Закона № 58, который определяет порядок предоставления персональной информации самим субъектам персональной информации, Законы № 42 и № 58 предусматривает возможность запроса соответствующих документов любыми заинтересованными лицами (ст. 3 Закона № 42 и ст. 3 Закона № 58).

(2) Законы определяют такие документы, которые не подлежат предоставлению. В целом, исключения, предусмотренные данными законами, совпадают с теми, что предусмотрены Законом о защите персональной информации (ст. 5 Закона № 42 и ст. 5 Закона № 57).

4. Юридическая ответственность за нарушение условий обработки персональной информации

(1) За незаконное предоставление третьему лицу Информационного файла (содержащего персональную информацию) работник государственного органа несет ответственность в виде лишения свободы на срок до двух лет или штрафа в размере до 1 000 000 йен (примерно 560 000 рублей), ст. 54 Закона № 58.

(2) За незаконное предоставление Обрабатываемой персональной информации или сбор персональной информации в превышение своих полномочий, работник государственного органа несет ответственность лишения свободы на срок до одного года или штрафа в размере до 500 000 йен (примерно 230 000 рублей), ст. 54 Закона № 58.

(3) Интересно, что дополнительно предусмотрена ответственность в отношении

лиц, которые обманным путем получают Обрабатываемую персональную информацию (ст. 57 Закона № 58.).

5. Опубликование информации государственных органов в форме открытых данных

Законы не содержат положений, которые бы предусматривали обязанность или порядок опубликования информации государственных органов в форме открытых данных.

Однако фактически в Японии многие сведения государственных органов опубликованы в форме открытых данных, что согласуется со Стратегией открытого правительства (Open Government Data Strategy[394]) , принятой в 2012 г.

Начиная с 2013 г. планы и программы специального структурного элемента, отвечающего за цифровое развитие Японии, предусматривают необходимость раскрытия информации государственных органов в форме открытых данных.

Министерство внутренних дел и связи Японии как министерство, ответственное за развитие информационного общества предпринимает определенные меры для опубликования государственными органами сведений в форме открытых данных (в том числе при его поддержке создан портал открытых данных), предусматривает какие именно сведения можно считать открытыми данными[395], функционирует портал открытытх данных Японии (http://www.data.go.jp/?lang=english).

Тем не менее, на законодательном уровне не урегулирован порядок и случаи раскрытия открытых данных.

Специфика юрисдикции Японии в свете целей и задач исследования раскрывается в ***репрезентативной судебной практике***.

Тайна связи.

Решение Верховного суда Японии № 2003 (A) 1796. Дата: 19.04.2004. (Keishu Vol. 58, No. 4). Лицо приобрело кассету с записью телефонного разговора двух других лиц, затем перезаписало эту запись на другую кассету и проигрывало его в присутствии третьих лиц, которые могли слышать существо разговора. За эти действия лицо было привлечено к ответственности за разглашение тайны связи в соответствии со ст. 104 Закона о

[394]Open Government Data Strategy [Electronic resource] // Prime Minister of Japan and His Cabinet [Site]. – URL: https://japan.kantei.go.jp/policy/it/20120704/text.pdf (accessed: 08. 08.2018).

[395] Promotion of Open Data Strategies [Electronic resource]: Ministry of Internal Affairs and Communications [Site]. – URL: http://www.soumu.go.jp/menu_seisaku/ictseisaku/ictriyou/opendata/eng/index_e.html (accessed: 08.08.2018).

телекоммуникационном бизнесе. Лицо, привлеченное к ответственности, обжаловало решения нижестоящих судов в Верховный суд Японии.

Верховный суд Японии оставил решения нижестоящих судов в силе. По мнению Верховного суда Японии, обязанность по сохранению тайны связи распространяется на любых лиц, вне зависимости от того, причастны ли они к записи телефонных разговоров и сообщений.

Решение Верховного суда Японии № 1999 (A) 96. Дата: 2000.07.12. (Keishu Vol.54, No.6, at 513). Лицо, привлеченное к уголовной ответственности, обжаловало использование записи телефонного разговора, сделанное потерпевшим без его согласия, как использование недопустимого доказательства.

Верховный суд решил, что для защиты прав и законных интересов правомерно делать запись телефонного разговора без ведома второй стороны и использовать такую запись в рамках судебного разбирательства.

Решение Верховного суда Японии № 2009 (Ju) 609 от 13.04. 2010. (Minshu Vol. 64, No. 3). Лицо, имеющее статус специального посредника в соответствии с Законом Японии об ограничении ответственности посредников, обжаловало в Верховный суд решения судов нижестоящих инстанций о привлечении к ответственности за отказ от предоставления идентификационных сведений пользователя услуг.

Верховный суд Японии вынес решение в пользу посредника на основании следующего:

(1) Предоставление сведений о пользователе Интернет услуг является ограничением его прав на тайну личной жизни, тайну связи, свободу выражений. В этой связи такая информация не может раскрываться третьим лицам без достаточных оснований: «*The identification information of the sender is information that is concerned with the sender's privacy, freedom of expression, and secrecy of communication and should not be disclosed to any third party without justifiable grounds, and if such information is disclosed, it would be impossible to recover the original state prior to the disclosure.*»

(2) В этой связи Закон Японии об ограничении ответственности посредников предусматривает строгие условия предоставления такой информации, одним из которых является нарушение прав и интересов лица, запрашивающего информацию. В рассматриваемом случае сообщение пользователя содержало

оценочное суждение «сумасшедший», которое, хотя и являясь оскорбительным, прав истца не нарушает.

Решение Окружного Токийского суда (47 гражданское отделение) от 21.03. 2013 по делу № 2012 (Wa) 16391. Лицо, которое посчитало, что его авторские права были нарушены передачей через Интернет и опубликованием в Интернете статьи, потребовало раскрытия идентификационных данных пользователя телекоммуникационных услуг.

Суд обязал посредника раскрыть соответствующие сведения в соответствии со ст. 4 Закона Японии об ограничении ответственности посредников.

Банковская тайна.

Решение Верховного суда Японии № 2007 (Kyo) 23 от 11.12.2007. (Minshu Vol. 61, No. 9). Это прецедентное дело, в рамах которого Верховный суд Японии подтвердил, что финансовые организации имеют обязательства по сохранению конфиденциальной информации клиента. Дело имеют особую значимость в связи с тем, что Законодательство Японии прямо такое обязательство не предусматривает. Для того чтобы установить неосновательное обогащение клиента финансовой организации, лица обратились в финансовую организацию с требованием о предоставлении сведений о движении денежных средств на счете.

Финансовая организация отказалась выдавать такие сведения, сославшись на то, что такие сведения составляют профессиональную тайну в соответствии с ГПК Японии (ст. 220 (4(c)), ст. 1973(1)).

Суд первой инстанции решил, что запрашиваемые сведения к профессиональной тайне не относятся. Суд второй инстанции с судом первой инстанции не согласился, отметив, что финансовая организация связана обязательством по сохранению конфиденциальности сведений своего клиента: «*Financial institutions maintain the relationships of mutual trust with their customers and carry out their operations smoothly by keeping secret the contents of the transactions with their customers and other information on their customers that they have learned in relation to such transactions…. In this case, it is obvious that the Records, which can clarify the full particulars of the transactions with B, are a document stating professional secrets* ». Также суд второй инстанции посчитал, что раскрытие сведений возможно для целей судебного разбирательства, если без такого раскрытия установление обстоятельств по делу невозможно. В рассматриваемом случае суд не нашел достаточных оснований для раскрытия.

Согласившись с судом второй инстанции в том, что финансовая организация связана

обязательством конфиденциальности пред клиентом, Верховный суд Японии нашел основания для раскрытия информации в конкретном деле. В частности, если запрашивается информация, которую сам клиент должен был бы представить в рамках судебного разбирательства, то финансовая организация вправе ее представить. Также Верховный суд отметил, что у финансовой организации нет собственного интереса в неразглашении соответствующей информации в соответствии с названными выше положениями ГПК Японии.

Решение Верховного суда Японии № 2008 (Kyo) 18 от 25.11.2008. (Minshu Vol. 62, No. 10). В рамках гражданского процесса контрагенты компании обратились в банк, который обслуживает компанию, с запросом выдать информацию о финансовом состоянии компании. Банк отказался выдать информацию на основании ст. 220 ГПК Японии, которая разрешает не предоставлять информацию, являющуюся профессиональной тайной или информацией, в отношении которой сохраняется обязательство по конфиденциальности.

Суд второй инстанции разделил запрашиваемую информацию на следующие виды: (1) финансовая информация, отраженная в финансовой отчетности, такой как отчёт о прибылях и убытках и т.д., (2) конфиденциальная финансовая информация, предоставленная клиентом на условиях конфиденциальности; (3) информация о кредитоспособности клиента, полученная у стороннего агентства; (4) результаты оценки финансового и коммерческого состояния клиента, прогнозы будущего финансового состояния клиента, которые были сделаны самим банком на основании имеющейся информации;

Суд второй инстанции обязал банк раскрыть информацию, за исключением той, которая относится к пункту 3 и части информации из пунктов 2 и 4, которая относится не только к клиенту, но и к третьим лица, таким как партнеры банка.

Банк обжаловал решение в Верховный суд Японии.

Верховный суд отказал банку, хотя и признал, что информация, указанная в пункте 4, относится к профессиональной тайне банка, который сам получил эту информацию. По мнению Верховного суда, вопрос о раскрытии информации, которая составляет профессиональную тайну (в данном случае банковскую) должен решаться на основании оценки баланса интересов: необходимо соизмерить ущерб от раскрытия такой информации с ущербом от сохранения конфиденциальности. «*Even where the document requested by an order to submit a document contains any information that can be regarded as professional secrets, the holder of the document is allowed to refuse when the professional secrets contained in the requested*

document are worthy of protection, and this should be determined by balancing various factors … on one hand, the content and nature of the information, what disadvantage the holder of the information might suffer from its disclosure and the extent of such disadvantage, and on the other hand, the content and nature of the civil case in which the information is requested, and the extent to which the document is needed as evidence in the case».

Медицинская тайна.

Решение Верховного суда Японии № 2010 (A) 126 от 2012.02.13. (Keishu Vol. 66, No. 2). Психиатр, который раскрыл информацию о пациенте и его родителях, ставшую ему известной в ходе проведения экспертизы, был привлечён к ответственности в соответствии со ст. 134 УК Японии.

В данном деле Верховный суд Японии пришел к выводу о том, что лицо, которое проводило медицинскую экспертизу, обязано сохранять конфиденциальность как информации лица, в отношении которого проводится экспертиза, так и в отношении третьих лиц, информация о которых стала ему известна в ходе поведения экспертизы.

2. АНАЛИЗ ДЕЙСТВУЮЩИХ МЕЖДУНАРОДНЫХ ДОГОВОРОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

Основополагающим международным договором, гарантирующим охрану тайны личной жизни, тайны корреспонденции, является **Всеобщая декларация прав человека** (принята Генеральной Ассамблеей ООН 10.12.1948). Данная декларация содержит базовые положения о неприкосновенности личной жизни, на которых в дальнейшем базируются все последующие положения международных договоров, обеспечивающих охрану личной информации о лице. Статья 17 декларации устанавливает положение, в соответствии с которым никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательством на корреспонденцию лица, а также право каждого лица на защиту на основании закона от таких вмешательств. Декларация не содержит как такового понятия " тайна личной жизни", тем не менее, декларирует необходимость предоставления защиты личной информации о лице и его корреспонденции.

Развитие принципа охраны тайны личной жизни произошло с принятием **"Международного пакта о гражданских и политических правах"** (1966) в его статье 17, которая, по сути , повторила статью Всеобщей декларации прав человека. В своём замечании

общего порядка 27 Комитет по правам человека, комментируя норму о возможных ограничениях права в целях общественной безопасности, охраны общественного порядка , отметил, что ограничение права должно не только служить достижению разрешённых целей, но и быть необходимыми для такой защиты и наименее ограничительными из числа возможных. Данные комментарии применимы и к вопросам ограничения права на тайну личной жизни. К положениям статьи 17 приняты также замечания общего порядка #16, где отмечено, что данные положения требуют от государств принятия законодательных и иных мер для запрещения произвольного вмешательства в личную и семейную жизнь человека.

Отраслевые международные договоры Российской Федерации, регулирующие трансграничную передачу информацию (например, при отправке постовых отправлений) предусматривают общую обязанность субъектов, в чье распоряжение попадают персональные данные, сохранять конфиденциальность таких данных.

"Всемирная почтовая конвенция" (Заключена в г. Дохе 11.10.2012, в России утверждена распоряжением Правительства РФ от 15.01.2014 N 16-р, вступила в действие в России в 2014 году). Данная Конвенция была разработана и принята в рамках деятельности Всемирного почтового союза как унификационный акт в целях развития связи между народами посредством эффективного функционирования почтовых служб и содействия достижению целей международного сотрудничества. Статья 12 данного акта посвящена вопросам, связанным с обработкой персональных данных клиентов. Данная статья предусматривает обязанность стран-членов и их назначенных операторов обеспечивать конфиденциальность и защиту персональных данных клиентов, соблюдая своё национальное законодательство. Назначенные операторы должны информировать своих клиентов об использовании их персональных данных и о конечной цели их использования.

"Устав Международного союза электросвязи " в статье 37 устанавливает, что члены Союза обязуются принимать все законные меры, совместные с применяемой системой электросвязи, с целью сохранения тайны международных сообщений. Однако сохраняется право передавать такие сообщения уполномоченным государственным органам, чтобы обеспечить соблюдение внутреннего законодательства или выполнение международных соглашений, участником которых они являются.

Коммерческая тайна охраняется, в первую очередь, положениями **соглашений ТРИПС.** В соответствии с Соглашениями ТРИПС, охрана коммерческой тайны понимается как защита информации , которая на законных основаниях контролируется юридическим или

физическим лицом и которая:

(А) Является секретной, поскольку в целом, либо в конкретном сочетании или расположении её компонентов не является известной или легко доступной лицам, принадлежащим определённому кругу, обычно имеющему дело с подобным видом информации;

(Б) имеет коммерческую ценность ;

(В) в конкретных обстоятельствах была подвергнута определённым мерам охраны лицом, контролирующим эту информацию на законных основаниях, в целях сохранения её секретности.

Положения о раскрытии тайны личной жизни, тайны переписки содержатся также в договорах о правовой помощи, которые регулируют порядок раскрытиях информации правоохранительным органам иностранного государства, раскрытие информации для целей судебного производства в иностранном государстве.

Налоговая тайна.

(1) С 1 июля 2015 года в РФ вступила в силу “Конвенция о взаимной административной помощи по налоговым делам” (Заключена в г. Страсбурге 25.01.1988) на основании закона от 04.11.2014 N 325-ФЗ "О ратификации Конвенции о взаимной административной помощи по налоговым делам".

Конвенция распространяется на Государства-члены Совета Европы и страны-члены Организации экономического сотрудничества и развития (ОЭСР), подписавшие Конвенцию (Преамбула).

Стороны обмениваются любой информацией, в частности в соответствии с положениями настоящего раздела, которая предположительно является важной для администрирования или обеспечения соблюдения законодательства в отношении налогов, на которые распространяется настоящая Конвенция (ч. 1 ст. 4 Конвенции).

Выделяется три типа обмена информацией – по запросу (ст. 5 Конвенции), автоматический (ст. 6 Конвенции), инициативный (ст. 7 Конвенции).

В зависимости от категорий дел и в соответствии с процедурами, которые определяются по взаимной договоренности, две или более Стороны автоматически обмениваются информацией, указанной в статье 4. (ст. 6 Конвенции).

Реализация на практике Многостороннего соглашения об автоматическом обмене

финансовой информацией (Multilateral Competent Authority Agreement) означает, что автоматический обмен налоговой информацией будет осуществляться на основе разработанного ОЭСР стандарта автоматического обмена информацией о финансовых счетах (Common reporting standard, CRS), которым установлены содержательные и технические детали процесса обмена информацией (Письма Минфина России от 07.04.2016 N 03-08-05/19761, от 02.03.2016 N 03-08-05/11875). В рамках международного обмена информацией финансовые институты всех стран-участниц собирают соответствующие сведения о своих клиентах (ФЛ и ЮЛ) и передают их в налоговые органы своей страны. Затем происходит обмен информации между налоговыми органами стран-участниц.

Федеральным законом от 27.11.2017 N 340-ФЗ «О внесении изменений в часть первую Налогового кодекса Российской Федерации в связи с реализацией международного автоматического обмена информацией и документацией по международным группам компаний» были приняты изменения, в частности, п.п. 4 п. 1 ст. 102 НК РФ был дополнен словами «в том числе в рамках международного автоматического обмена информацией», часть 1 НК РФ была дополнена разделом VII.1 – «Выполнение международных договоров Российской Федерации по вопросам налогообложения и взаимной административной помощи по налоговым делам». Предоставляемые налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями) сведения (также и в рамках автоматического обмена) не подпадают под режим налоговой тайны (п.п. 4 п. 1 ст. 102 НК РФ).

21 декабря 2017 года на сайте Организации экономического сотрудничества и развития (ОЭСР) появилась информация о юрисдикциях, которые готовы в автоматическом режиме предоставлять РФ информацию в отношении финансовых счетов компаний и физических лиц – налоговых резидентов РФ. На текущий момент (26 июля 2018) из России налоговая информацией будет в автоматическом режиме отправляться в 59 стран, а в Россию - из 82 стран[396].

Следующая информация будет передаваться в автоматическом режиме (часть 5

[396] The Automatic Exchange of Information (AEOI) portal [Electronic resource] // The Automatic Exchange of Information (AEOI) portal [Site]. – URL: http://www.oecd.org/tax/automatic-exchange/international-framework-for-the-crs/exchange-relationships/ (accessed: 30.07.2018).

CRS (Chapter 5: The information that gets reported and exchanged)):

- данные банка, где открыт счет;
- номер счета;
- баланс счета;
- отчетный период;
- данные о клиенте банка, для ФЛ - код страны, ИНН, ФИО, дата рождения, адрес проживания;
- данные о клиенте банка, для ЮЛ - код страны, ИНН, наименование, регистрационный адрес;
- данные о контролирующем лице компании (код страны, ИНН, ФИО, дата рождения, адрес проживания);
- поступления за отчетный период и остаток на счете на конец отчетного периода.

(2) Кроме вышеуказанного международного договора, существуют также двусторонние договоры с отдельными странами, также предполагающие обмен информацией (но не автоматический), например:

a. Соглашение между Правительством РФ и Правительством Демократической Социалистической Республики Шри-Ланка от 02.03.1999 «Об избежании двойного налогообложения и предотвращении уклонения от налогообложения в отношении налогов на доходы»;
b. Конвенция между Правительством РФ и Правительством Республики Филиппины от 26.04.1995 «Об избежании двойного налогообложения и предотвращении уклонения от налогообложения в отношении налогов на доходы»;
c. Соглашение между Правительством Российской Федерации и Правительством Турецкой Республики об избежании двойного налогообложения в отношении налогов на доходы (Заключено в г. Анкаре 15.12.1997);
d. иные.

3. АНАЛИЗ УТВЕРЖДЕННОЙ И РАЗРАБАТЫВАЕМОЙ ДОКУМЕНТАЦИИ МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЙ

3.1. Международный союз электросвязи (МСЭ)

МСЭ была создана в Женеве в 1865 году как международная организация, формулирующая рекомендации в сфере радио и телекоммуникаций и международное использование радиочастот. МСЭ является специализированным учреждением ООН в области информационно-коммуникационных технологий.

Рекомендации МСЭ не являются обязательными для исполнения (если только не приняты в рамках национального законодательства), однако широко признаются во всем мире. Всего в сфере стандартизации с момента своего основания МСЭ подготовлены более пяти тысяч рекомендаций. Ниже приведены несколько рекомендаций, касающихся защиты конфиденциальности данных и информационной безопасности.

Руководящие указания по защите информации, позволяющей установить личность, при применении технологии RFID. Рекомендация МСЭ-Т X.1275.[397] Рекомендация посвящена технологии RFID, которая позволяет получать информацию, относящуюся, в частности, к носимым технологиям, а также иным предметам. Данная технология влечет за собой риски, связанные с нарушением конфиденциальности данных или возможностью отслеживания местоположения человека. Рекомендация содержит положения, направленные на улучшение процедур защиты информации, позволяющей установить личность человека.

Информация, позволяющая установить личность человека – это информация, относящаяся к любому человеку, которая позволяет идентифицировать его личность (включая информацию, которая используется в сочетании с другой информацией, даже если эта информация не позволяет четко определить личность). Иными словами, это широкое понятие персональных данных.

Руководящие принципы основываются на принципах конфиденциальности, которые включают в себя следующие аспекты: ограничение в отношении сбора данных, качество данных, определение целей, ограничение в отношении использования, меры обеспечения безопасности, открытость, участие физических лиц и ответственность. В Рекомендации приведена таблица с возможными угрозами для информации, которая позволяет установить

[397] Руководящие указания Международного союза электросвязи по защите информации, позволяющей установить личность, при применении технологии RFID. X.1275. от 17.12.2010 [Электронный ресурс] // ITU [Сайт]. – URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=10441&lang=ru (дата обращения: 30.07.2018).

личность человека применительно к следующим областям: здравоохранение, электронное правительство, информационные услуги.

Обзор кибербезопасности. Рекомендация МСЭ-Т X.1205[398]**.** Рекомендация вводит понятие кибербезопасности, которое понимается как набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя. Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в киберсреде.

В Рекомендации описываются угрозы кибербезопасности и уязвимости с учетом разных уровней сетевой иерархии. В связи с этим в Рекомендации описываются технологии, позволяющие устранять указанные угрозы.

Информационные технологии. Методы безопасности. Кодекс практики для защиты информации, позволяющей установить личность.[399] В связи с увеличением количества обрабатываемой личной информации увеличиваются и ожидания в отношении защиты такой информации. В документе определены цели и меры контроля, руководящие принципы для его осуществления. Принципы основаны на ISO/IEC 27002 и могут применяться при построении системы информационной безопасности в организации.

Угрозы и требования к защите информации, позволяющей установить личность, в приложениях, использующих идентификацию на основе маркеров. Рекомендация МСЭ-Т X.1171.[400] Распространение RFID-технологий может вызывать обеспокоенность в отношении возможного нарушения конфиденциальности. Такая обеспокоенность связана со способностью RFID-технологий осуществлять автоматический сбор и обработку данных, а

[398] Overview of cybersecurity [Electronic resource]: prepared by International Telecommunication Union ITU-T X.1205 dated of 18.04.2008 // ITU [Site]. – URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136 (accessed: 30.07.2018).

[399] Information technology - Security techniques - Code of practice for personally identifiable information protection [Electronic resource]: prepared by International Telecommunication Union ITU-T X.1058 dated of 30.03.2017 // ITU [Site]. – URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13182&lang=en (accessed: 30.07.2018).

[400] Threats and requirements for protection of personally identifiable information in applications using tag-based identification [Electronic resource]: Prepared by International Telecommunication Union ITU-T X.1171 dated of 20.02.2009 // ITU [Site]. – URL : https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9454&lang=en (accessed: 30.07.2018).

также с возможностью раскрытия полученных данных неограниченному кругу лиц. В Рекомендации описываются угрозы и требования к защите информации, позволяющей установить личность в приложениях, использующих идентификацию на основе маркеров, то есть приложений, которые запускается маркером ID (включая RFID).

В частности, в п.10.4. Рекомендации указывается, что сервер подобных приложений должен поддерживать конфиденциальность данных и защищать данные от неавторизованных подключений. Кроме того, в п.10.5 отмечается, что сервер таких приложений должен поддерживать и процедуру получения согласия для сбора данных. При этом если собранная информация планируется к использованию в целях, отличных от ранее определенных целей, необходимо получить соответствующее согласие пользователя.

Руководящие указания по безопасности данных потребителей облачных услуг. Рекомендации МСЭ-Т X.1641.[401] Документ содержит общие рекомендации по обеспечению безопасности данных потребителя облачных услуг в среде облачных вычислений. При этом Руководящие указания касаются случаев, когда ответственность за обработку данных несет поставщик облачной услуги. В Рекомендациях определяются основные угрозы безопасности данных потребителя (например, несанкционированный доступ к данным, незащищенность данных при трансграничной передаче, отказы программного и аппаратного оборудования). Фактически рекомендации подразумевают собой выполнение принципа privacy by design, поскольку средства безопасности должны осуществляться уже на этапе создания и далее в течение всего жизненного цикла данных.

Глобальная программа по кибербезопасности (ГПК) МСЭ.[402] ГПК имеет своей целью предложение стратегии для поиска решений в области укрепления доверия и безопасности. Программа, как отмечается, будет основываться на национальных и региональных инициативах. В ГПК сформулированы несколько причин ее принятия, а именно: постоянно эволюционирующий характер киберугроз, в том числе, угроз конфиденциальности информации, ослабление барьеров и совершенствование технических способов совершения киберпреступлений, лазейки в существующих правовых системах,

[401] Guidelines for cloud service customer data security [Electronic resource]: Prepared by International Telecommunication Union ITU-T X.1641 dated of 07.09.2016 // ITU [Site]. – URL : https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12853&lang=en (accessed: 30.07.2018).

[402] Глобальная программа кибербезопасности (ГПК) МСЭ. Основа для международного сотрудничества в области кибербезопасности от 04.2008 [Электронный ресурс] // ITU [Сайт]. – URL: http://www.ifap.ru/pr/2008/080908aa.pdf (дата обращения: 30.07.2018); Кибербезопасность. Международный союз электросвязи [Электронный ресурс] // ITU [Site]. – URL : http://www.un.org/ru/ecosoc/itu/cybersecurity.shtml (дата обращения: 30.07.2018).

уязвимость программных приложений, отсутствие надлежащих организационных структур.

3.2. Ассоциация GSM (GSMA)

Ассоциация GSM (GSMA)[403] – торговая ассоциация, созданная в Лондоне в 1995 году, представляющая интересы операторов мобильной связи во всем мире. Одной из глобальных задач Ассоциации является обеспечение доступности мобильных телефонов и беспроводной связи по всему миру. Ассоциация отстаивает интересы операторов мобильной связи при решении разного рода проблем (как национальных, так и глобальных) в сфере развития сотовой связи. Документы, разрабатываемые Ассоциацией, носят технический характер (стандарты, рекомендации, спецификации) и не влияют на юридическое толкование действующего в данной сфере регулирования. Документы направлены на поддержку, развитие, разработку, унификацию решения разного рода проблем мобильной связи (обеспечение безопасности клиентских терминалов, вопросы, связанные с применением SIM-карт, вопросы роуминга и тарификации и т.д.).

Предложения GSMA, касающиеся кражи мобильных телефонов и безопасности IMEI (2003).[404] GSMA отметила, что международный идентификатор мобильного оборудования (IMEI) является ключевым элементом в дискуссии о кражах мобильных телефонов и торговли украденными мобильными телефонами. Именно IMEI может повысить эффективность борьбы с такими кражами.

На 2003 год большинство телефонов имели IMEI, как указывается в публикации. Согласно стандарту ETSI TS 122.016 «IMEI не должен изменяться после окончания производственного процесса мобильного телефона. IMEI должен предотвращать вмешательства, то есть изменения, любыми способами (например, физическим, программным, электрическим). Это требование действительно для нового типа GSME, утвержденного после 1 июня 2002 года. Производитель несет ответственность за подтверждение уникальности IMEI».

Поскольку стандарт является добровольным для исполнения, то не все производители мобильных телефонов имели защищенный IMEI. В связи с этим GSMA предложила

[403] GSMA [Electronic resource] – URL : http://www.gsma.com/ (accessed: 30.07.2018).

[404] GSME proposals regarding mobile theft and IMEI security dated of June 2003. [Electronic resource] // GSMA [Site]. – URL: https://www.gsma.com/gsmaeurope/wp-content/uploads/2012/03/gsme_proposals_mobile_thefts_imei_security.pdf (accessed: 30.07.2018).

формулировку пункта 3.3.d в Директиву ЕС о радиотехнике 2014/53/EU: «Оборудование для мобильных телекоммуникационных терминалов должно быть сконструировано таким образом, чтобы его использование после кражи можно было предотвратить. Оборудование должно иметь общедоступный идентификатор мобильного оборудования, который должен предотвращать несанкционированное вмешательство».

Отметим, что данная формулировка не была внесена в Директиву. Тем не менее, GSMA ведет единую глобальную базу «Международная база идентификаторов мобильных устройств» (IMEI DB), которая содержит основную информацию о серийных номерах (IMEI) миллионов мобильных устройств всего мира.

Защищенность, защита частной жизни и безопасность в мобильной экосистеме. Ключевые вопросы и практические выводы (2017).[405] С учетом роста экономической и социальной значимости Интернета в целом и мобильного интернета в частности, существует необходимость защиты потребителей таких услуг, обеспечения защиты и безопасности их использования. В своем отчете GSMA рассматривает основные проблемы защиты потребителей, частной жизни, общественной безопасности, а также выделяет потенциальные проблемы и шаги для их решения (как те, которые уже предпринимаются или могут быть предприняты в будущем).

Отчет включает в себя набор принципов, поддерживаемых участниками GSMA, связанных с защитой потребителей, защитой частной жизни потребителей (аспект персональных данных), публичной безопасности, сетевой безопасности и целостности устройства.

3.3. Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ)

Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ)[406] - межправительственный орган, созданный в 1989 г. по решению министров государств-членов. ФАТФ устанавливает стандарты и содействует эффективному применению правовых, регулирующих и оперативных мер по борьбе с отмыванием денег, финансированием терроризма и финансированием распространения оружия массового

[405] Safety, privacy and security across the mobile ecosystem. Key issues and policy implications. Prepared by GSMA 2017 [Electronic resource] // GSMA [Site]. – URL: https://www.gsma.com/publicpolicy/wp-content/uploads/2017/02/GSMA_Safety-privacy-and-security-across-the-mobile-ecosystem.pdf (accessed: 30.07.2018).

[406] FATF [Electronic resource] – URL: http://www.fatf-gafi.org/ (accessed: 30.07.2018).

уничтожения и иными связанными угрозами целостности международной финансовой системы.

Рекомендации ФАТФ. Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения (в редакции 2018 г.).[407] Согласно статье 9 раздела D «Превентивные меры» страны должны обеспечить отсутствие препятствий для реализации Рекомендаций ФАТФ со стороны законодательства о защите тайны финансовых учреждений.

В разделе 2 Рекомендаций предусматривается необходимость национального сотрудничества и координации. Так, должно быть обеспечено наличие эффективного механизма, позволяющего компетентным органам страны сотрудничать друг с другом, координировать свои действия (когда это необходимо) в отношении разработки и реализации политики и деятельности по борьбе с отмыванием денег, финансированием терроризма и финансированием распространения оружия массового поражения. В 2018 году в данный раздел были внесены дополнения о том, что такое сотрудничество и координация направлены, в том числе, на обеспечение совместимости AML/CFT требований с правилами по защите персональных данных и другими аналогичными положениями (например, в части защиты данных, локализации и т.д.).

Вопросам освобождения от ответственности за раскрытие информации и нарушение конфиденциальности посвящена ст.21 Рекомендаций.

Объединенное издание стандартов ФАТФ в сфере обмена информацией (2017).[408] Документ содержит собрание Рекомендаций ФАТФ, которые устанавливают требования к:

- типам информации, которую необходимо раскрывать, включая типы информации, которую компетентные органы должны размещать в открытом доступе
- обстоятельствам, в которых такая информация должна быть раскрыта, и
- мерам, обеспечивающим защиту и гарантии, применяемые к обмену информацией.

Положения касаются обмена информации на разных уровнях: внутри частного сектора, между частным сектором и публичным, и между уполномоченными органами (по их

[407] International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations (amended February 2018) [Electronic resource] // FATF [Site]. – URL : http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (accessed: 30.07.2018).

[408] Consolidated FATF Standards on Information Sharing. Relevant excerpts from the FATF Recommendations and Interpretive Notes. Prepared by FATF (updated November 2017) [Electronic resource] // FATF [Site]. – URL: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Consolidated-FATF-Standards-information-sharing.pdf (accessed: 30.07.2018).

видам). При этом, подразумевается как обмен информации внутри страны, так и трансграничный.

3.4. Организация экономического сотрудничества и развития (ОЭСР)

ОЭСР[409] – международная экономическая организация развитых стран, созданная в 1948 году в Париже. ОЭСР проводит широкую аналитическую работу (см. например, «Укрепление информационной инфраструктуры здравоохранения для управления качеством медицинского обслуживания» (2013)[410], или «Защита личных данных, размещенных онлайн» (2003)[411]). Помимо этого, ОЭСР вырабатывает рекомендации, в том числе, относящиеся к обработке персональных данных, включая их трансграничную передачу.

Изучение инноваций, основанных на данных, в качестве нового источника развития. Определение вопросов построения политики в связи с технологиями big data (2013).[412] Отчет посвящен потенциальной роли данных и их аналитики для создания конкурентных преимуществ и формирования капитала, основанного на знаниях, позволяющего стимулировать инновации и устойчивый рост экономики и общества. В Отчете описывается влияние big data на разные области – рекламу, здравоохранение, транспорт, коммунальное хозяйство и государственный сектор. В практических выводах Отчета первым аспектом, который должен быть обеспечен при использовании технологии big data, указывается защита частной жизни.

Отдельный раздел Отчета посвящен защите личной информации и защите потребителей. Так, появление большого числа товаров и сервисов, основанных на данных,

[409] OECD [Electronic resource] – URL: https://www.oecd.org/ (accessed: 30.07.2018).

[410] Strengthening Health Information Infrastructure for Health Care Quality Governance. Good Practices, New Opportunities and Data Privacy Protection Challenges. Prepared by OECD 2013 [Electronic resource] // OECD [Site]. – URL: https://www.oecd-ilibrary.org/social-issues-migration-health/strengthening-health-information-infrastructure-for-health-care-quality-governance/protection-of-privacy-in-the-collection-and-use-of-personal-health-data_9789264193505-9-en (accessed: 30.07.2018).

[411] Privacy Online. OECD Guidance on Policy and Practice. Prepared by OECD – 2003 [Electronic resource] // OECD [Site]. – URL: https://www.oecd-ilibrary.org/science-and-technology/privacy-online_9789264101630-en (accessed: 30.07.2018).

[412] Exploring Data-Driven Innovation as a New Source of Growth. Mapping the Policy Issues Raised by "Big Data". Prepared by Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy of OECD dated of 18 June 2013 [Electronic resource] // OECD [Site]. – URL: https://www.oecd-ilibrary.org/docserver/5k47zw3fcp43-en.pdf?expires=1532885941&id=id&accname=guest&checksum=002E2D4F737B29719CBA621F48C50B3E (accessed: 30.07.2018).

интенсифицируют вопросы о применении таких базовых принципов защиты данных как определение цели и ограничение использования. Произошедшие изменения, увеличение количества и источников обрабатываемых данных могут означать, что необходим поиск более гибкого и поддающегося адаптации подхода к распределению обязанностей.

Управление цифровой безопасностью и рисками защиты частной жизни. Справочный доклад, представленный на совещании на уровне министров о цифровой экономике (2016).[413] В отчете обсуждается изменение экономических и социальных аспектов цифровой безопасности и конфиденциальности в контексте цифровой среды и инноваций, основанных на обработке данных. В отчете изложены аргументы в пользу использования подхода, основанного на системе управления рисками, необходимой в новой цифровой среде.

Малые и средние предприятия (МСП) и начинающие стартапы, в частности, важны для экономического развития. Они двигают конкуренцию и инновации, способствуют созданию новых рабочих мест. Они также сталкиваются с проблемами управления безопасности в цифровой середе и рисками защиты частной жизни. Для поддержки МСП и стартапов предлагается разработать подход, включающий в себя руководство по оценке рисков, а также стимулирование использования страхования цифровых рисков.

Отмечается, что одним из наиболее существенных изменений в онлайн и мобильной среде за последние десять лет стало появление социальных сетей и значительное увеличение пользовательского контента. Люди создают, опубликовывают и распространяют на разных платформах информацию о них самих и их друзьях, родственниках, учителях и даже людях, которых они не знают. Люди могут непреднамеренно скомпрометировать свою собственную конфиденциальность, когда они распространяют информацию о себе, поскольку у них практически отсутствует контроль над тем, что третьи лица могут делать с их контентом, как он может быть интерпретирован ими. Это порождает сложные вопросы о том, как законодатель должен реагировать на новую роль людей в качестве создателей и распространителей контента, включая свои персональные данные.

Хотя отчет преимущественно посвящен вопросам информационной безопасности, в нем отмечается, что нарушение защиты персональных данных может происходить и по иным

[413] Managing Digital Security and Privacy Risk. Background Report from 2016 Ministerial Meeting on the Digital Economy. Prepared by OECD – 2016 [Electronic resource] // OECD [Site]. – URL: https://www.oecd-ilibrary.org/docserver/5jlwt49ccklt-en.pdf?expires=1532886027&id=id&accname=guest&checksum=6DF302F57942A41C30109715E4BFB08B (accessed: 30.07.2018).

причинам, например, когда обработка персональных данных осуществляется с нарушением принципов обработки.

Регулирование трансграничных потоков данных в соответствии с законами о защите персональных данных и частной жизни (2011).[414] Трансграничная передача данных стала важным элементом экономического, политического и социального развития со времени принятия в 1980 году Руководящих принципов по защите конфиденциальности и трансграничных потоках персональных данных (обновлены в 2013 году). Исследование OECD имеет своей целью описание актуального состояния регулирования трансграничной передачи данных и побуждение к размышлению о ее целях, функционировании и эффективности, в том числе, в будущем.

Отмечается, что регулирование в большей степени заждется на реализации преимуществ для электронной коммерции (например, регион АТЭС). В исследовании обращается внимание на важную роль гармонизации, согласовании законодательства разных стран в указанной сфере. Кроме того, указано, что существует тенденция применения национального законодательства об обработке данных в других странах (при трансграничной передаче данных), что может привести к конфликтам с обязательными положениями закона страны импорта, а также потребует маркировки данных, в зависимости от того, какой именно домашний режим защиты данных к ним применяется.

Рекомендации Совета касательно Рекомендаций по защите частной жизни и трансграничных потоках персональных данных (2013).[415] В Рекомендациях странам участницам предлагается имплементировать предложенные в них следующие принципы:

- ограничение сбора персональных данных
- качество данных
- определение цели
- ограничение использования
- меры обеспечения безопасности
- открытость

---

[414] C. Kuner Regulation of Transborder Data Flows under Data Protection and Privacy Law. Past, Present and Future. OECD Digital Economy Papers No. 187. – 2011 [Electronic resource] // OECD [Site]. – URL: https://www.oecd-ilibrary.org/docserver/5kg0s2fk315f-en.pdf?expires=1532886032&id=id&accname=guest&checksum=E42C47589D17B131D70C6FB93AFC436B (accessed: 30.07.2018).

[415] The OECD Privacy Framework – 2013 [Electronic resource] // OECD [Site]. – URL: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (accessed: 30.07.2018).

- индивидуальное участие
- подотчетность контролера персональных данных

Устанавливается, что любые ограничения трансграничной передачи персональных данных должны быть соразмерными потенциально возможным рискам с учетом чувствительности данных, цели и условий обработки данных.

RFID: курс на информационную безопасность и защиту частной жизни (2008)[416]. В документе описаны главные характеристики RFID технологий, а также их влияние на информационную безопасность и защиту частной жизни в краткосрочной перспективе. Использование RFID несет в себе большое количество потенциальных рисков, которые затрагивают каждый из трех классических аспектов безопасности: доступность, целостность и конфиденциальность.

При использовании RFID технологий помимо базовых сведений о защите данных в уведомления о конфиденциальности целесообразно включать также дополнительные сведения, такие как: 1) наличие RFID меток 2) их содержание, использование и контроль 3) наличие считывателя 4) активность считывания 5) возможность отключения RFID меток 6) где можно получить помощь.

В документе также определены типы рисков, а также методы контроля, позволяющие минимизировать их.

Отдельно рассматриваются вопросы защиты налоговой информации при межстрановом обмене финансовой информацией в целях предотвращения уклонения от уплаты налогов. Обмен информацией по запросу между юрисдикциями происходит на основе следующих договоров:

1. **Модельное соглашение ОЭСР об обмене информацией в сфере налогообложения** (Agreement on Exchange of Information on Tax Matters, или Tax Information Exchange Agreements, далее — «TIEA»); или

2. **Модельная конвенция ОЭСР об избежании двойного налогообложения по налогам на доходы и капитал** (Model convention with respect to taxes on income and on capital). Статья 26 данной конвенции регулирует вопросы обмена налоговой информацией.

В данных соглашениях не предусмотрено особое регулирование налоговой тайны, но

[416] Radio-Frequency Identification (RFID) A Focus on Information Security and Privacy. OECD Digital Economy Papers No. 138 dated of 14 January 2008 [Electronic resource] // OECD [Site]. – URL: https://www.oecd-ilibrary.org/docserver/230618820755.pdf?expires=1532885980&id=id&accname=guest&checksum=8C506A504953B560241DFB12428A26C2 (accessed: 30.07.2018).

урегулированы общие положения о конфиденциальности передаваемой информации, например, ст. 8 в TIEA «Конфиденциальность» и отдельные положения в ст. 26 Модельной конвенции «Обмен информацией» (положения схожи). В частности, декларируется, что любая информация, полученная в соответствии с соглашением, считается конфиденциальной в той же мере, как это предусмотрено законодательством договаривающейся страны. Информация может быть раскрыта только лицам или органам (включая суды и административные органы), которые вовлечены в оценку, сбор, исполнение или судебное разбирательство в отношении уплаты налогов. Указанные лица могут использовать полученную информацию только в данных целях. Информация не может быть раскрыта любому другому физическому или юридическому лицу или органу власти или любой другой юрисдикции без письменного согласия компетентного органа запрашиваемой стороны.

Схожие положения содержатся и в статье 22 «Тайна» **Многосторонней Конвенции о взаимной административной помощи в налоговых вопросах** (Multilateral Convention on Mutual Administrative Assistance in Tax Matters).

Многостороннее Соглашение компетентных органов об автоматическом обмене финансовой информацией от 29 октября 2014 г. (Common Reporting Standard – CRS), к которому 12 мая 2016 г. присоединилась Федеральная налоговая служба РФ, устанавливает систему правовых и технических средств сбора, получения и передачи сведений о состоянии финансовых активов юридических и физических лиц в автоматическом режиме. Статьей 5 настоящего соглашения устанавливается, что вся информация передается при соблюдении режима конфиденциальности, и определяются меры по защите данных в соответствии с требованиями национального законодательства.

Достаточно подробные параметры режима конфиденциальности налоговой информации содержатся в **Руководстве ОЭСР по обеспечению конфиденциальности информации**[417] (Keeping It Safe: The OECD Guide on the Protection of Confidentiality of Information Exchanged for Tax Purposes). Данное руководство содержит как общие рекомендации по защите конфиденциальности налоговых данных при налоговом администрировании и контроле внутри страны, так и конкретные рекомендации в отношении обмена информацией.

[417]Keeping It Safe: The OECD Guide on the Protection of Confidentiality of Information Exchanged for Tax Purposes [Electronic resource] // OECD [Site]. – URL: http://www.oecd.org/ctp/exchange-of-tax-information/keeping-it-safe-report.pdf (accessed: 30.07.2018).

Основополагающими в руководстве являются следующие постулаты защиты налоговой тайны:

1. Конфиденциальной считается как информация, представленная в запросе, так и информация, полученная в ответ на запрос.
2. Для обеспечения конфиденциальности применяются как положения международных соглашений, так и внутреннее законодательство.
3. Обмен информацией может использоваться только в определенных целях.
4. Обмен информацией может быть раскрыт только определенным лицам.

Кроме этого, рассматриваются разные подходы к соотношению между принципами защиты информации в законодательстве договаривающейся страны и в международном соглашении (с. 11 руководства). Во второй части руководства анализируются политики по администрированию режима налоговой тайны (с. 16 руководства). Основными принципами такой комплексной политики являются следующие утверждения:

1. Политика обеспечения налоговой тайны должна быть разработана и применяться
2. Такая политика должна быть одобрена высшим органом власти страны
3. Налоговый орган должен назначить лиц, ответственных за реализацию политики
4. Комплексная политика должна включать положения:
   - о проверке сотрудников, имеющих доступ к налоговой тайне;
   - подготовке таких сотрудников;
   - порядке доступа в помещения;
   - порядке доступа к записям на электронных и физических носителях;
   - правилах удаления информации; и
   - о работе с несанкционированным раскрытием информации.
5. Информация, направленная иностранному компетентному органу, должна передаваться по надежным каналам связи и в случае электронной передачи - с соответствующим уровнем шифрования.
6. Информация и входящие запросы, полученные от компетентного иностранного органа, должны быть надлежащим образом классифицированы, надежно сохранены, должны быть приняты меры, чтобы обеспечить использование и раскрытие такой информации в соответствии с договором или механизмом обмена информацией.

3.5. Всемирная организация здравоохранения (ВОЗ)

ВОЗ[418] – специальное учреждение ООН, организованное в 1948 году в Женеве. Основная функция ВОЗ – решение различных проблем здравоохранения в мире. Позиции ВОЗ в отношении права на частную жизнь (с учетом специфики медицинских данных) сформулированы в некоторых разрабатываемых организацией документах.

Декларация о правах пациентов в Европе (1994).[419] Вопросам частной жизни и конфиденциальности посвящен раздел 4 Декларации. В частности, указывается, что вся информация о здоровье человека, его состоянии, диагнозах, прогнозах течения болезни, лечения и вся иная информация, имеющая личный характер, должна оставаться конфиденциальной даже после смерти. Конфиденциальная информация может быть раскрыта только с явно выраженного согласия пациента или если закон прямо предусматривает такое раскрытие. Вмешательство в частую жизнь пациента и его семьи не допускается, если только он прямо не выразит согласия на это, и это не будет оправдываться необходимостью его диагностики, лечения и ухода.

Информатика и телематика в здравоохранении. Настоящее и потенциальное использование (1988).[420] Еще в 1988 году ВОЗ выпустила отчет по результатам исследований применения информационных технологий в здравоохранении в разных странах мира. В отчете указывается на необходимость создания национальной политики в сфере использования информационных технологий в здравоохранении. В качестве одного из четырех основных элементов такой политики выделяется определение мер и стандартов обеспечения безопасности и защиты данных.

В 2012 году был опубликован Инструментарий по формированию национальной стратегии цифрового здравоохранения[421], в котором защита частной жизни и

[418] World Health Organization [Electronic resource] // World Health Organization [Site]. – URL : http://www.who.int/ (accessed: 30.07.2018).

[419] A Declaration on the Promotion of Patients' Rights in Europe. European consultation on the rights of patients. Prepared by WHO dated of 28 June 1994 [Electronic resource] // World Health Organization [Site]. – URL: http://www.who.int/genomics/public/eu_declaration1994.pdf (accessed: 30.07.2018).

[420] Informatics and Telematics in Health. Present and Potential Uses. Prepared by WHO – 1988 [Electronic resource] // World Health Organization [Site]. – URL : http://apps.who.int/iris/bitstream/handle/10665/37201/9241561173-eng.pdf?sequence=1&isAllowed=y (accessed: 30.07.2018).

[421] National eHealth Strategy Toolkit. Prepared by WHO and ITU – 2012 [Electronic resource] // World Health Organization [Site]. – URL :

конфиденциальность также была поименована в качестве одного из ключевых условий.

Работа с информацией пациентов. Тенденции и трудности в странах-участницах (2012).[422] Отчет описывает шаги стран-участниц по применению информационных систем информации о пациентах. Так, отмечается, что необходимо четкое законодательное регулирования защиты личной тайны пациентов, а также защиты безопасности медицинской информации, содержащейся в электронных медицинских картах.

Сборник прецедентов по этическим вопросам в международных медицинских исследованиях (2009).[423] Исследования являются жизненно важным элементом для развития всемирной охраны здоровья. Один из важнейших компонентов исследований здоровья – это строгий набор этических стандартов, широко распространенных и применяемых командами исследователей и спонсоров. Глава 7 исследования посвящена защите частной жизни и конфиденциальности, и содержит несколько реальных примеров, когда был необходим поиск баланса между ценностью результатов исследований и угрозой нарушения конфиденциальности. Указывается, что в некоторых случаях конфликт между интересами науки и интересами участников исследователей в защите их личной информации и конфиденциальности не может быть разрешен до конца. Хотя по умолчанию приоритет имеет позиция участников в таких случаях, этические исследовательские комиссии могут, если потребуется, определить, насколько серьезно интересы участников будут затронуты исследованием, оценить потенциальные риски в сравнении с ценностью данных, которые можно получить в результате проведения исследования.

Появление электронного здравоохранения, появление и увеличение числа банков генетических данных, иных хранилищ медицинской информации свидетельствует о начале эпохи, когда люди будут терять способность контролировать то, что другие люди могут узнать об их здоровье и жизни в целом. Несмотря на это, изменения порождают преимущества для отдельных лиц и общества в целом. Однако преимущества могут быть замедлены или заблокированы в целом, если доступ и использование информации, которая

---

http://apps.who.int/iris/bitstream/handle/10665/75211/9789241548465_eng.pdf?sequence=1&isAllowed=y (accessed: 30.07.2018).

[422] Management of patient information. Trends and challenges in Member States. – Global Observatory for eHealth series – Volume 6 – 2012 [Electronic resource] // World Health Organization [Site]. – URL: http://apps.who.int/iris/bitstream/handle/10665/76794/9789241504645_eng.pdf?sequence=1 (accessed: 30.07.2018).

[423] R. Cash, D. Wikler, A. Saxena, A. Capron. Casebook on Ethical Issues in International Health Research. Prepared by WHO – 2009 [Electronic resource] // World Health Organization [Site]. – URL: http://apps.who.int/iris/bitstream/handle/10665/44118/9789241547727_eng.pdf?sequence=4&isAllowed=y (accessed: 30.07.2018).

может идентифицировать человека и которая защищается и охраняется, слишком сложны. Это, как отмечается, вызывает некоторые опасения, когда, например, угроза конфиденциальности не велика или существует только в теории, а потенциальная ценность результатов исследований напротив велика.

Рекомендации ВОЗ об этических проблемах государственного наблюдения за состоянием здоровья населения (2017).[424] На сегодня наблюдение за состоянием здоровья населения является иногда предметом горьких противоречий. Такое наблюдение может не только ограничивать право на частную жизнь, но также и иные гражданские свободы. В документе сформулированы 17 рекомендаций, которым необходимо следовать для построения системы наблюдения за здоровьем населения.

3.6. Международная организация по изучению генома человека (HUGO)

HUGO[425] была создана в Женеве в 1989 году в рамках международного научно-исследовательского проекта «Геном человека» (проект создан под эгидой Национальной организации здравоохранения США). Основная цель организации – поощрение и стимулирование сотрудничества между специалистами в сфере генетики в мире. В организации участвуют генетики разных стран мира.

Комитет по этике, праву и вопросам общественности (CELS) является механизмом, с помощью которого HUGO ведет диалог по этическим, правовым и социальным вопросам, связанным с генетикой и геномикой, их потенциале использования во благо человечества. В качестве основных документов CELS, касающихся генетической тайны, можно привести следующие.

Декларация о принципах проведения генетических исследований (1995).[426] Рекомендовано обеспечивать конфиденциальность и защиту от несанкционированного

[424] WHO guidelines on ethical issues in public health surveillance. Prepared by WHO – 2017 [Electronic resource] // World Health Organization [Site]. – URL: http://apps.who.int/iris/bitstream/handle/10665/255721/9789241512657-eng.pdf?sequence=1&isAllowed=y (accessed: 30.07.2018).

[425] HUGO [Electronic resource] // HUGO [Site]. – URL : http://www.hugo-international.org/ (accessed: 30.07.2018).

[426] Statement on the Principled Conduct of Genetics Research. Prepared by HUGO ELSIC dated of 21.12.1995 [Electronic resource] // HUGO [Site]. – URL : http://www.hugo-international.org/Resources/Documents/CELS_Statement-PrincipledConductofGeneticsResearch_1995.pdf (accessed: 30.07.2018).

доступа к генетической информации.

Декларация об отборе проб ДНК: контроль и доступ (февраль 1998).[427] Констатируется, что по своей природе генетическая информация является как личной, так и семейной. Следует избегать использования и передачи образцов, которые могут идентифицировать человека. Кодирование образцов – это техника, которая направлена на защиту конфиденциальности. Второй аспект – это анонимизация образцов.

Уважение согласия, а также сохранение конфиденциальности в процессе сбора, хранения и использования ДНК человека – краеугольные камни этического поведения при проведении исследований. В связи с этим HUGO сформулировала несколько рекомендаций, среди которых есть и те, которые относятся к вопросам конфиденциальности генетической информации (создание необходимых механизмов обеспечения безопасности, анонимизация). Если иное не предусмотрено законом сведения об участии в исследованиях не должны раскрываться третьим лицами (учреждениям), а также не должны раскрываться результаты исследований, которые могут идентифицировать отдельных лиц или семью. Как и иные медицинские данные, генетическая информация не подлежит раскрытию без соответствующего согласия.

Декларация о базе данных генома человека (декабрь 2002).[428] База данных генома человека – это набор систематически организованных данных, позволяющих осуществлять поиск. Геномные данные могут включать, среди прочего, разновидности нуклеиновых кислот, последовательностей белка, полиморфные гаплотипы. Работа, связанная с базой данных, включает в себя сбор, аннотирование, отбор, хранение, проверку и подготовку определенных наборов для передачи.

Для работы с базой данных генома человека CELS сформулировал несколько принципов и рекомендаций. Одна из рекомендаций касается вопросов конфиденциальности. В частности, в пункте 4 Декларации указывается, что необходимо уважать выбор и тайну личной жизни отдельных лиц, семей и общин в отношении использования их данных:

(a) выбор может быть сделан в отношении: пожертвования, хранения и использования

---

[427] Statement on DNA Sampling: Control and Access. Prepared by HUGO Ethics Committee dated of February 1998 [Electronic resource] // HUGO [Site]. – URL: http://www.hugo-international.org/Resources/Documents/CELS_Statement-DNASampling_1998.pdf (accessed: 30.07.2018).

[428] Statement on Human Genomic Databases. Prepared by HUGO Ethics Committee dated of December 2002 [Electronic resource] // HUGO [Site]. – URL : http://www.hugo-international.org/Resources/Documents/CELS_Statement-HumanGenomicDatabase_2002.pdf (дата обращения: 30.07.2018)

и образцов и информации, полученной из них. Информированное согласие может включать в себя уведомление об использовании (фактическом или будущем) или возможности отказа от использования, или, в некоторых случаях, может быть дано полное согласие;

(б) необходимо создавать механизмы для обеспечения уважения такого выбора;

(в) участники должны быть проинформированы о степени возможной идентификации их данных и о применяемых механизмах безопасности, обеспечивающих конфиденциальность;

(г) участники должны быть проинформированы о том, что их образцы могут быть переданы другим исследователям, в том числе, из других стран, коммерческим организациям и путем публикации или загрузки в сети Интернет.

Критическая роль конфиденциальности генетической информации отмечается также в Открытой концепции «Предполагаемое будущее: преимущества геномной расшифровки генетической последовательности для общества»[429] и Кодексе поведения раскрытия данных о геноме и здоровье человека (раздел 4)[430].

[429] Imagined Futures: Capturing the Benefits of Genome Sequencing for Society. Prepared by HUGO – 2013 [Electronic resource] // HUGO [Site]. – URL: http://www.hugo-international.org/Resources/Documents/CELS_Article-ImaginedFutures_2014.pdf (accessed: 30.07.2018).

[430] Sugano: International code of conduct for genomic and health-related data sharing. The HUGO Journal 2014 [Electronic resource] // HUGO [Site]. – URL: http://www.hugo-international.org/Resources/Documents/CELS_Article-InternationalCodeofConduct_2014.pdf (accessed: 30.07.2018).

4. ОБОБЩЕНИЕ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ, ОПРЕДЕЛЯЮЩИХ КОНТЕКСТ ВЫВОДОВ И ПРЕДЛОЖЕНИЙ

4.1. Общие закономерности правового регулирования различных видов тайн

В контексте разработки предложений о возможных для применения в российской правовой системе подходов, прежде всего, отметим основные выводы сравнительно правового исследования. Так, в результате проведенного сравнительно-правового исследования, которое допустимо считать первым в Российской Федерации комплексным анализом правового регулирования общественных отношений по поводу различных видов тайн на уровне репрезентативных юрисдикций и в актуальном контексте развития цифровой экономики, были сделаны выводы о наличии следующих **основных закономерностей** (закономерности разделены по обобщенным составляющим направлений исследования, соответствующих техническому заданию научно-исследовательской работы):

1. Для большинства юрисдикций характерен «принцип открытого перечня» формирования состава сведений, составляющих различные виды тайн. В большинстве юрисдикций в основе формирования данного открытого перечня в части наиболее актуальных видов тайны (тайна связи, врачебная тайна, банковская тайна, налоговая тайна) лежит соответствующая конституционно-правовая ценность, и преимущественно это неприкосновенность частной жизни. Как следствие, принцип отнесения данных к соответствующей тайне реализуется в зависимости от специфики конкретного случая и может быть выражен в подходе, предполагающем соотнесение конкретной информации, потенциально составляющей ту или иную тайну, с возможностью нарушения соответствующего конституционного права. Так, например, тайна связи может включать в себя потенциально неограниченный круг возможных данных, но при условии, что такие данные позволяют охарактеризовать коммуникацию между абонентами, включая содержание сообщений, а также сам факт и обстоятельства коммуникации. Напротив, сведения об абоненте, которые не «привязаны» к конкретному факту коммуникации в большинстве случаев не будут составлять именно тайну связи (хотя к ним может быть применен иной правовой режим).

2. В отношении вопроса о разграничении различных видов тайн и иных видов конфиденциальной информации между собой для большинства юрисдикций характерен подход, предполагающий использование условной «модели квалифицирующих признаков информации», выраженной в явной или неявной форме. Один и тот же набор сведений может подпадать под различные, подчас пересекающиеся между собой правовые квалификации и режимы, применяемые одновременно. Так, один и тот же набор данных, в зависимости от своего содержания, может, например, составлять одновременно тайну связи и персональные данные. При этом тот же самый набор данных может содержать, в то же время, и врачебную тайну (допустим, речь идет о сообщении, которое передается по каналам связи и содержит информацию о заболевании какого-либо пациента). В большинстве исследованных юрисдикций не прослеживаются унифицированные подходы к разрешению возможных правовых коллизий, возникающих вследствие такой парадигмы информационно-правовых отношений. Отдельную сложность на данный момент для европейских юрисдикций составляет тот факт, что юридическая квалификация общественных отношений по поводу всех аспектов обработки данных физических лиц, составляющих различные виды тайн, осуществляется преимущественно через призму GDPR.

3. Возможность предоставления сведений, составляющих различные виды тайн, третьим лицам преимущественно строится на основе «классической модели», которая предполагает две основных группы оснований. Во-первых, это явно выраженный публичный интерес, в основном связанный с вопросами обеспечения безопасности и (или) обеспечения надлежащего государственного управления на разных уровнях (например, для целей оперативно-разыскной деятельности или реализации прямо определенных контролирующих функций органов исполнительной власти). Во-вторых, это явно выраженный частный интерес, в некоторых исключительных случаях подразумевающий возможность обработки соответствующих сведений без согласия субъекта тайны (преимущественно в целях защиты жизни и здоровья, когда иной порядок не представляется возможным в силу фактических обстоятельств), но в большинстве случаев предполагающий наличие явного согласия субъекта тайны или всех имеющих отношение к соответствующей информации субъектов тайны, как в случае с тайной связи, которая действует в отношении всех участников какой-либо коммуникации. При этом в рамках исследуемых юрисдикций, несмотря на отдельные возможные примеры из законодательства и практики, не выявлено унифицированного

подхода к форме и процедуре получения согласий на предоставление (раскрытие) сведений, составляющих различные виды тайны.

4. В правовой политике некоторых юрисдикций, например, Японии, прослеживаются конкретные примеры осознания потребностей цифровой экономики и необходимости разработки подходов к использованию больших данных, что предполагает главным образом использование различных технологий обезличивания информации, составляющей соответствующие виды тайны и (или) персональные данные. При этом можно констатировать, что на текущий момент отсутствует определенный и единообразный подход к тому, какая степень и форма обезличивания данных будет достаточной для защиты соответствующих конституционных прав, лежащих в основе норм о различных видах тайны, в условиях таких технологий больших данных, которые в некоторых случаях могут допускать восстановление исходных данных и, как следствие, нивелировать усилия по их анонимизации. В некоторых случаях прослеживается стремление уравновесить риски использования больших данных для конституционных прав граждан посредством обоснования необходимости их использования в публично-правовых или общественно-полезных целях, таких как, например, развитие здравоохранения и профилактика заболеваний на примере врачебной тайны.

При реализации указанных предложений о возможных для применения в российской правовой системе направлениях развития законодательства и практики полагаем возможным учитывать следующий опыт, выявленный в ходе сравнительно-правового исследования и приведенный ниже с учетом дифференциации по предмету анализа.

4.2. Особенности правового регулирования тайны связи

Рассматриваемая тайна прямо закреплена или подразумевается во всех рассмотренных юрисдикциях, однако имеет свои особенности как на содержательном уровне, так и в самом механизме защиты граждан от неправомерного использования и распространения информации, относимой к тайне связи. Особо заслуживает внимание тот факт, что законодательство Российской Федерации не содержит прямых норм, регулирующих порядок доступа специальных категорий лиц к сведениям, составляющим тайну связи, и из законодательства вытекает, что такие категории субъектов не вправе использовать, передавать третьим лицам, разглашать или иным образом обрабатывать сведения,

составляющие тайну связи. Кроме того, сами операторы связи, сервисы обмена сообщениями и иные подобные организации, оказывающие услуги в данной области, по общему правилу и без специального волеизъявления субъектов, не являются обладателями информации в том смысле, который предусмотрен Законом об информации, и соответственно не могут ее использовать или определять порядок использования. Более того, законодательство РФ не содержит специальных норм относительно правил получения и администрирования согласий, на предоставление третьим лицам сведений, составляющих тайну связи.

Если рассмотреть зарубежные правопорядки, то можно прийти к выводу, что все из них регламентируют передачу сведений, составляющих тайну связи, в адрес государственных органов. Можно выделить похожие основания, согласно которым возможна передача сведений, составляющих тайну связи, третьим лицам без согласия субъекта данных: (1) судебное решение, (2) если такая передача прямо предусмотрена законом (чаще всего это связано с ОРД, контролирующими функциями органов исполнительной власти и т.д.), (3) когда это необходимо для защиты от опасности, защиты жизни, здоровья или экономического благополучия субъекта данных или третьего лица (третьих лиц).

Единственной признаваемой всеми зарубежными правопорядками возможностью передачи данных без согласия субъекта тайны связи является де-идентификация данных (или обезличивание). В Корее известны случаи анонимизации данных, охраняемых тайной связи, и использовании таких данных. Так, Korea Telecom предлагала доступ к анонимизированным данным, содержащим данные о тестах пользовательских сообщений и мест звонков с целью поддержки транспортного планирования – оптимизации работы ночного транспорта и решения проблем с перегруженным трафиком. Также эстонские операторы связи вправе обрабатывать данные о месте нахождения пользователей (*location data*), если это не охватывается иным законным основанием для обработки из ранее перечисленных, только при условии предварительной анонимизации. Кроме того, анонимизация или де-идентификация персональных данных в США занимает большое место в разрешении проблем, возникающих в связи с технологией больших данных. Используются для данных целей следующие методы: (1) маскирование данных, (2) добавление шумов, (3) скремблирование букв, (4) кодирование и т.д.[431]

[431] Dr. Khaled El Elmam Health Data De-Identification [Electronic resource] // The International Association of Privacy Professionals (IAPP) [Site]. – URL:

Особо примечателен пример из судебной практики Сингапура (дело *Teo Wai Cheong v. Credit Industriel et Commercial*), где было указано, что записи телефонных разговоров с клиентами возможно передавать (раскрывать) третьим лицам, если вместо имен клиентов в информации о звонке будут обозначены обезличенные идентификаторы «A», «B», «C» и т.д. Поэтому информация, передаваемая в обезличенной форме, не регламентируется законодательством о персональных данных Сингапура, а поэтому может быть свободно передаваема. Однако стоит отметить, что тайна связи может быть нарушена не только наличием описания и детализации звонка, но также и фактом прослушивания содержания такого звонка, по которому также возможно идентифицировать лицо. Поэтому подход в вышеприведенной практике не является однозначным, и должен быть критически воспринят, а также принят во внимание тот факт, что в Сингапуре все операторы связи являются либо государственными компаниями, либо организациями, частично аффилированными с государством, что по объективным причинам отдаляет Сингапур от Российской Федерации.

4.3. Особенности правового регулирования врачебной тайны

Несмотря на существенные различия в системах здравоохранения рассмотренных государств, медицинская, или врачебная, тайна имеет общую для всех стран природу и похожие методы регламентации для защиты от неправомерного использования.

В преамбуле GDPR поясняется, что такие особые категории персональных данных, которые требуют более высокого уровня защиты, должны обрабатываться в целях, связанных со здоровьем, только если это необходимо для достижения целей в интересах физических лиц или общества в целом, что в общем и целом соотносится с отнесением данных о здоровье к категории специальных персональных данных в России, так как подход ЕС, как и подход РФ исходят из природы медицинских данных как вида особо чувствительной информации. Однако применительно к сфере медицины важно отметить особенности в законодательстве ЕС, предусмотренные в отношении обработки персональных данных в целях научных исследований или в статистических целях, допускаемой без получения согласия лица. В частности, например, последующая обработка данных, осуществляемая в интересах общества, в целях проведения научного исследования или осуществления статистического

https://iapp.org/media/pdf/knowledge_center/Perspectives_on_Health_Data_De-Identification_final.pdf (accessed: 27.07.2018).

учета не должна рассматриваться в качестве несовместимой с первоначальными целями обработки, на которые было получено согласие субъекта.

В качестве примера использования открытых и больших данных на государственном уровне необходимо указать на систему электронного здравоохранения eHealth Эстонии. Ее основой является система Electronic Health Record (*e-Health Record* или *EHR*), построенная с использованием технологии блокчейн (*blockchain*) и интегрирующая данные различных медицинских организаций с целью создания единых учетных записей, доступ к которым может быть предоставлен каждому пациенту онлайн. Доступ к системе имеют пациенты, поставщики медицинских услуг, судебные эксперты-криминалисты (внесении данных о смерти лица) и другие лица, обрабатывающие данные (государственные органы, органы статистики, научные организации). Последние вправе использовать данные из EHR в целях проведения исследований, анализа и подготовки статистических данных, необходимых для разработки политики в сфере здравоохранения и исполнения международных обязательств, при условии, что все данные закодированы (обезличены). Для использования обезличенных данных получение согласия лица не требуется. При этом пациенты осуществляют полный контроль над своими данными и вправе в любой момент ограничить доступ к данным, содержащимся в системе. В этом случае лицу будет направлено уведомление, что предоставление медицинских услуг на базе неполной информации о его состоянии может быть опасным для здоровья.

4.4. Особенности правового регулирования банковской тайны

Перечень сведений, составляющих банковскую тайну в РФ, является открытым, к ней относится (1) информация о клиентах кредитной организации и о корреспондентах клиентов; (2) информация об операциях, счетах и вкладах клиентов и корреспондентов; (3) иные сведения, которые отнесены к банковской тайне внутренними документами кредитной организации. Напрямую вопрос возможности предоставления банковской тайны третьим лицам с согласия самого субъекта законодательством РФ не урегулирован, подробно не определены формы согласий, порядок их предоставления и администрирования, а возможность предоставления сведений, относимых к банковской тайне, аффилированным лицам холдинга возможен только в заранее определенных Законом о банках целях. Авторами проанализированы зарубежные юрисдикции, и с точки зрения технологии «больших данных»

и регламентации открытых данных, а также облегчения способов обмена сведениями, составляющими банковскую тайну, самыми показательными являются решения Германии и Великобритании кратко представленные ниже.

В Германии банковская тайна также не носит исчерпывающий характер, но, в отличие от России, для определения вводится следующий критерий: только такая информация, которая проистекает из деловых отношений банка и клиента, покрывается банковской тайной. Этот критерий называется «inner connection» (внутренние взаимоотношения) между деловыми отношениями и тем, как банк получает соответствующую информацию. Важно подчеркнуть, что в Германии существует SCHUFA – агентство по оценке кредитоспособности (Агентство)[432], принцип работы построен следующим образом. Клиенты дают согласие банкам на раскрытие их данных SCHUFA в качестве обязательного условия для вступления в отношения с банком, агентство собирает данные обо всех должниках Германии и предает собранную информацию кредиторам. Банки, торговые компании и компании иных секторов экономики являются такими кредиторами и могут получить доступ к базе данных Агентства на основе принципа взаимности. То есть если они сами сообщают данные о своих должниках в Агентство, они вправе получить доступ ко всей информации, которую предоставляют и иные кредиторы.

Отдельного внимания заслуживают аспекты больших данных в Великобритании. 6 ноября 2014 года Управление по защите конкуренции и рынкам Великобритании запустило большое исследование рынка розничных банковских услуг для физических лиц и малых и средних предприятий[433]. Учитывая, что крупные банки обладают большим количеством информации, было принято решение, что к таким данным должен быть обеспечен доступ для других компаний посредством разрешения использования API крупных банков. Кроме того, Управление приняло Приказ об исследовании розничного банковского рынка[434]. Полномочия Управления по изданию такого приказа установлены в ст.138 Закона о предпринимательской деятельности 2002 года[435]. В Приказе определены крупнейшие банки Великобритании,

[432] SCHUFA [Electronic resource]. – URL: https://www.schufa.de/de/ (accessed: 07.08.2018).

[433] Retail banking market investigation [Electronic resource] // Gov.uk [Site]. – URL: https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk#terms-of-reference (accessed: 31.07.2018).

[434] Retail Banking Market Investigation Order 2017 [Electronic resource] // Gov.uk [Site]. – URL: https://assets.publishing.service.gov.uk/media/5893063bed915d06e1000000/retail-banking-market-investigation-order-2017.pdf (accessed: 31.07.2018).

[435] Enterprise Act 2002 [Electronic resource] // Legislation.gov.uk. [Site]. – URL: http://www.legislation.gov.uk/ukpga/2002/40/contents (accessed: 31.07.2018).

которые должны открыть свои API к 13 января 2018 года. Клиенты банка участвуют в данном проекте только после дачи согласия, учитывая положения законодательства в личном кабинете физическое лицо может указать, к каким именно данным открыт доступ, как долго они могут обрабатываться. В целом проект позволяет пользователям видеть свои банковские аккаунты в режиме «одного окна», а также получить более персонализированные предложения. Данные, которые становятся доступными для третьих лиц через API, включают в себя, например, расположение филиалов банков, сведения о банковских продуктах и т.д. Цель проекта – облегчение поиска банков, сравнение банковских продуктов для выбора лучшего предложения. Что более важно, доступными в определенной мере становятся и данные о транзакциях.

4.5. Особенности правового регулирования налоговой тайны

В российском законодательстве понятие «налоговая тайна» имеет более или менее четкую дефиницию, выводимые принципы формирования таких сведений, в отличие от ряда зарубежных стран. Однако упираясь на сравнительно-правовую методологию, обмен рассматриваемых данных является приблизительно также развит как в иных зарубежных странах, например, в РФ раскрытие соответствующих сведений допускается только на основании закона и только полномочным лицам, и, таким образом, единственная возможность использовать информацию, относимую к налоговой тайне – это на основании согласия налогоплательщика. Анализ российского законодательства и судебной практики, а также зарубежных правопорядков указывает на то, что правовое регулирование сведений, составляющих налоговую тайну, приблизительно одинаково: (1) признание права на налоговую тайну и, по большей части, закрепление перечня сведений или критериев отнесения сведений к налоговой тайне, (2) в большинстве случаев содержится закрытый перечень лиц-государственных органов, которым возможна передача сведений, относящихся к налоговой тайне, (3) правомочие, закрепленное за государственными органами, на передачу данных для исполнения международных соглашений отдельно выделяется как еще одно основание передачи данных большинством стран. Ни в одной из рассмотренных юрисдикций не было обнаружено ни одной инициативы, связанной с открытыми данными или с технологией больших данных.

4.6. Обезличивание данных, составляющих предмет различных видов тайн

На сегодняшний день обезличивание данных, составляющих предмет любого вида тайны, является, пожалуй, единственным легитимным инструментом отчуждения информации третьим лицам для использования ее в рамках технологии больших данных, если не брать во внимание передачу персональных данных на основании согласия. Если в России существует правовая неопределенность, берущая начало в двух возможных интерпретациях подзаконного нормативно-правового акта,[436] то, например, в Японии механизм обезличивания настолько структурирован с позиции юридической техники, что не порождает коллизий и альтернативных интерпретаций.

Японская Декларация «О создании самой передовой в мире страны в области информационных технологий» (принята Кабинетом министров 14 июня 2013 года) гласит следующее: «Чтобы создать среду для использования данных и способствовать использованию открытых данных и больших данных, новая исследовательская организация будет немедленно создана в ИТ-стратегическом штабе. Эта новая организация будет работать над разработкой правил использования данных, которые способствуют широкому использованию данных, а также должна будет обеспечить защиту личной информации и конфиденциальности в кратчайшие сроки до конца этого года. В то же время политика будет также сформулирована к концу этого года с учетом введения новых правовых мер, таких как создание третьей организации с функциями контроля, надзора, рассмотрения жалоб и разрешения споров»[437].

Согласно Отчету об использовании анонимной информации, подготовленному Японским ведомством в сфере защиты персональной информации (The PPC Secretariat Report on Anonymously Processed Information[438]) адреса электронной почты, номера телефонов отнесены к информации, которая может идентифицировать персональную информацию, то есть это так называемые идентификаторы, которые при наличии иной информации могут отнести всю совокупность информации к персональным данным. В Японии существует

[436] Приказ Роскомнадзора от 05.09.2013 N 996 «Об утверждении требований и методов по обезличиванию персональных данных».

[437] The PPC Secretariat Report on Anonymously Processed Information [Electronic resource]: Personal Information Protection Commission of Japan // Personal Information Protection Commission of Japan [Site]. – URL: https://www.ppc.go.jp/en/legal/ (accessed: 08.08.2018).

[438] The PPC Secretariat Report on Anonymously Processed Information [Electronic resource]: Personal Information Protection Commission of Japan // Personal Information Protection Commission of Japan [Site]. – URL: https://www.ppc.go.jp/en/legal/ (accessed: 28.08.2018).

концепция т. н. «связующих кодов» («codes linking»). Отчет предусматривает, что создания обезличенной информации связующие коды (например, идентификационный номер устройства), которые могут быть использованы для идентификации лица, должны быть удалены (п. 4.1.3 Отчета), тем самым данная концепция очень напоминает американский подход обезличивания, построенный на удалении идентификаторов.

Отчет регламентирует не только данные, которые могут быть использованы в рамках технологии больших данных, но и виды обезличивания, которые должны быть применимы к каждому из них. Подчеркивается, что от вида доступности данных, зависят методы обезличивания. Имеется три вида так называемых видов доступной информации: (i) информация, ставшая публично доступной, (ii) информация, доступная для коммерческих организаций при регистрации пользователя, (iii) информация, доступная только близким людям и родственникам. Также от вида сложности получения новой информации о пользователе из совокупности всех представленных данных она ранжируется на (1) информацию, получаемую путем простого механического сопоставления и (2) информацию, получаемую нетипичными методами, например, с помощью сложного алгоритма или машинного обучения. Из анализа предложенных классификаций делается вывод, что единственным проблемным случаем при анонимизации персональных данных будет анонимизация информации (i). Кроме того, если в будущем механизмы машинного обучения станут общедоступны для обычных граждан, в этом случае такие данные также попадут в категорию (i) и будут классифицированы как общедоступные. Именно от вышеприведенных классификаций необходимо отталкиваться при определении метода обезличивания, т.е. в зависимости от обрабатываемой и получаемой информации.

Авторами настоящего исследования предлагается использовать методику вышеназванного японского отчета для учета специфики технологии больших данных в рамках обработки сведений, относящихся к различным видам тайн.

Дополнительно необходимо подчеркнуть, что принципы обработки данных, например, принцип минимизации не всегда совместим с технологией «больших данных», что было проиллюстрировано в зарубежных судебных решениях о признании нормативно-правовых актов неконституционными. Дело Tele2 Sverige AB v Post-och telestyrelsen указало на то, что государственные органы не имеют права хранить персональные данные на особых началах (например, необоснованно большой срок и состав данных). И хотя цель в виде борьбы с особо тяжкими преступлениями может выступать основанием для хранения таких данных, но

только при условии, что оно будет ограничено рамками строго необходимого. То есть храниться могут только определенные категории данных, относительно указанных видов средств связи, данные конкретных лиц, а также в течении фиксированного срока. Похожий подход был выработан в Деле Digital Rights Ireland. Суд ЕС установил, что Директива приводит к серьезному вмешательству в права, гарантированные статьями 7 и 8 Хартии Европейского союза по правам человека. Хотя Суд ЕС признал, что такое вмешательство пропорционально цели, ради которой оно осуществляется (борьба с тяжкими преступлениями и, как следствие, обеспечение общественной безопасности), Суд установил, что вмешательство не соразмерно целям Директивы. Так, вмешательство не дифференцировало средства связи, виды данных или типы пользователей, не была определена процедура доступа к данным, и при этом сроки хранения данных также не были определены объективно.

Вышеназванные судебные решения не просто указывают на нарушение порядка ограничения конституционных прав, но также иллюстрируют, что любая обработка данных, даже государственным органом, должна быть соразмерна целям, не избыточна и обладать обоснованными сроками хранения. В условиях технологии «Больших данных» такие судебные решения лишний раз подтверждают, что общепризнанные принципы обработки без детальной законодательной регламентации плохо совместимы с постоянно меняющимися целями обработки больших массивов данных.

Заслуживают внимания отдельные практические вопросы применения принципов защиты налоговой тайны. Так, с точки зрения рекомендаций в части пересмотра некоторых параметров налоговой тайны предлагается синхронизировать работу налоговых органов и третьих лиц, имеющих право на получение информации, составляющей налоговую тайну, непосредственно у субъектов налоговой тайны. Так, в частности, при осуществлении Фондом «Сколково» проверок деятельности участников инновационного центра «Сколково»[439], а также в рамках проверок резидентов особой экономической зоны (ОЭЗ) уполномоченным органом исполнительной власти[440], у участников «Сколково» (резидентов ОЭЗ) запрашиваются сведения из бухгалтерской отчетности, налоговые декларации и прочие сведения. Эту же информацию организации-участники предоставляют в налоговые органы в

[439] Правила осуществления исследовательской деятельности участниками проекта создания и обеспечения функционирования инновационного центра «Сколково» от 11 декабря 2013 года.

[440] Приказ Минэкономразвития России от 23 августа 2016 г. N 530 "Об утверждении порядка осуществления контроля за исполнением резидентом особой экономической зоны соглашения об осуществлении промышленно-производственной, технико-внедренческой, туристско-рекреационной деятельности или деятельности в портовой особой экономической зоне"

составе налоговой отчетности, в связи с чем указанные сведения составляют налоговую тайну. При этом проверяющие органы не могут запросить необходимые сведения в налоговых органах напрямую в связи с ограничением доступа к сведениям, составляющим налоговую тайну, предусмотренным положениями ст. 102 НК РФ.

Для оптимизации подобной двойной нагрузки по предоставлению отчетности на организации, которые являются участниками специальных режимов (Сколково, ОЭЗ), а также для устранения дублирования функций органами исполнительной власти и уполномоченными третьими лицами, представляется целесообразным предусмотреть на уровне федерального законодательства РФ возможность особого режима охраны сведений, составляющих налоговую тайну, для обеспечения доступа к ним и обработки накопленных данных уполномоченными третьими лицами.

4.7. Регулирование открытых данных

Так как на сегодняшний день рынок открытых данных имеет существенный экономический потенциал, различные страны разрабатывают государственные программы по продвижению их использования, привлекают коммерческие структуры, используют в исследовательских, статистических и научных целях. Целью эстонской инициативы Advancing the Use of Open Data является систематическое развитие использования открытых данных в Эстонии, увеличение степени осведомленности населения об открытых данных и их пользователях, усиление взаимодействия между владельцами данных и пользователями, развитие инновационных сервисов на основе данных. В Японии начиная с 2013 года планы и программы специального государственного органа, отвечающего за цифровое развитие Японии, предусматривают необходимость раскрытия информации государственных органов в форме открытых данных. И хотя на законодательном уровне не урегулирован порядок и случаи раскрытия открытых данных, Министерство внутренних дел и связи Японии предпринимает определенные меры для опубликования государственными органами сведений в форме открытых данных, предусматривает какие именно сведения можно считать открытыми данными[441], осуществляет поддержку функционирования портала открытых

[441] Promotion of Open Data Strategies [Electronic resource]: Ministry of Internal Affairs and Communications [Site]. – URL: http://www.soumu.go.jp/menu_seisaku/ictseisaku/ictriyou/opendata/eng/index_e.html (accessed: 08.08.2018).

данных Японии.[442] В Испании в региональном правительстве Каталонии имеется программа по развитию системы открытых данных о здоровье, генерируемых в данном регионе ("PADRIS"). Основной принцип программы заключается в том, чтобы медицинская информация, касающаяся отдельных пациентов, которая ранее хранилась в отдельных медицинских организациях, была объединена в единую базу данных, допускающую анализ посредством технологий больших данных. Целью программы является развитие исследований и инновации в медицинских науках. В декларативных документах программы предусматривается их «полная анонимизация», что является достаточно либеральным подходом в плане возможности использования данных о здоровье в алгоритмах технологии больших данных, так как обработка больших массивов данных о здоровье может привести к деанонимизации и, как следствие, к неправомерной дискриминации со стороны работодателей, страховщиков, банков, что может повлечь материальные потери и моральный вред заинтересованных физических лиц.

5. ПРЕДЛОЖЕНИЯ О ВОЗМОЖНЫХ ДЛЯ ПРИМЕНЕНИЯ В РОССИЙСКОЙ ПРАВОВОЙ СИСТЕМЕ ПОДХОДАХ

5.1. Выводы и предложения, основанные на результатах исследования

В свете выявленных закономерностей и с учетом конкретного эмпирического материала полагаем возможным сформулировать следующие основные выводы и соответствующие им предложения о возможных для применения в российской правовой системе направлениях развития законодательства и практики в рассматриваемых областях.

5.1.1. Устранение формальной неопределенности понятий различных видов тайн для целей правоприменения

Вывод(-ы) и постановка проблемы. Понятия различных видов тайн, как они закреплены и используются в российском законодательстве и практике, лишены четкого определения, что приводит к спорам относительно того, относятся или нет конкретные

[442] См.: http://www.data.go.jp/?lang=english (accessed: 08.08.2018).

сведения к тому или иному виду тайны. Даже в тех случаях, когда отдельные виды информации, составляющей какую-либо тайну, перечисляются в нормативных правовых актах достаточно подробно, перечень носит открытый характер (например, «…иные сведения, полученные при его медицинском обследовании и лечении» в отношении врачебной тайны), или используются термины, позволяющее неопределенно широкое толкование в зависимости от ситуации («…любые, полученные налоговым органом… сведения о налогоплательщике» в случае с налоговой тайной). Отсутствие единообразия в толковании определений в целом подтверждается судебной практикой. Материалы исследования подтверждают актуальность данной проблемы для многих юрисдикций.

Рекомендация(-и). Несмотря на то, что создание в отношении каждого вида тайны универсального и «раз и навсегда» установленного конкретного определения вряд ли возможно, допустимо **на нормативном уровне закрепить принцип отнесения той или иной информации к соответствующему виду тайны**. На примере тайны связи в качестве такого принципа может выступить относимость информации к акту коммуникации (сведения, индивидуализирующие конкретное сообщение и обстоятельства его передачи). Методология определения принципов может основываться на представлении о том, в каких случаях права субъекта тайны могут быть нарушены способом, непосредственно соответствующем характеру отношений.[443] При разработке соответствующих конкретных нормативных определений допустимо и необходимо учитывать судебную и иную правоприменительную практику. При этом следует учитывать, что даже при наличии отдельных определенных подходов, отраженных в правоприменительной практике, включая акты Конституционного Суда Российской Федерации, такие позиции в российской правовой системе не могут заменить по юридической силе положения федерального законодательства. Соответственно, указанные поправки целесообразно вводить на уровне актов федерального законодательства, определяющих различные виды тайн (ст. 63 Закона о связи, ст. 13 Закона об основах охраны здоровья граждан, ст. 26 Закона о банках и банковской деятельности, ст. 102 НК РФ).

В качестве отдельного возможного направления для последующих обсуждений дополнительно возможно отметить, что в Российской Федерации на данный момент в целом отсутствуют единообразные общие нормы, регулирующие институт тайн как таковой.

[443] Так, на примере тайны связи, в случае с датой и временем отправки сообщения, права субъекта могут быть нарушены непосредственно в связи с той ценность, которую субъекту дают услуги связи, и в данном случае речь идет о тайне связи; но в случае разглашения сведений об абоненте нарушается не тайна связи, а права субъекта персональных данных.

Единственным нормаивным актом, в котором данный вопрос рассматривается системно, остается Указ Президента Российской Федерации от 06.03.1997 г. № 188 (ред. от 13.07.2015) «Об утверждении перечня сведений конфиденциального характера» принятый более двадцати лет назад и естественным образом не учитывающий последующее серьезное развитие законодательства и практики. Для целей обеспечения единообразия правового регулирования различных видов тайн и правоприменения в данной области полагаем допустимым в перспективе оценить целесообразность подхода, нацеленного на то, чтобы установить общее понятие «тайны» на уровне Закона об информации (как разновидности конфиденциальной информации, определяемой в п. 7 ст. 2 Закона об информации) и определить правовой статус «обладателя тайны» по аналогии с «обладателем информации» (ст. 6 Закона об информации).

5.1.2. Устранение формальной неопределенности понятия «персональные данные» в соотношении с различными видами тайн

Вывод(-ы) и постановка проблемы. Исследование показывает, что в юрисдикиях, опирающихся главным образом на европейскую модель регулирования отношений по поводу персональных данных, нередко отсутствует определенность по поводу соотношения персональных данных и различных видов тайн. Это связано, во-первых, с возможностью расширительного толкования самого понятия персональных данных в целом («любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу», согласно п. 1 ст. 3 Закона о персональных данных), а во-вторых с неопределенностью конкретных составляющих данного понятия в контексте сопоставления с правовым режимом различных видов тайн – в частности, термина «косвенно» из определения выше. Соответственно, усматривается два аспекта данной проблемы: (1) к одному и тому же набору данных одновременно применяются нормы о соответствующей тайне и о персональных данных, что может представлять существенную сложность на практике; (2) неясно, может ли информация в определенных случаях составлять тайну и при этом не составлять персональные данные.

Рекомендация(-и). Принять правовую позицию, согласно которой персональные данные в контексте проблем правового регулирования тайн являются специальным институтом по отношению к каждому конкретному виду тайны. По общему правилу

действующего законодательства (в том числе, с учетом европейских примеров), к одному и тому же набору данных может применяться одновременно и законодательство о соответствующем виде тайны, и законодательство о персональных данных. В то же время, с учетом того, что в условиях цифровой экономики в некоторых случаях требуется упрощение юридических процедур, связанных с обработкой информации, и в некоторых случаях режим тайны уже может предоставлять достаточную защиту, допустимо **закрепить в Законе о персональных данных норму, допускающую возможность ограничивать «абсолютное право» в отношении персональных данных, и для этих целей предусматривающую полномочие Правительства Российской Федерации устанавливать на уровне подзаконного акта изъятие из применения законодательства о персональных данных (полностью или в части) к информации, охраняемой посредством норм о каком-либо виде тайны и (или) уточнять критерии, по которым информация может или не может рассматриваться как персональные данные в конкретном случае**.

5.1.3. Совершенствование правовых норм об обезличивании данных и установление четкого правового режима обезличенных данных

Вывод(-ы) и постановка проблемы. Исследование показывает, что в большинстве изученных юрисдикций, включая Российскую Федерацию, последующий экономически целесообразный оборот данных, полученных в рамках режима какой-либо тайны (и, как правило, сопутствующего режима персональных данных) возможен лишь при условии предварительного «снятия» таких режимов, что может быть реализовано только при условии анонимизации (обезличивания) такой информации. В ином случае последующий оборот данных в формате больших данных будет затруднен в силу многочисленных и сложных для соблюдения на текущем технологическом уровне требований, касающихся соответствующих согласий – в то же время, возможность получения согласий не исключена и представляется необходимой в случаях, когда экономическую ценность представляет «таргетированная» информация (см. п. 5.1.5 настоящего раздела Отчета). В то же время, достичь указанных целей позволит лишь «необратимое обезличивание», тогда как «обратимое обезличивание» может рассматриваться как способ защиты информации, а не изменения правового режима таковой. В рамках текущих нормативных актов не могут быть достигнуты цели обработки больших объемов необратимо обезличенной информации, утрачивающей режим

персональных данных или какой-либо тайны (в виду отсутствия формальной определенности в отношении такой квалификации).

Рекомендация(-и). Ключевая рекомендация в данном случае – **закрепление на уровне Закона об информации** (рассматриваемого как нормативный правовой акт, устанавливающий общие правила как для персональных данных, так и для различных видов тайн – в т.ч. с учетом рекомендации, отраженной в п. 5.1.1 настоящего раздела Отчета) **понятий «обратимое обезличивание информации» и «необратимое обезличивание информации» либо аналогичных им по форме внешнего выражения**. При определении данных понятий учитывать, что «обратимое обезличивание» подразумевает возможность восстановления первоначальной информации, как это, например, предполагается в Приказе Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных», предусматривающем сохранение полноты, структурированности, релевантности, семантической целостности и применимости обезличенных персональных данных, а также подчеркивающем, что обезличивание персональных данных направлено на их защиту от несанкционированного использования (таким образом, речь идет об «обратимом обезличивании информации»[444]). Напротив, «необратимое обезличивание информации» подразумевает невозможность восстановления относимости информации к определенному лицу и, с учетом международного опыта, требует устранения «связующих кодов» в содержании информации. **Дополнительно в Законе об информации требуется установить, что необратимо обезличенная информация утрачивает режим персональных данных и какой-либо применимой тайны**. К такой информации по-прежнему могут применяться общие положения о конфиденциальности на основании договора, и такая информация, при прочих равных условиях, может, например, выступать предметом гражданско-правового оборота как база данных.[445] Необратимое обезличивание может иметь экономическую ценность в тех случаях, когда последующее использование больших данных необходимо для аналитических целей, а не для «таргетированных» обращений к субъектам данных.

[444] Дополнительно следует отметить, что «анонимность» в терминологии п. 4 рассматриваемого Приказа подразумевает «невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без *применения дополнительной информации*».

[445] При выполнении условий, установленных Гражданским кодексом Российской Федерации, об оборотоспособности интеллектуальных прав на базы данных.

С точки зрения юридической техники, закрепление «необратимого обезличивания» применительно к персональным данным также потребует внесения изменений в ст. 3 Закона о персональных данных, определяющую обезличивание персональных данных как действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных, а также в иные положения данного закона, в которых обезличивание («обратимое обезличивание») рассматривается как «обработка *персональных* данных». Кроме того, данная рекомендация соотносится с рекомендацией, отраженной в п. 5.1.2 настоящего раздела Отчета, поскольку «необратимое обезличивание» посредством удаления «связующих кодов» предполагает устранение косвенной относимости информации к соответствующему физическому лицу.

5.1.4. Конкретизация полномочий органов исполнительной власти в отношении различных видов информации

Вывод(-ы) и постановка проблемы. Для значительного количества видов тайн и, прежде всего, рассматриваемых в настоящем исследовании как наиболее актуальные (тайна связи, врачебная тайна, банковская тайна и налоговая тайна), характерен приоритет защиты частных интересов. В то же время, в контексте предметного пересечения различных видов тайн и иных режимов информации, прослеживается тенденция, согласно которой защита таких интересов находится в ведении различных публичных органов, что в итоге может приводить к дублированию функций государственного управления. В условиях цифровой экономики, в том числе процессов интеграции сложных информационных систем различного назначения, имеет смысл обеспечить координацию деятельности органов исполнительной власти в этой области.

Рекомендация(-и). Указанная проблема особенно актуальна в системе других приведенных рекомендаций, в частности – о возможности закрепления подхода, предполагающего утрату информацией режима тайны и персональных данных (см. п. 5.1.3 настоящего раздела Отчета). С учетом этого представляется целесообразным **сохранить подход, предполагающий разграничение предметов ведения между органами исполнительной власти, для случаев, когда информация все еще составляет отдельные виды тайн и (или) персональные данные, однако предусмотреть, что с того момента как**

информация утрачивает режим тайны и персональных данных, несмотря на потенциальную относимость к определенной сфере общественных отношений, оборот такой информации не будет подлежать специальному регулированию. Предусмотреть указанный порядок возможно на уровне Закона об информации. Отдельные рекомендации (например, см. п. 5.1.2 настоящего раздела Отчета) также связаны с данной рекомендацией и косвенно предполагают внесение ясности в разграничение ведения между органами исполнительной власти на данный момент, в зависимости от того, рассматривается ли определенная информация как персональные данные в составе соответствующей тайны или как тайна без включения персональных данных.

5.1.5. Закрепление конкретных требований к согласиям на передачу (распространение) информации, составляющей различные виды тайн

Вывод(-ы) и постановка проблемы. В ходе исследования не было выявлено устоявшегося подхода к определению требований к самой возможности, а также к форме и процедуре волеизъявления, лежащего в основе согласия на передачу (раскрытие) информации третьим лицам и использование информации. Данный аспект также содержательно подразумевает возможные коллизии между требованиями к согласиям, установленным в нормативных правовых актах, ориентированных на различные предметы регулирования (например, законодательство о персональных данных и законодательство о связи). В связи с развитием цифровых технологий для гармонизации правового регулирования и правоприменения представляется целесообразным в предметном законодательстве разработать и детально раскрыть требования к предмету и форме соответствующих согласий.

Рекомендация(-и). **Принять подход, согласно которому лицо, в интересах которого установлен режим тайны, вправе выразить согласие на использование таких сведений одним волеизъявлением, предметом которого является обработка, в том числе, передача (распространение) информации, составляющей различные виды тайн**. Отдельно допустимо рассмотреть вопрос о целесообразности предусмотрения общих принципов, допускающих применение «гражданско-правового» подхода к выражению волеизъявлений, но при этом не исключающие определенность такого рода согласий – т.е. допустимость общих, но при этом определенных формулировок (например, «предоставление

аффилированным лицам» или «предоставление любым третьим лицам»). Необходимость такого рода принципов обусловлена правоприменительной практикой по вопросам согласий на обработку персональных данных, в которой встречается ограничительное толкование ч. 4 ст. 9 Закона о персональных данных (в частности, предполагающее невозможность указания более чем одной цели обработки персональных данных в одном согласии, что не соответствует предлагаемому подходу). Дополнительно может быть целесообразным учесть контекст цифровых отношений в части формы согласия и прояснить, в каких случаях согласие может рассматриваться как «письменное» либо предусмотреть возможность предоставления согласия в электронной форме, рассматриваемой как альтернатива «письменной», с учетом современных средств удаленной идентификации субъектов.

5.2. Отдельные вопросы по результатам обсуждения на заседании тематической рабочей группы

Подводя итоги в отношении предложений о возможных для применения в российской правовой системе подходов и принимая во внимание результаты обсуждения проекта отчета о настоящем исследовании на заседании Тематической рабочей группы «Большие данные» в рамках реализации Плана мероприятий по направлению «Нормативное регулирование» программы «Цифровая экономика Российской Федерации» 11 сентября 2018 года (далее – «ТРГ»), необходимо отметить следующее. В контексте актуальной социально-экономической проблематики основным выводом можно считать вывод о том, что мировые тенденции заключаются в постепенной (нередко – фрагментарной) адаптации законодательства и практики его толкования и применения к условиям больших данных, при этом в качестве основного и, вероятно, единственно возможного адекватного способа найти баланс между потребностями экономики, с одной стороны, и конституционно-правовыми ценностями, с другой стороны, является **анонимизация данных** для целей последующего оборота, включая коммерциализацию. При этом задача совершенствования нормативно-правовой базы в целях обеспечения инструментов анонимизации должна учитывать сложную систему существующих норм, закрепляющих различные виды тайн и иной конфиденциальной информации.

В рамках отечественной правовой системы вызывал бы сомнение подход, предполагающий фрагментарное разрешение данной задачи, как минимум, поскольку в

реальной системе государственного управления различные виды тайн и иной конфиденциальной информации относятся к предметам ведения широкого круга государственных органов. В связи с этим наиболее целесообразным направлением совершенствования законодательства представляется такое направление, которое будет нацелено на то, чтобы «разрубить гордиев узел», а именно разработка единой системы правовых норм, нацеленных на обеспечение инструментов анонимизации *любой* информации, которая до анонимизации может относиться к произвольной комбинации квалифицирующих признаков, определяющих ее конфиденциальный характер, а после – представлять собой информацию, которая бы отвечала требованиям необратимой анонимизации. Разработка конкретного решения и стандартов анонимизации может опираться на зарубежный опыт, предполагающий, в том числе, удаление «связующих кодов» или «идентификаторов» (опыт Японии и США). Данный подход представляется научно-оправданным по двум причинам. Во-первых, это возможность обобщения всех возможных видов тайн и иной конфиденциальной информации собственно в термине «конфиденциальная информация», в том смысле, в котором понятие «конфиденциальности», например, употребляется в п. 7 ст. 2 и ч. 2 ст. 9 Закона об информации. Во-вторых, это представление о том, что определенным образом обезличенная информация, которая до этого момента являлась конфиденциальной, после обезличивания необратимым способом теряет основания для квалификации ее и как «конфиденциальной», и как отдельных возможных квалифицированных видов таковой (включая отдельные виды тайн и персональные данные), а значит, как предмет правоотношений, может с этого момента рассматриваться как «информация» per se.

Конкретное выражение правил «легитимации» данных для целей оборота посредством определенных видов и форм анонимизации полагаем возможным закрепить в виде отдельной специальной статьи в Федеральном законе от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», которая может быть поименована, например, как «Обработка информации, составляющей большие данные». В такой статье могут быть закреплены правила, относящиеся к «единой процедуре анонимизации данных» для указанных целей. При этом возможность использовать такую «единую процедуру» не должна заменять уже существующие подходы, позволяющие использовать информацию в технологиях больших данных в доступных на данный момент случаях, предполагающих, в том числе, прямое указание закона и (или) получение соответствующих согласий.

Существующий подход следует оставить как альтернативное решение, позволяющее разрешать точечные проблемы обработки данных в конкретных случаях. В то же время, сохранение известной процедуры не означает отсутствие изменений и в ее отношении – главным необходимым таким изменением видится конкретизация и прямое закрепление положений о форме соответствующих согласий. В первую очередь, речь идет о прямом и конкретном прояснении формальной неопределенности в отношении того, что можно считать «согласием в письменной форме», как это соотносится с понятием «электронного сообщения (документа)». Дополнительное направление для совершенствования законодательства, выявленное в результате проведения настоящего исследования, заключается в придании формальной определенности отдельным понятиям, определяющим квалифицированные виды конфиденциальной информации.

В частности, например, в ходе обсуждения на заседании ТРГ, был поднят репрезентативный для исследуемой проблематики вопрос о возможности относить к тайне связи геолокационные данные и метаданные, такие как IMS, IMEI и др. Из материалов настоящего исследования вытекает, что такие данные или аналогичные им, действительно, могут быть отнесены к тайне связи, но только при условии, что они характеризуют сообщение (например, геолокационные данные, привязанные ко времени звонка и (или) сведениям об абоненте). Однако, действительно, из проанализированной правоприменительной практики следует, что соответствующие части текста применимых нормативных актов лишены формальной определенности в данном аспекте. Как показывает сравнительно-правовое исследование, в отрыве, включая «связующие коды», от сообщения эти данные не следует признавать относящимися именно к тайне связи – такой подход соответствует как мировым тенденциям, так и значительной части подходов, известных в Российской Федерации. В то же время, отсутствие установленного законодательно определения тайны связи (которое, как минимум, отражало бы принцип, лежащий в его основе) в текущих условиях допустимо рассматривать как пробел в законодательстве. Из чего следует, в частности, предложение о введении такого рода определений соответствующих видов тайн – например, дополнить ст. 63 Федерального закона от 07.08.2003 г. № 126-ФЗ «О связи» определением понятия «тайна связи», включив в число основных принципов связь информации с сообщением (разумеется, отметив и само содержание сообщения).

Возвращаясь к вопросу о предоставлении согласий на раскрытие информации, составляющей какую-либо тайну, вновь отметим, что мировые тенденции подтверждают

тезис о том, что такое согласие должно предоставляться всеми субъектами тайны. Такой подход, отметим, не исключает, например, создание технических инфраструктурных элементов, позволяющих выразить согласие всех субъектов тайны – так, на примере тайны связи, это может быть предусмотренная приложением возможность каждого из участников переписки выразить согласие на раскрытие такой информации. В то же время, такая возможность должна рассматриваться в контексте указанного выше предложения о прояснении требований к согласиям на раскрытие различных видов тайн с точки зрения формы, содержания и принципов. При разработке таких норм, вероятно, следует по аналогии учитывать положения ч. 1 ст. 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», предусматривающих ряд общих требований к согласиям на обработку персональных данных, которые должны предоставляться, в том числе, свободно, и быть конкретными, информированными и сознательными.

В отношении последних следует учитывать то обстоятельство, что конкретность, информированность и сознательность согласия не в полной мере согласуются с потенциалом технологий больших данных. Вполне вероятно, в системе рекомендуемых мер это, однако, не составит существенной проблемы, поскольку основным способом вовлечения информации в оборот больших данных предполагается все же их анонимизация. В то же время, на примере тайны связи, можно допустить более свободный режим для метаданных (например, предусмотреть разумный набор случаев, когда метаданные сообщения могут обрабатываться ограниченным кругом лиц для ограниченных целей – характерным примером здесь может послужить обработка таких данных техническими посредниками и (или) провайдерами вспомогательных услуг для целей совершенствования услуг связи). В случае с другими видами тайн также представляется возможным введение отдельных специальных случаев в целях создания благоприятной среды для оборота данных. Так, ориентируясь, в том числе, на общий подход, который прослеживается в системах англо-американского права, можно рассмотреть возможность получения и использования банками отдельных данных, изначально составляющих банковскую тайну, для расширения объема сервисов и (или) для отдельных коммерческих целей – как минимум, это должно быть возможно при условии анонимизации, но при этом можно допустить и обработку таких данных, например, в B2C сегменте. При этом в последнем случае для целей обеспечения баланса интересов представляется необходимым обеспечить надлежащее информирование граждан и предоставить им возможность отзыва «подразумеваемого» согласия. Аналогично, по

поднимавшемуся на ТРГ вопросу о согласии на передачу информации, составляющей банковскую тайну, третьим лицам для оказания их услуг и предоставления ими доступа к различным сервисам, помимо анонимизации (или, разумеется, согласия всех субъектов банковской тайны), если клиент сам инициирует такую услугу, можно закрепить принцип согласия, вытекающего из конклюдентных действий для таких случаев. Представляется также, что к третьим лицам, получающим указанную информацию подобным образом, должны быть применимы аналогичные требования в области информационной безопасности. В наиболее репрезентативном ключе концепция «подразумеваемого» согласия с возможностью его отзыва (opt-out), пожалуй, отражена в праве штата Калифорния, США (см. Раздел 1.5 настоящего исследования). Отдельно следует отметить и проблему, связанную с предоставлением сведений, составляющих банковскую тайну, кредитными организациями в соответствии с законодательством о противодействии отмыванию доходов, полученных преступным путем, отдельным государственным органам и должностным лицам (стр. 179 – 180 настоящего Отчета). В этой части полагаем необходимым придать положениям законодательства должный уровень формальной определенности.

Отдельно следует отметить, что вопросы, связанные с *медицинской тайной*, помимо указанной выше проблематики, также по-своему актуализируют процессы цифровизации общественных отношений. Например, актуален вопрос о том, можно ли считать медицинской тайной информацию, собираемую посредством носимых устройств (гаджетов). В целом ответ на данный вопрос зависит от того, является ли такое носимое устройство «обычным», ориентированным на массового потребителя, или же его использование сопряжено с процессами оказания медицинской помощи – в большинстве стран мира действует подход, аналогичный представленному в ч. 1 ст. 13 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан», согласно которому к врачебной тайне относятся сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении. При наличии таких признаков информация в объективном смысле будет составлять врачебную тайну. В отсутствие таких признаков сведения, собираемые посредством носимых устройств, не могут составлять врачебную (медицинскую) тайну, однако будут, по общему правилу, относиться к специальной категории персональных данных, как согласно GDPR, так и согласно российскому законодательству.

Возвращаясь к вопросу об анонимизации данных как основному принципу создания

благоприятной среды для оборота больших данных, допустимо также отметить пример Японии, относящийся к области R&D. Так, в 2018 году в Японии вступил в силу закон, получивший название «Jisedai Iryo-kiban Ho» (англ. «The next-generation medical infrastructure law», «Закон нового поколения о медицинской инфраструктуре»). Данный закон позволяет обезличивать «медицинские» большие данные таким образом, чтобы они могли быть использованы для исследований заболеваний и при разработке новых лекарств. Фактически, данный закон устанавливает особый доступ к медицинским данным, позволяя осуществить такой доступ без согласия пациента. Однако, чтобы использовать такие данные, каждый госпиталь и клиника должен обезличить данные, удалив ФИО пациентов и другую личную информацию. Закон позволяет предоставлять данные только по запросу специально аккредитованных государством учреждений. Система не является обязательной: каждое медицинское учреждение самостоятельно принимает решение, будет ли оно предоставлять такую информацию.[446]

В ближайшей перспективе при этом может быть намечен и другой, более масштабный вопрос о возможных объемах накопления и использования такой информации в глобальной трансграничной экономике, поскольку большие данные, собираемые в области медицины, здравоохранения и в целом в отношении здоровья граждан, в определенных случаях могут иметь стратегическое значение для национальных (государственных) интересов. Этот ракурс рассмотрения медицинской тайны отсылает нас к более широкому контексту, который, в том числе, связан с концепцией критической информационной инфраструктуры. Следует согласиться с экспертами, полагающими недостаточно определенным вопрос, например, о том, подразумевает ли Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» в определении субъекта критической информационной инфраструктуры возможность иностранных лиц учреждать российские юридические лица и, таким образом, вовлекать в пространство критической информационной инфраструктуры России элементы иностранной технической инфраструктуры. Этот и другие вопросы влияют на формирование общего нормативного ландшафта регулирования оборота информации, составляющей различные виды тайн, а также больших данных.

Наконец, общим вопросом для всех видов тайн, рассмотренных в настоящем

[446] См.: https://www.japantimes.co.jp/news/2017/05/15/reference/medical-big-data-pooled-disease-research-drug-development-japan/#.W7N64GcUn7w

исследовании, является вопрос о соотношении таковых с персональными данными. Как уже отмечалось, мировая тенденция (далекая при этом от определенности по всем конкретным вопросам) заключается в том, что один и тот же набор сведений может одновременно квалифицироваться как соответствующий вид тайны и как персональные данные. При этом, основываясь на материалах исследования, можно предположить, что получение согласия на обработку персональных данных может рассматриваться, особенно, в условиях неопределенности требований к согласиям по конкретным видам тайн, и как согласие на обработку информации, составляющей соответствующую тайну, но только в части прямого соответствия (пересечения) такой информации с персональными данными. В контексте обсуждения и развития предложений по совершенствованию законодательства полагаем возможным дополнительно оценить концепцию предоставления «универсального согласия» на обработку, во-первых, и персональных данных, и различных видов тайн, а во-вторых, без конкретизации и заблаговременного определения исчерпывающим образом целей обработки данных, поскольку иное не в полной мере соответствует потенциалу технологий больших данных. Данный подход был ранее обоснован авторами настоящего исследования применительно к рассмотрению проблемы формальной определенности понятия «персональные данные» в контексте больших данных.[447] В рассматриваемом контексте данный подход, скорее, может быть реализован в отношении «естественных операторов больших данных» (телекоммуникационные компании, банки и пр.), которые одновременно являются операторами персональных данных и различных видов тайн. При этом данный подход, скорее, может выступить одной из промежуточных альтернатив и не может заменять иные представленные предложения, в частности приоритет анонимизации как основного способа «легитимации» использования информации в условиях больших данных.

Процесс совершенствования законодательства в соответствии с представленными в настоящем отчете предложениями должен осуществляться с учетом контекста иных, разрабатываемых в рамках Программы «Цифровая экономика Российской Федерации», инициатив, включая такие ожидаемые результаты реализации программы как разработка порядка и правил доступа к общедоступным данным, а равно разработка порядка обезличивания персональных данных, условий и порядка их использования, а также порядка

[447] См.: Arkhipov V., Naumov V., The Legal Definition of Personal Data in the Regulatory Environment of the Russian Federation: Between Formal Certainty and Technological Development // Computer Law and Security Review. Dorchester (UK), 2016. Volume 32. Issue 6. PP. 868-887

получения согласия и обеспечения соблюдения прав и интересов граждан, уточнений аспектов ответственности за ненадлежащие обработку и безопасность персональных данных. Представляется, что предложения, отраженные в настоящем отчете, находятся в концептуальном единстве с иными разрабатываемыми инициативами по смежной тематике и вполне с ними согласуются.

6. ОБЗОР СУЩЕСТВУЮЩИХ И ВОЗМОЖНЫХ ДЛЯ ПРИМЕНЕНИЯ В РОССИИ МЕТОДИК РАСЧЕТА УЩЕРБА

6.1. Институт взыскания убытков как общая предпосылка методик расчета ущерба

Российским законодательством прямо установлено, что лицо, право которого было нарушено, может требовать полного возмещения причиненных ему убытков, если законом или договором не предусмотрено возмещение убытков в меньшем размере[448]. Под убытками понимаются расходы, которые лицо, чье право нарушено, произвело или должно будет произвести для восстановления нарушенного права, утрата или повреждение его имущества (реальный ущерб), а также неполученные доходы, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено (упущенная выгода). Если лицо, нарушившее право, получило вследствие этого доходы, лицо, право которого нарушено, вправе требовать возмещения наряду с другими убытками упущенной выгоды в размере не меньшем, чем такие доходы[449]. Кроме того, в некоторых случаях возможна компенсация морального вреда[450].

Институт взыскания убытков является межотраслевым и универсальным (теоретическая возможность взыскания практически при любом нарушении права и законных интересов в различных отраслях права)[451]. В том числе ущерб различным субъектам права может быть причинен вследствие разглашения либо несанкционированного использования коммерчески значимой информации, охраняемой в режиме тайны.

Для возмещения причиненного ущерба необходимо доказать наличие совокупности

[448] Гражданский кодекс Российской Федерации (часть первая) Ст. 15, П.1 [Электронный ресурс]: от 30.11.1994 N 51-ФЗ (ред. от 03.08.2018). – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 30.07.2018).

[449] Гражданский кодекс Российской Федерации (часть первая) Ст. 15, П.2 [Электронный ресурс]: от 30.11.1994 N 51-ФЗ (ред. от 03.08.2018). – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 30.07.2018).

[450] Гражданский кодекс Российской Федерации (часть вторая) Ст. 151 [Электронный ресурс]: от 26.01.1996 N 14-ФЗ (ред. от 29.07.2018). – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 30.07.2018).

[451] Либанова С.Э. Особенности возмещения убытков в различных отраслях права. Научно-практическое пособие. – Курган: КГУ, 2013. – 187 С.

следующих факторов[452]:

- наличие материального ущерба;
- противоправное поведение, ставшее следствием причинения вреда;
- причинную связь между противоправностью действий и наступившими убытками.

Согласно разъяснениям Пленума ВС РФ[453] размер подлежащих возмещению убытков должен быть установлен с разумной степенью достоверности. В случае если точный размер подлежащих восстановлению убытков невозможно установить, то их размер определяется судом с учетом всех обстоятельств дела, исходя из принципов справедливости и соразмерности ответственности допущенному нарушению[454]. Несмотря на требования ГК РФ, возместить ущерб, полученный в том числе от несанкционированного раскрытия информации, представляющей собой тайну, в полном объеме, зачастую не представляется возможным в связи с тем, что в отсутствии утвержденной методологии сложно обосновать размер понесенного ущерба. Таким образом, вопрос создания методологии оценки размера причиненного ущерба является актуальным вопросом, особенно в контексте развития цифровой экономики.

В то же время, проблему разработки подходов к расчету нанесенного ущерба необходимо рассматривать отдельно в контексте конкретной области права. В рамках настоящего исследования указанная проблема рассматривается в разрезе неправомерного раскрытия конфиденциальной информации, составляющей различные виды тайн.

6.2. Методики оценки ущерба от разглашения информации, составляющей различные виды тайн, представленный в российских источниках

Неправомерное раскрытие конфиденциальной информации может нанести ущерб как конкретному человеку, так и организации. Российским законодательством предусмотрено право граждан на возмещение полученного материального ущерба, а также на компенсацию морального вреда. Юридические лица же не могут претендовать на возмещение морального

[452] ФАС Московского округа от 04.10.2012 по делу № А40-49046/11 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 30.07.2018).

[453] Постановление Пленума Верховного Суда Российской Федерации от 23 июня 2015 г. N 25 "О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации" [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 30.07.2018).

[454] Там же.

вреда, если в случае противоправных действий был нанесен урон их деловой репутации[455]. Однако по мнению ВС[456] положения ГК РФ не препятствуют защите нарушенного права посредством заявления юридическим лицом требования о возмещении вреда, причиненного репутации юридического лица. В данном случае под вредом, причиненным деловой репутации, понимается всякое ее умаление, которое проявляется, в частности в наличии у юридического лица убытков, обусловленных распространением порочащих сведений и иных неблагоприятных последствиях в виде утраты юридическим лицом в глазах общественности и делового сообщества положительного мнения о его деловых качествах, утраты конкурентоспособности, невозможности планирования деятельности и т.д.[457] Таким образом, размер ущерба, причиненного репутации компании, также должен быть оценен исходя из материальных потерь, которые понесло юридическое лицо вследствие ухудшения своей репутации.

Независимо от того, какой ущерб был нанесен, для возмещения понесенных убытков необходимо доказать связь между противоправными действиями и фактом возникновения убытков, а также обосновать их объем.

В настоящее время в России отсутствую какие-либо законодательно утвержденные методические рекомендации для исчисления убытков, полученных от раскрытия тайной информации. Однако эксперты предлагают различные подходы к оценке как материального, так и морального видов ущерба.

6.2.1. Методики оценки материального ущерба

Оценивая имущественные потери в связи с несанкционированным раскрытием коммерчески значимых сведений, рекомендуется провести оценку следующих последствий[458]:

– прекращение или снижение уровня деловых отношений с партнерами;

[455] Гражданский кодекс Российской Федерации (часть первая) Ст.152, П.11 [Электронный ресурс]: от 30.11.1994 N 51-ФЗ (ред. от 03.08.2018). – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 30.07.2018).

[456] Определение Верховного Суда РФ от 18.11.2016 N 307-ЭС16-8923 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 30.07.2018).

[457] Там же.

[458] Северин В.А. Коммерческая тайна в России. 2-е изд., перераб. и доп. — М.: ИКД «Зерцало-М», 2009. — 472 С.

- срыв переговоров и выгодного контракта;
- невыполнение договорных обязательств;
- необходимость проведения маркетинговых исследований и разработки новой рыночной стратегии;
- отказ от ранее принятых решений, ставших неэффективными в результате утечки сведений;
- экономические санкции в отношении организации;
- возникновение сложных ситуаций в снабжении, производстве, сбыте продукции;
- потеря приоритета в научных исследованиях и возможностях патентования, продажи лицензий и ноу-хау;
- сокращение затрат конкурентов на проведение НИОКР;
- потери, связанные с утратой лидерства в научных исследованиях.

Для оценки материального вреда в стоимостном выражении можно использовать такие показатели как:

- стоимость непроизведенной продукции вследствие невыполнения обязательств контрагентами по поставкам оборудования, сырья и материалов, в результате отказа партнеров от экономического и научно-технического сотрудничества и осуществления конкурентами недружественных действий, связанных с неправомерным использованием коммерчески значимой информации;
- стоимость неправомерно используемых конкурентами отдельных результатов НИОКР (определяется экономия затрат конкурента на проведение собственных научных исследований);
- эффект от внедрения в производство неправомерно полученных конкурентами результатов НИОКР (определяется коммерческая выгода конкурентного преимущества в реализации товаров);
- стоимость приобретенного у конкурентов оборудования и технологий, которые изготовлены с использованием незаконно полученной коммерчески значимой информации;
- возможные объемы продаж товаров на рынке с использованием незаконно полученной конкурентами информации, другие показатели, характеризующие

возможный материальный вред организации [459].

Ряд приведенных показателей имеют однозначно определенное стоимостное выражение, значение других необходимо рассчитывать или оценивать экспертным путем. Так, например, для оценки ущерба от раскрытия конфиденциальных результатов НИОКР можно воспользоваться методом оценки ценности нематериальных активов и интеллектуальной собственности (доходным, расходным или сравнительным)[460]. Доходный метод оценки является наиболее оптимальным[461]. В этом случае экономический эффект, который мог бы быть получен от использования результатов НИОКР, можно представить в виде формулы:

$$U_{\text{общ}} = \text{С}_0 + \text{П}, \quad (1)$$

где С_0 – начальная стоимость конфиденциальной информации, П – прибыль от ее использования на интервале жизненного цикла.

При этом для оценки величины потенциальной прибыли в условиях изменения стоимости коммерчески значимых сведений можно воспользоваться формулой[462]:

$$\text{П} = N * \Delta\text{П}_1 + (N-1) * \Delta\text{П}_2 + \ldots + \Delta\text{П}_N, \quad (2)$$

где $\Delta\text{П}_i$ – значение приращения прибыли на i-м частичном интервале жизненного цикла коммерчески значимой информации, N- общее число частичных интервалов жизненного цикла.

Указанный выше подход может быть использован не только для оценки ущерба от разглашения конфиденциальных результатов НИОКР, но и от разглашения других конфиденциальных сведений. Тем не менее, приведенные формулы не лишены субъективизма в отношении ожидаемых значений приращения прибыли на каждом из этапов, а также в определении количества интервалов жизненного цикла.

6.2.2. Методики оценки морального ущерба

[459] Северин В.А. Коммерческая тайна в России. 2-е изд., перераб. И доп. — М.: ИКД «Зерцало-М», 2009. — 472 С.

[460] Козырев А.Н., Макаров В.Л. Оценка стоимости нематериальных активов и интеллектуальной собственности. – М.: Интерреклама, 2003. — 398 С.

[461] Там же.

[462] Росенко А.П., Аветисов Р.С. Математическое моделирование вероятного ущерба от утечки конфиденциальной информации в автоматизированной информационной системе. // Доклады ТУСУРа. – 2009. – №1 (19), часть 2. – С. 33 – 35

Проблема оценки морального ущерба является актуальной не только в случаях разглашения конфиденциальных сведений, но и в других областях права. В настоящее время в России отсутствуют какие-либо нормативно утвержденные методики оценки размера возмещения морального вреда. Величина компенсации определяется судом на основании следующих критериев:

- степени вины нарушителя;
- степени физических и нравственных страданий, связанных с индивидуальными особенностями лица, которому причинили вред;
- характера физических и нравственных страданий, который должен оцениваться с учетом фактических обстоятельств при которых был причинён моральной вред;
- требования разумности и справедливости;
- иных заслуживающих внимания обстоятельств.

Зачастую, при вынесении решений и присуждении меры наказания суды ориентируются на сложившуюся по данному вопросу судебную практику. Однако в случае с определением морального вреда данный подход не применим в связи с тем, что сложившаяся в России практика крайне неоднородна.

Тем не менее в юридической литературе встречается множество методик оценки морального вреда. Так, один из существующих методов сводится к установлению денежной компенсации за причиненный моральный вред в зависимости от размера санкции статьи УК РФ, применяемой к подсудимому[463]. В этом случае во внимание берется только один вид наказания – лишение свободы, выраженный в месяцах. За каждый месяц лишения свободы предлагается засчитывать сумму в один минимальный размер оплаты труда (МРОТ). По имущественным преступлениям предложено взыскивать моральный ущерб в размере половины суммы причиненного материального ущерба. Однако это положение противоречит Постановлению ВС[464], в котором закреплено, что размер возмещения морального вреда не может быть поставлен в зависимость от размера удовлетворения иска о возмещении материального вреда, убытков и других материальных требований.

Наиболее проработанной методикой оценки размера компенсации морального вреда

[463] Панарин В.Я. Защита имущественных прав личности в уголовном процессе Российской Федерации: автореф. дис. ... д-ра юрид. наук : 12.00.09 / В. Я. Понарин ; Воронеж. гос. ун-т. – Воронеж, 1994. – 37 с.

[464] Постановление Пленума Верховного Суда РФ от 20.12.1994 N10 «Некоторые вопросы применения законодательства о компенсации морального вреда» [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 30.07.2018).

является методика А.М. Эрделевского[465]. Согласно его методике размер компенсации может быть рассчитан по формуле:

$$D = d * f(v) * i * c * (1 - f(s)) * p, \quad (3)$$

где D – размер компенсации действительного морального вреда; d – размер компенсации презюмируемого морального вреда; f(v) – степень вины причинителя вреда ($0 \leq f(v) \leq 1$); i – коэффициент индивидуальных особенностей потерпевшего ($0 < i < 2$); c – коэффициент учета заслуживающих внимания обстоятельств ($0 < c < 2$); f(s) – степень вины потерпевшего ($0 \leq f(s) \leq 1$); p – коэффициент учета имущественного положения причинителя вреда, при этом $0{,}5 \leq p \leq 1$.

Каждому виду правонарушения А.М. Эрделевский определил размер компенсации презюмируемого морального вреда, при этом его максимальное значение составляет 720 МРОТ, а минимальное – 7,2 МРОТ. В части нарушений, связанных с разглашением конфиденциальных данных, А.М. Эрделевский отмечает только нарушение тайны переписки, телефонных переговоров, почтовых или иных сообщений. Презюмируемый моральный вред от данного правонарушения составляет 24 МРОТ.

Методология А.М. Эрделевского является первой и на данный момент единственной тщательно проработанной методологией, снижающей субъективность принимаемых решений. Тем не менее предложенный метод также не лишен недостатков, в частности возникают вопросы к обоснованности и соразмерности презюмируемого морального вреда, а также к полноте перечисленных видов нарушений. В настоящее время указанная методология не является общепринятой, но может использоваться при составлении исков.

Еще одна попытка формализовать подход к оценке морального ущерба был предпринята В.П. Палиюком[466]. Методика предполагает установление верхнего и нижнего пределов компенсаций. При расчете итоговой компенсации используется следующая формула:

$$D = D' * S * F * (1 - F'), \quad (4)$$

где D’ – базовая сумма материального эквивалента морального вреда, которая

[465] Эрделевский А.М. Моральный вред и компенсация за страдания. Научно-практическое пособие. М.: Издательство Век, 1998. – 188 с.

[466] А.А. Швец. Методические основы компенсации морального ущерба в Украине [Электронный ресурс] // УВЕКОН ИНТЕЛЛЕКТ [Сайт]. – URL: http://www.uvecon.in.ua/?mod=content&page=pub_5&lang=rus (дата обращения: 08.08.2018)

рассчитывается сугубо индивидуально исходя из исследования причиненного вреда и личностных особенностей потерпевшего; S – суммарный стрессовый эквивалент, рассчитанный на основе мнения психолога; F- коэффициент виновности ответчика, принимает значения 0.25, 0.5, 0.75 и 1; F’ – коэффициент виновности потерпевшего ($0 \leq F' \leq 1$).

Для оценки базовой суммы материального эквивалента морального вреда (D’) по 100-бальной шкале оценивается перечень факторов, включающих интенсивность психотравмирующего воздействия, величину вреда, причиненного социальному престижу и деловой репутации, нарушение жизненных/ профессиональных планов и перспектив, интенсивность переживаний и ряд других факторов. Каждый фактор имеет свой материальный коэффициент, величина которого соответствует полной оплате мер, направленных на восстановление первичного состояния потерпевшего.

В отличие от методики А.М. Эрделевского указанная методика предусматривает более личностный подход. При этом акцент делается на выделении повышающих и понижающих критериев, схожих с представленными в методике А.М. Эрделевского.

6.3. Методики оценки ущерба от разглашения информации, составляющей различные виды тайн, представленные в иностранных источниках

Проблема оценки ущерба от разглашения конфиденциальных сведений актуальна не только в России но в других странах мира. Так, некоторые европейские страны и США сделали первые шаги в части формализации подхода к оценке убытков, полученных в результате раскрытия тайной информации. Кроме того, в некоторых странах удалось на законодательном уровне закрепить механизмы оценки морального вреда.

6.3.1. Методы оценки реального ущерба и упущенной выгоды

Наиболее репрезентативным являются методы, представленные в законодательстве и доктрине США. Сущность коммерческой тайны и способы ее защиты определены в законе

«О коммерческой тайне»[467] и в Законе США «Об экономическом шпионаже»[468]. Согласно ним ущерб от несанкционированного раскрытия коммерчески значимых сведений складывается из реальных убытков потерпевшей организации и ее упущенной прибыли.

Недополученная прибыль рассчитывается как разница между упущенной выручкой и затратами, необходимыми для получения этой выручки. Для оценки реального убытка а также упущенной выручки используют следующие методы[469]:

- метод «до и после»;
- сравнительный метод;
- метод «если бы не»;
- метод, основанный на условиях базовых соглашений (соглашение о конфиденциальности, соглашение о неразглашении и т.д.).

Метод «до и после» предполагает сравнение операционных показателей потерпевшей компании до и после утечки конфиденциальных сведений. В качестве исходных данных для этих целей может использоваться финансовая и бухгалтерская отчетность компании. Фактически данный метод позволяет определить реальные потери компании в связи с разглашением ее конфиденциальных сведений.

Сравнительный метод позволяет оценить нанесенный компании ущерб, сравнивая показатели ее деятельности с показателями деятельности других аналогичных компаний или средними показателями по отрасли. При использовании данного метода ключевым является вопрос сопоставимости отобранных компаний пострадавшей компании.

Метод «если бы не» позволяет оценить упущенную компанией выручку от раскрытия коммерчески значимых секретных данных. При использовании данного метода изучаются финансовые прогнозы компании, бюджеты, планы и стратегии, разработанные до момента раскрытия тайны. Проводится оценка доли рынка, которую бы заняла компания, если бы раскрытия конфиденциальных сведений не случилось, строятся финансовые модели, оценивается влияние на цену, объем и ассортимент производимой компанией продукции.

В случае когда расчет понесенного убытка производится в отношении конкретного контракта, многие данные для расчета могут быть заранее указаны в договоре (прогнозное

---

[467] Uniform Trade Secrets Act (UTSA) [Electronic resource] // Uniform Trade Secrets Act (UTSA) [Site]. – URL: http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf (accessed: 30.07.2018).

[468] U.S. Economic Espionage Act (EEA) [Electronic resource] // Federation of American Scientists [Site]. – URL: https://fas.org/sgp/crs/secrecy/R43714.pdf (accessed: 30.07.2018).

[469] Shawn D. Fox, CPA “Calculating Damages in Misappropriation of Trade Secrets Matters” [Electronic resource] // Willamette [Site]. – URL: http://www.willamette.com/insights_journal/16/spring_2016_2.pdf (accessed: 30.07.2018).

значение производимой продукции, цена на продукцию и др.). В таком случае расчет упущенной выручки проводится на основе данных контракта.

Подробные рекомендации к расчету ущерба по каждому из вышеперечисленных методов приведены в практическом руководстве Американского института дипломированных независимых бухгалтеров[470].

На следующем шаге для определения недополученной прибыли необходимо оценить расходы, которые бы понесла компания для получения выручки, рассчитанной по методу «если бы не». Для оценки возможных расходов необходимо провести анализ структуры себестоимости производимой продукции, прямых и косвенных расходов. В руководстве по оценке нематериальных активов прямо указано, что дополнительные расходы представляют собой только те расходы, которые не были понесены, поскольку дополнительная выручка не была получена[471].

В случае когда раскрытие коммерческой тайны связано с недобросовестной конкуренцией недополученная прибыль потерпевшей компании может быть оценена как дополнительная прибыль компании, незаконно завладевшей коммерчески важной информацией. В рамках данного подхода также оценивается дополнительная выручка компании, завладевшей коммерческой тайной, и дополнительные затраты на получение данной выручки. При этом используются методы, схожие с описанными выше.

6.3.2. Методы оценки стоимости коммерчески значимых сведений

В случаях когда не удается оценить прямой ущерб компании и ее упущенную выгоду, а также дополнительную прибыль кампании-нарушителя, целесообразно оценить непосредственную стоимость коммерчески значимой информации. Американское общество оценщиков предлагает методы оценки стоимости коммерческой тайны во многом перекликающиеся с методами, представленными в исследованиях отечественных авторов[472]:

---

[470] The American Institute of Certified Public Accountants (AICPA) Practice Aid 06-4, “Calculating Lost Profits” [Electronic resource] // The American Institute of Certified Public Accountants [Site]. – URL: https://www.aicpa.org/InterestAreas/ForensicAndValuation/Resources/PractAidsGuidance/DownloadableDocuments/PA_064_Excerpt.pdf (accessed: 30.07.2018).

[471] Reilly and Schweihs, Guide to Intangible Asset Valuation [Electronic resource] // Willamette [Site]. – URL: http://www.willamette.com/insights_journal/14/autumn_2014_4.pdf (accessed: 30.07.2018).

[472] [Electronic resource] // [Site]. – URL: http://www.appraisers.org/docs/default-source/discipline_bv/bv-standards.pdf(accessed: 30.07.2018).

– затратный метод (включает оценку всех прямых и косвенных расходов на создание тайны, а также ожидаемую прибыль от его использования);
– метод рыночной стоимости (основан на анализе сделок по продаже/ приобретению аналогичных коммерческих тайн или лицензий на их использование);
– доходный метод (оценивается суммарный доход от непосредственного использования коммерческой тайны или продажи лицензии на нее).

Часто затратный метод используется в случаях, когда коммерческая тайна будет приносить дополнительную прибыль. Метод рыночной стоимости используется достаточно редко, поскольку информации о подобных сделках довольно мало, кроме того, коммерческие тайны довольно специфичны, что усложняет поиск схожих сделок. Доходный метод целесообразно использовать когда ожидается, что коммерческая тайна будет обеспечивать дополнительный денежный поток.

6.3.3. Методы оценки «справедливого роялти»

В ситуациях, когда рассчитать ущерб от разглашения коммерчески значимых сведений не представляется возможным, целесообразно использовать метод «справедливого роялти». Для расчета справедливого роялти могут быть использованы следующие методы[473]:

– метод дополнительной прибыли;
– метод дифференцированного дохода;
– метод сопоставимых сделок;
– метод сопоставимой прибыли.

В рамках метода дополнительной прибыли фактическая прибыль компании, незаконно завладевшей коммерческой тайной, сравнивается с прибылью компаний, обладающих схожей средневзвешенной стоимостью активов (без учета коммерческой тайны). Полученная разница расценивается как прибыль от незаконного использования коммерческой тайны и используется для расчета справедливой ставки роялти.

В рамках метода дифференцированного дохода сравниваются дисконтированные денежные потоки компании, пострадавшей от раскрытия коммерческой тайны. Первый

[473] Reilly and Schweihs, Guide to Intangible Asset Valuation [Electronic resource] // Willamette [Site]. – URL: http://www.willamette.com/insights_journal/14/autumn_2014_4.pdf (accessed: 30.07.2018).

дисконтированный денежный поток соответствует текущим ожиданиям компании, а второй – ожиданиям до момента раскрытия конфиденциальных сведений. Таким образом справедливая ставка роялти рассчитывается как отношение разницы между денежными потоками к годовой выручке компании, незаконно завладевшей коммерческой тайной.

Метод сопоставлений предполагает анализ случаев использования аналогичных коммерчески значимых сведений в рамках лицензионных правоотношений.

Согласно методу сопоставимой прибыли ожидаемая прибыль компании, завладевшей коммерчески значимой информацией, сравнивается со средней прибылью сопоставимых компаний, не владеющих аналогичными коммерчески значимыми сведениями. Полученная разница является основой для расчета роялти.

Резюмируя результаты проведенного исследования можно выделить следующие наиболее распространенные виды компенсации ущерба, нанесенного раскрытием конфиденциальных сведений:

- компенсация прямого материального убытка и упущенной выгоды;
- компенсация в размере прибыли, полученной компанией-нарушителем в результате использования незаконно разглашенных коммерчески значимых сведений;
- компенсация в виде непосредственной стоимости коммерческой тайны;
- компенсация в виде справедливого роялти.
- компенсация морального вреда.

Как правило, указанные методы описаны в контексте раскрытия коммерческих тайн, однако их использование возможно и при разглашении иных конфиденциальных сведений, повлекших материальные убытки.

6.4. Зарубежная практика применения различных видов расчетов компенсации ущерба от разглашения конфиденциальной информации

В юрисдикциях большинства стран (Бельгии, Болгарии, Франции, Люксенбурге, Мальте, Португалии, Румынии, Словакии, Словении, Испании и других) отсутствуют какие-

либо критерии для расчета ущерба[474]. В таком случае, используются любые из доступных методов оценки, при этом важно, чтобы проводимые расчеты были максимально объективны и основывались на конкретных данных.

Например, в Италии и Великобритании компании могут сами выбрать способ расчета полученного ущерба – оценивая свою упущенную выгоду, либо необоснованную выгоду компании, воспользовавшейся незаконно разглашенной коммерческой тайной[475]. В дополнение к возмещенному ущербу компании Великобритании могут потребовать прекращения дальнейшего использования коммерческой тайны компанией-нарушителем[476].

В законе о недобросовестной конкуренции в Японии предусмотрено три варианта для расчета суммы ущерба (упущенная выгода, дополнительная выгода, сопоставимые лицензионные платежи). Во Франции при оценке ущерба оценивают только убытки потерпевшей компании, при этом дополнительная прибыль компании, воспользовавшейся коммерческой тайной, не учитывается[477].

В таких странах как Австрия, Германия, Венгрия, Италия, Нидерланды и Великобритания в качестве возможной опции, для расчета причиненного ущерба оценивают возможный размер лицензионных платежей за использование коммерческой тайны[478]. То есть моделируется ситуация, когда компания добровольно продала лицензию на коммерчески значимую информацию другой компании. При этом в Австрии таким образом рассчитывается минимально возможный размер компенсации.

В ряде стран (Ирландии, Великобритании и США) помимо возмещения ущерба нарушитель также обязан выплатить штраф потерпевшему. В Польше и Венгрии штраф используется для благотворительных целей[479].

В Китае компании, незаконно завладевшей коммерческой тайной, могут запретить ее

---

[474] Study on Trade Secrets and Confidential Business Information in the Internal Market. Prepared for the European Commission [Electronic resource] // European Commission [Site]. – URL: http://ec.europa.eu/DocsRoom/documents/27703/ (accessed: 30.07.2018).

[475] European Observatory on Counterfeiting and Privacy. Damages in Intellectual Property Rights [Electronic resource] // European Commission [Site]. – URL: http://ec.europa.eu/internal_market/iprenforcement/docs/damages_en.pdf (accessed: 30.07.2018).

[476]Hogan Lovells, Trade Secrets Global Guide, 2018 [Electronic resource] // Hagan Lovells [Site]. – URL: http://www.hoganlovells.com/en/pdfdownload?page={6CCEEEF4-48E2-4D44-ACE9-A40280A3523D}&p=1 (accessed: 30.07.2018).

[477] Ibid.

[478] Study on Trade Secrets and Confidential Business Information in the Internal Market. Prepared for the European Commission [Electronic resource] // European Commission [Site]. – URL: http://ec.europa.eu/DocsRoom/documents/27703/ (accessed: 30.07.2018).

[479] Ibid.

дальнейшее использование. В качестве компенсации потерпевшая компания может рассчитывать на возмещение в размере понесенных потерь или прибыли конкурента, полученной в результате использования незаконно разглашенных сведений. Если определить ущерб не представляется возможным, суд в праве сам назначить сумму компенсации, но не более USD 470k. В таком случае суд оценивает стоимость самой коммерческой тайны а также обстоятельства дела в целом[480]. Суды ряда других стран (например, Бельгии, Дании, Испании, Японии) также могут назначать справедливую компенсацию ущерба по своему усмотрению.

Директивой ЕС[481] помимо возмещения материальных убытков предусмотрена компенсация морального ущерба, в случаях когда это применимо. В отличии от России (см. п. 2.2), где у судов отсутствуют какие-либо ориентиры для определения морального ущерба, законодательство ряда европейских стран более формализовано.

Так, в Великобритании сумма компенсации морального вреда определяется исходя из тарифной схемы[482]. Приведенный в тарифной схеме перечень содержит информацию о всевозможных преступлениях, способных нанести моральный вред. Виды вреда разбиты на 25 групп с фиксированных размером компенсации по каждой группе.

В США подход к компенсации морального вреда зависит от штата. На практике довольно трудно взыскать компенсацию морального ущерба, причиненного по неосторожности, но если моральный ущерб причинен умышленно или вследствие грубой неосторожности, то он, скорее всего, будет компенсирован, даже если размер вреда незначителен. В то же время максимальный размер компенсации морального ущерба не может превышать установленной суммы.[483]

Во Франции установлены фиксированные значения компенсаций морального ущерба в случае полной утраты трудоспособности. В остальных случаях, для расчета суммы

---

[480] Hogan Lovells, Trade Secrets Global Guide, 2018 [Electronic resource] // Hagan Lovells [Site]. – URL: http://www.hoganlovells.com/en/pdfdownload?page={6CCEEEF4-48E2-4D44-ACE9-A40280A3523D}&p=1 (accessed: 30.07.2018).

[481] Directive (EU) No. 2016/943 Of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, Strasbourg, 8.VI.2016 [Electronic resource] // Official Journal of the European Union [Site]. – // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0943&rid=1 (accessed: 30.07.2018).

[482] The Armed Forces and Reserve Forces (Compensation Scheme), Schedule 3 “The tariff and supplementary awards” [Electronic resource] // Pension Appeal Tribunal Scotland [Site]. – // URL: https://www.patscotland.org.uk/sites/default/files/ruleandledg/AFRFCS_Order_2011.pdf (accessed: 30.07.2018).

[483] Институт стратегического анализа: Николаев И.А., Точилкина О.С., аналитический доклад «Экономика морального вреда» [Электронный ресурс] // Финансовые и бухгалтерские консультанты [Сайт]. – URL: https://www.fbk.ru/upload/docs/moral_damage.pdf (дата обращения: 08.08.2018).

компенсации используется формула:

$$D = S * F,$$

где S – степень инвалидности (в %), F – нормативный размер компенсации.

Нормативные размеры компенсации устанавливаются на законодательном уровне. Моральный ущерб, не связанный с физическими повреждениями, компенсируется исходя из универсальной концепции морального вреда.

В Австрии и Германии отсутствуют точные критерии для определения компенсации морального вреда. При этом в Австрии законодательно установлены дневные ставки компенсации морального ущерба в случае телесных повреждений в зависимости от степени страданий. При определении размера моральной компенсации в Германии судьи ориентируются на сложившуюся судебную практику, которая там вполне однородна.

ЗАКЛЮЧЕНИЕ

Настоящее исследование включает в себя сравнительно-правовой анализ действующих норм права, правоприменительных правктик и тенденций регулирования, дифференцированный по видам тайн, рассматриваемым в качестве наиболее значимых для контекста информационного общества и цифровой экономики (тайна связи, врачебная тайна, банковская тайна, налоговая тайна), и репрезентативным примерам, относящимя к Российской Федерации, а также таким зарубежным юрисдикциям как ЕС, Великобритания, США, Япония, Сингапур, Южная Корея, Израиль, ОАЭ.

На основе проведенного сравнительно-правового анализа были сделаны выводы о наличии основных закономерностей, связанных с предметом исследования. Так, для большинства юрисдикций характерен «принцип открытого перечня» формирования состава сведений, составляющих различные виды тайн, при том, что конкретный состав сведений определяется, как правило, в зависимости от определенного конституционного права. В большинстве юрисдикций при этом прослеживается подход, предполагающий использование условной модели квалифицирующих признаков информации, согласно которой один и тот же набор сведений может подпадать под различные правовые режимы, включая режим персональных данных. Предоставление информации третьим лицам, как правило, возможно либо в силу специально определенных в законе оснований, связанных с явно выраженным публичным или частным интересом либо на основе согласия субъекта тайны. При этом, однако, в наиболее интересных с точки зрения предмета исследования юрисдикций прослеживается тенденция к внедрению и нормативному закреплению инструментов для обезличивания данных в целях последующего использования в общественно-полезных целях и (или) их коммерциализации.

С учетом выявленных закономерностей и конкретных эмпирических примеров предложены направления развития законодательства и практики Российской Федерации в рассматриваемых областях. В число данных направлений входит развитие законодательства в области персональных данных и методических подходов в части квалификации информации данным образом и соотношения такой информации с различными видами тайн, а также в области автоматизированной обработки данных. Целесообразным представляется развитие и нормативное закрепление подходов к обезличиванию информации в целях обеспечения

последующего использования и оборота. Предложено направление, предполагающее разработку методологии и обеспечение координации деятельности органов исполнительной власти в рассматриваемой области, развитие подходов к определению момента идентфикации субъектов при обработке информации в базах данных, а также в отношении требований к согласиям на передачу (раскрытие) информации.

При реализации указанных направлений законодательства и практики представляется возможным учитывать репрезентативные эмпирические примеры, относящиеся к отдельным юрисдикциям, нашедшим свое отражение в соответствующих разделах исследования и обобщенных в Разделе 4 «Предложения о возможных для применения в российской правовой системе подходов», включая опыт Южной Кореи, Сингапура, ЕС, Великобритании и Японии. В зависимости от дальнейших направлений развития российского законодательства и практики может оказаться полезным и иной опыт зарубежных юрисдикций, отраженный в сравнительно-правовой части настоящего исследования.

СПИСОК ИСТОЧНИКОВ

ИСТОЧНИКИ В ЧАСТИ ИССЛЕДОВАНИЯ ПО ВОПРОСАМ ПРАВА РОССИЙСКОЙ ФЕДЕРАЦИИ

Нормативно-правовые акты и иные официальные документы

1. Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 № 95-ФЗ (ред. от 03.08.2018) [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
2. Вправе ли налоговый орган по запросу организации предоставить информацию о зарегистрированной другой организацией-налогоплательщиком ККТ, с применением которой происходит поступление выручки от реализации товаров? [Электронный ресурс]: Письмо УФНС РФ по г. Москве от 20.06.2008 № 22-12/059038 – Доступ из справ.-правовой системы «КонсультантПлюс».
3. Гражданский кодекс Российской Федерации (часть первая) [Электронный ресурс]: от 26 янв. 1996 г. № 14-ФЗ. – Доступ из справ.-правовой системы «КонсультантПлюс»
4. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ (ред. от 03.08.2018) [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
5. Информационное письмо Президиума ВАС РФ от 13.09.2011 № 146 05 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
6. Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс]: от 30.12.2001 № 195-ФЗ (ред. от 29.07.2018) (с изм. и доп., вступ. в силу с 31.07.2018). – Доступ из справ.-правовой системы «КонсультантПлюс».
7. Конституция Российской Федерации [Электронный ресурс]: принята всенародным голосованием 12 дек. 1993 г. – Доступ из справ.-правовой системы «КонсультантПлюс».
8. Методические рекомендации по публикации открытых данных государственными органами и органами местного самоуправления, а также технические требования к публикации открытых данных. Версия 3.0 (утв. протоколом заседания Правительственной комиссии по координации деятельности Открытого Правительства от 29.05.2014 № 4) [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 08.08.2018).
9. Налоговый кодекс Российской Федерации (часть первая) [Электронный ресурс]: от 31.07.1998 № 146-ФЗ (ред. от 03.08.2018) – Доступ из справ.-правовой системы «КонсультантПлюс».
10. О банках и банковской деятельности [Электронный ресурс]: Федеральный закон от 02.12.1990 № 395-1 (ред. от 03.08.2018) – Доступ из справ.-правовой системы «КонсультантПлюс».
11. О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс]: Федеральный закон от 26.07.2017 № 187-ФЗ – Доступ из справ.-правовой системы «КонсультантПлюс».

12. О внесении изменений в статью 102 части первой Налогового кодекса Российской Федерации [Электронный ресурс]: Федеральный закон от 01.05.2016 № 134-ФЗ – Доступ из справ.-правовой системы «КонсультантПлюс».
13. О государственной гражданской службе Российской Федерации [Электронный ресурс]: Федеральный закон от 27.07.2004 № 79-ФЗ (ред. от 03.08.2018) – Доступ из справ.-правовой системы «КонсультантПлюс».
14. О добровольном декларировании физическими лицами активов и счетов (вкладов) в банках и о внесении изменений в отдельные законодательные акты Российской Федерации [Электронный ресурс]: Федеральный закон от 08.06.2015 № 140-ФЗ (ред. от 19.02.2018) – Доступ из справ.-правовой системы «КонсультантПлюс».
15. О единой государственной информационной системе в сфере здравоохранения (вместе с «Положением о единой государственной информационной системе в сфере здравоохранения») [Электронный ресурс]: Постановление Правительства РФ от 05.05.2018 № 555 – Доступ из справ.-правовой системы «КонсультантПлюс».
16. О кредитных историях [Электронный ресурс]: Федеральный закон от 30.12.2004 № 218-ФЗ (ред. от 03.08.2018) – Доступ из справ.-правовой системы «КонсультантПлюс».
17. О национальной платежной системе [Электронный ресурс]: Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 27.06.2018) – Доступ из справ.-правовой системы «КонсультантПлюс».
18. О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 31.12.2017). – Доступ из справ.-правовой системы «КонсультантПлюс».
19. О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 31.12.2017) – Доступ из справ.-правовой системы «КонсультантПлюс».
20. О полиции [Электронный ресурс]: Федеральный закон от 07.02.2011 № 3-ФЗ (ред. от 29.07.2018) – Доступ из справ.-правовой системы «КонсультантПлюс».
21. О почтовой связи [Электронный ресурс]: федеральный закон от 17.07.1999 №176-ФЗ (ред. От 06.07.2016) – Доступ из справ.-правовой системы «КонсультантПлюс».
22. О представлении информации по пунктам 5 и 10 приложения № 1 к Соглашению об информационном взаимодействии между Центральным банком Российской Федерации и Федеральной налоговой службой [Электронный ресурс]: <Письмо> Банка России N 01-40-7/7949, ФНС России № ММВ-20-2/150@ от 02.10.2017 – Доступ из справ.-правовой системы «КонсультантПлюс».
23. О представлении информации по пунктам 5 и 10 приложения № 1 к Соглашению об информационном взаимодействии между Центральным банком Российской Федерации и Федеральной налоговой службой [Электронный ресурс]: <Письмо> Банка России № 01-40-7/7949, ФНС России № ММВ-20-2/150@ от 02.10.2017 – Доступ из справ.-правовой системы «КонсультантПлюс».
24. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (с изм. и доп., вступ. в силу с 23.07.2018) [Электронный ресурс]: Федеральный закон от 07.08.2001 № 115-ФЗ (ред. от 23.04.2018)) – Доступ из справ.-правовой системы «КонсультантПлюс».
25. О распространении режима налоговой тайны на запросы [Электронный ресурс]: Письмо Минфина России от 13.02.2015 № 03-02-08/6483 – Доступ из справ.-правовой системы «КонсультантПлюс».
26. О связи [Электронный ресурс]: федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 03.08.2018). – Доступ из справ.-правовой системы «КонсультантПлюс».

27. О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации [Электронный ресурс]: Указ Президента РФ от 22.12.2017 № 620 – Доступ из справ.-правовой системы «КонсультантПлюс».
28. О технических требованиях к системе технических средств для обеспечения функций оперативно-розыскных мероприятий на сетях электросвязи Российской Федерации [Электронный ресурс]: Приказ Госкомсвязи РФ от 20.04.1999 № 70 З – Доступ из справ.-правовой системы «КонсультантПлюс».
29. О трансплантации органов и (или) тканей человека [Электронный ресурс]: Закон РФ от 22.12.1992 № 4180-1 (ред. от 23.05.2016) – Доступ из справ.-правовой системы «КонсультантПлюс».
30. О Центральном банке Российской Федерации (Банке России) [Электронный ресурс]: Федеральный закон от 10.07.2002 № 86-ФЗ (ред. от 29.07.2018) – Доступ из справ.-правовой системы «КонсультантПлюс».
31. Об аудиторской деятельности [Электронный ресурс]: Федеральный закон от 30.12.2008 № 307-ФЗ (ред. от 23.04.2018) – Доступ из справ.-правовой системы «КонсультантПлюс».
32. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 19.07.2018). – Доступ из справ.-правовой системы «КонсультантПлюс».
33. Об использовании федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (вместе с «Правилами использования федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме») [Электронный ресурс]: Постановление Правительства РФ от 10.07.2013 № 584 (ред. от 30.06.2018) @ – Доступ из справ.-правовой системы «КонсультантПлюс».
34. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления [Электронный ресурс]: Федеральный закон от 09.02.2009 № 8-ФЗ (ред. от 28.12.2017) – Доступ из справ.-правовой системы «КонсультантПлюс».
35. Об обязательном пенсионном страховании в Российской Федерации [Электронный ресурс]: Федеральный закон от 15.12.2001 № 167-ФЗ (ред. от 27.06.2018) – Доступ из справ.-правовой системы «КонсультантПлюс».
36. Об оперативно-розыскной деятельности [Электронный ресурс]: Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 06.07.2016) – Доступ из справ.-правовой системы «КонсультантПлюс».
37. Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных (Зарегистрировано в Минюсте России 18.03.2016 № 41455) [Электронный ресурс]: Указание Банка России от 10.12.2015 № 3889-У – Доступ из справ.-правовой системы «КонсультантПлюс».
38. Об организации предоставления государственных и муниципальных услуг (с изм. и

доп., вступ. в силу с 31.07.2018) [Электронный ресурс]: Федеральный закон от 27.07.2010 № 210-ФЗ (ред. от 04.06.2018) – Доступ из справ.-правовой системы «КонсультантПлюс».
39. Об основах охраны здоровья граждан в Российской Федерации [Электронный ресурс]: Федеральный закон от 21.11.2011 № 323-ФЗ (ред. от 19.07.2018) – Доступ из справ.-правовой системы «КонсультантПлюс».
40. Об отнесении информации о наличии либо отсутствии денежных средств на банковском счете налогоплательщика к сведениям, составляющим налоговую тайну, а также о праве налогового органа приостанавливать операции по счетам в банке [Электронный ресурс]: Письмо УФНС РФ по г. Москве от 31.12.2008 № 09-17/122410 – Доступ из справ.-правовой системы «КонсультантПлюс».
41. Об отнесении к налоговой тайне сведений о подтверждении налогового статуса (резидентства) гражданина [Электронный ресурс]: Письмо ФНС России от 02.12.2015 № ЗН-3-17/4568 – Доступ из справ.-правовой системы «КонсультантПлюс».
42. Об отнесении представленных в налоговый орган сведений о доходах физических лиц и суммах начисленного и удержанного НДФЛ к налоговой тайне, не подлежащей разглашению налоговыми органами [Электронный ресурс]: Письмо ФНС РФ от 20.10.2011 № ПА-3-12/3437) – Доступ из справ.-правовой системы «КонсультантПлюс».
43. Об услугах по принятию (выдаче) документов, связанных с постановкой на учет, и выдаче пароля от личного кабинета налогоплательщика [Электронный ресурс]: Письмо ФНС России от 09.11.2015 № ОА-19-17/276 – Доступ из справ.-правовой системы «КонсультантПлюс».
44. Об утверждении Концепции информационной безопасности Федеральной налоговой службы [Электронный ресурс]: Приказ ФНС России от 13.01.2012 № ММВ-7-4/6@ – Доступ из справ.-правовой системы «КонсультантПлюс».
45. Об утверждении Концепции системы управления информационной безопасностью ФНС России [Электронный ресурс]: – Доступ из справ.-правовой системы «КонсультантПлюс».
46. Об утверждении Перечня должностных лиц системы МВД России, пользующихся правом доступа к сведениям, составляющим налоговую тайну (Зарегистрировано в Минюсте России 20.02.2012 № 23253) [Электронный ресурс]: Приказ МВД России от 11.01.2012 № 17(ред. от 06.06.2018) – Доступ из справ.-правовой системы «КонсультантПлюс».
47. Об утверждении перечня средств связи, подлежащих обязательной сертификации [Электронный ресурс]: Постановление Правительства РФ от 25.06.2009 № 532 (ред. от 28.01.2015) – Доступ из справ.-правовой системы «КонсультантПлюс».
48. Об утверждении Положения о защите информации в платежной системе [Электронный ресурс]: Постановление Правительства РФ от 13.06.2012 № 584 – Доступ из справ.-правовой системы «КонсультантПлюс».
49. Об утверждении Порядка ведения персонифицированного учета в сфере обязательного медицинского страхования (Зарегистрировано в Минюсте России 08.02.2011 № 19742) [Электронный ресурс]: Приказ Минздравсоцразвития России от 25.01.2011 № 29н (ред. от 08.12.2016) – Доступ из справ.-правовой системы «КонсультантПлюс».
50. Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации (Зарегистрировано в Минюсте России 08.02.2018 № 49966) [Электронный ресурс]: Приказ ФСТЭК России

от 06.12.2017 № 227 – Доступ из справ.-правовой системы «КонсультантПлюс».
51. Об утверждении Порядка доступа к конфиденциальной информации налоговых органов (Зарегистрировано в Минюсте РФ 26.03.2003 № 4335) [Электронный ресурс]: Приказ МНС РФ от 03.03.2003 № БГ-3-28/96 – Доступ из справ.-правовой системы «КонсультантПлюс».
52. Об утверждении Порядка доступа к конфиденциальной информации налоговых органов (Зарегистрировано в Минюсте РФ 26.03.2003 № 4335) [Электронный ресурс]: Приказ МНС РФ от 03.03.2003 № БГ-3-28/96 – Доступ из справ.-правовой системы «КонсультантПлюс».
53. Об утверждении Порядка доступа к конфиденциальной информации налоговых органов (Зарегистрировано в Минюсте РФ 26.03.2003 № 4335) [Электронный ресурс]: Приказ МНС РФ от 03.03.2003 N БГ-3-28/96 – Доступ из справ.-правовой системы «КонсультантПлюс».
54. Об утверждении Порядка осуществления контроля за соблюдением держателями сертификатов соответствия и декларантами обязательств по обеспечению соответствия поставляемых средств связи установленным требованиям. Часть I. Порядок осуществления контроля за соблюдением держателями сертификатов соответствия обязательств по обеспечению соответствия поставляемых средств связи установленным требованиям (Зарегистрировано в Минюсте России 20.05.2016 № 42203) [Электронный ресурс]: Приказ Минкомсвязи России от 01.02.2016 № 28 – Доступ из справ.-правовой системы «КонсультантПлюс».
55. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений [Электронный ресурс]: Постановление Правительства РФ от 08.02.2018 № 127 ФЗ – Доступ из справ.-правовой системы «КонсультантПлюс».
56. Об утверждении Правил оказания услуг связи по передаче данных [Электронный ресурс]: Постановление Правительства РФ от 23.01.2006 № 32 (ред. от 25.10.2017) – Доступ из справ.-правовой системы «КонсультантПлюс».
57. Об утверждении Правил организации и проведения работ по обязательному подтверждению соответствия средств связи [Электронный ресурс]: Постановление Правительства РФ от 13.04.2005 № 214 (ред. от 28.01.2012) – Доступ из справ.-правовой системы «КонсультантПлюс».
58. Об утверждении Правил применения автоматизированных систем расчетов (Зарегистрировано в Минюсте РФ 13.07.2007 № 9828) [Электронный ресурс]: Приказ Мининформсвязи РФ от 02.07.2007 № 73 – Доступ из справ.-правовой системы «КонсультантПлюс».
59. Об утверждении Правил применения аппаратуры повременного учета продолжительности соединения (Зарегистрировано в Минюсте России 23.04.2008 № 11583) [Электронный ресурс]: Приказ Мининформсвязи России от 08.04.2008 № 38 (ред. от 23.04.2013) 18 – Доступ из справ.-правовой системы «КонсультантПлюс».
60. Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть IV. Правила применения оборудования систем коммутации, включая программное обеспечение и технические средства накопления голосовой информации, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий

(Зарегистрировано в Минюсте России 28.03.2018 № 50536) [Электронный ресурс]: Приказ Минкомсвязи России от 26.02.2018 № 86 – Доступ из справ.-правовой системы «КонсультантПлюс».

61. Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть I. Правила применения оборудования оконечно-транзитных узлов связи сетей подвижной радиотелефонной связи, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий (Зарегистрировано в Минюсте России 13.01.2017 № 45201) [Электронный ресурс]: Приказ Минкомсвязи России от 12.12.2016 № 645 – Доступ из справ.-правовой системы «КонсультантПлюс».
62. Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть III. Правила применения оборудования коммутации и маршрутизации пакетов информации сетей передачи данных, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий (Зарегистрировано в Минюсте России 04.06.2014 № 32560) [Электронный ресурс]: Приказ Минкомсвязи России от 16.04.2014 № 83 – Доступ из справ.-правовой системы «КонсультантПлюс».
63. Об утверждении Правил применения оборудования транзитных, оконечно-транзитных и оконечных узлов связи. Часть XV. Правила применения комбинированных телефонных станций, использующих технологии мультисервисных сетей (Зарегистрировано в Минюсте России 17.04.2017 № 46389) [Электронный ресурс]: Приказ Минкомсвязи России от 21.03.2017 № 129 3 – Доступ из справ.-правовой системы «КонсультантПлюс».
64. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (Зарегистрировано в Минюсте России 14.05.2013 N 28375) [Электронный ресурс]: Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 23.03.2017) – Доступ из справ.-правовой системы «КонсультантПлюс».
65. 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 (Зарегистрировано в Минюсте России 18.08.2014 № 33620) [Электронный ресурс]: Приказ ФСБ России от 10.07.2014 № 378 – Доступ из справ.-правовой системы «КонсультантПлюс».
66. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (Зарегистрировано в Минюсте России 14.05.2013 № 28375) [Электронный ресурс]: Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 23.03.2017) – Доступ из справ.-правовой системы «КонсультантПлюс».

67. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: Постановление Правительства РФ от 01.11.2012 № 1119 – Доступ из справ.-правовой системы «КонсультантПлюс».
68. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: Постановление Правительства РФ от 01.11.2012 № 1119 – Доступ из справ.-правовой системы «КонсультантПлюс».
69. Об утверждении Требований к оборудованию автоматизированной сортировки почты, обеспечивающему выполнение установленных действий при проведении оперативно-розыскных мероприятий (Зарегистрировано в Минюсте России 08.12.2015 № 39997) [Электронный ресурс]: Приказ Минкомсвязи России от 23.07.2015 № 276 – Доступ из справ.-правовой системы «КонсультантПлюс».
70. Об утверждении Требований к оборудованию и программному обеспечению операторов почтовой связи для обеспечения доступа к базам данных об оказанных услугах почтовой связи и пользователях услугами почтовой связи при проведении оперативно-розыскных мероприятий (Зарегистрировано в Минюсте России 10.12.2015 № 40066) [Электронный ресурс]: Приказ Минкомсвязи России от 23.07.2015 № 279 – Доступ из справ.-правовой системы «КонсультантПлюс».
71. Об утверждении Требований к порядку организационно-технического взаимодействия операторов подвижной радиотелефонной связи при обеспечении перенесения абонентского номера (Зарегистрировано в Минюсте России 18.02.2016 № 41140) [Электронный ресурс]: Приказ Минкомсвязи России от 19.01.2016 № 3 – Доступ из справ.-правовой системы «КонсультантПлюс».
72. Об утверждении требований к построению, управлению, нумерации, организационно-техническому обеспечению устойчивого функционирования, условиям взаимодействия, эксплуатации сети связи при оказании универсальных услуг связи [Электронный ресурс]: Приказ Минкомсвязи России от 30.09.2015 № 371 – Доступ из справ.-правовой системы «КонсультантПлюс».
73. Об утверждении требований к сетям электросвязи для проведения оперативно-розыскных мероприятий. Часть III. Требования к сетям телеграфной связи для проведения оперативно-розыскных мероприятий (Зарегистрировано в Минюсте России 06.09.2016 № 43571) [Электронный ресурс]: Приказ Минкомсвязи России от 27.06.2016 № 285 – Доступ из справ.-правовой системы «КонсультантПлюс».
74. Об утверждении Требований к системному проекту сети связи (Зарегистрировано в Минюсте РФ 05.03.2008 № 11288) [Электронный ресурс]: Приказ Мининформсвязи РФ от 13.02.2008 № 18 – Доступ из справ.-правовой системы «КонсультантПлюс».
75. Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования (Зарегистрировано в Минюсте России 22.02.2018 № 50118) [Электронный ресурс]: Приказ ФСТЭК России от 21.12.2017 № 235 – Доступ из справ.-правовой системы «КонсультантПлюс».
76. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (Зарегистрировано в Минюсте России 31.05.2013 № 28608) [Электронный ресурс]: Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) – Доступ из справ.-правовой системы «КонсультантПлюс».

77. Об утверждении формы, формата согласия налогоплательщика (плательщика страховых взносов) на признание сведений, составляющих налоговую тайну, общедоступными, порядка заполнения формы, а также порядка его представления в налоговые органы (Зарегистрировано в Минюсте России 19.12.2016 № 44786) [Электронный ресурс]: Приказ ФНС России от 15.11.2016 N ММВ-7-17/615@ – Доступ из справ.-правовой системы «КонсультантПлюс».
78. Об утверждении формы, формата согласия налогоплательщика (плательщика страховых взносов) на признание сведений, составляющих налоговую тайну, общедоступными, порядка заполнения формы, а также порядка его представления в налоговые органы (Зарегистрировано в Минюсте России 19.12.2016 № 44786) [Электронный ресурс]: Приказ ФНС России от 15.11.2016 № ММВ-7-17/615@ – Доступ из справ.-правовой системы «КонсультантПлюс».
79. Об утверждении формы, формата согласия налогоплательщика (плательщика страховых взносов) на признание сведений, составляющих налоговую тайну, общедоступными, порядка заполнения формы, а также порядка его представления в налоговые органы (Зарегистрировано в Минюсте России 19.12.2016 № 44786) [Электронный ресурс]: Приказ ФНС России от 15.11.2016 N ММВ-7-17/615@ – Доступ из справ.-правовой системы «КонсультантПлюс».
80. Обзор судебной практики по вопросам, связанным с участием уполномоченных органов в делах о банкротстве и применяемых в этих делах процедурах банкротства (утв. Президиумом Верховного Суда РФ 20.12.2016) [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
81. Положение о требованиях к защите информации в платежной системе Банка России (утв. Банком России 24.08.2016 № 552-П) (Зарегистрировано в Минюсте России 06.12.2016 № 44582)) [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
82. Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств (утв. Банком России 09.06.2012 № 382-П) (ред. от 07.05.2018) (Зарегистрировано в Минюсте России 14.06.2012 № 24575) [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
83. Программа «Цифровая экономика Российской Федерации», утв. Распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. – [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 08.08.2018).
84. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014 (принят и введен в действие Распоряжением Банка России от 17.05.2014 № Р-399) [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
85. Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы, утв. Указом Президента Российской Федерации от 09.05.2017 г. № 203. – [Электонный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 08.08.2018).
86. Трудовой кодекс Российской Федерации [Электронный ресурс]: от 30.12.2001 № 197-ФЗ (ред. от 19.07.2018) – Доступ из справ.-правовой системы «КонсультантПлюс».
87. Уголовно-процессуальный кодекс Российской Федерации [Электронный ресурс]: от

18.12.2001 № 174-ФЗ (ред. от 19.07.2018). – Доступ из справ.-правовой системы «КонсультантПлюс».
88. Уголовный кодекс Российской Федерации [Электронный ресурс]: от 13.06.1996 № 63-ФЗ (ред. от 03.07.2018). – Доступ из справ.-правовой системы «КонсультантПлюс».

Судебная практика

89. Апелляционное определение Санкт-Петербургского городского суда от 28.11.2017 № 33-23320/2017 по делу № 2-6415/2017 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
90. Информационное письмо Президиума Высшего арбитражного суда от 13 сентября 2013 г. №146 [Электронный ресурс]. –Доступ из справ.-правовой системы «КонсультантПлюс».
91. Обзор судебной практики Верховного Суда Российской Федерации от 01.03.2006. Обзор судебной практики Верховного Суда Российской Федерации за четвертый квартал 2005 года [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
92. Определение Конституционного Суда Российской Федерации от 2 октября 2003 г. № 345-О [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
93. Определение Конституционного Суда Российской Федерации от 21 октября 2008 г. № 528-О-О [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
94. Определение Конституционного Суда Российской Федерации от 22 ноября 2012 г. № 2192-О [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
95. Определение Конституционного Суда Российской Федерации от 25 января 2018 г. № 189-О [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
96. Определение Конституционного Суда Российской Федерации от 30 сентября 2004 г. № 317-О [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
97. Постановление 9 арбитражного апелляционного суда по делу № А40-14902/16 [Электронный ресурс] // URL: https://kad.arbitr.ru/.
98. Постановление Арбитражного суда Восточно-Сибирского округа от 28 июля 2017 г. № Ф02-3705/2017 по делу № А19-22283/2016 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
99. Постановление ЕСПЧ по делу «Авилкина и другие (avilkina and others) против Российской Федерации» от 6 июня 2013 г. [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
100. Постановление ЕСПЧ по делу Романа Захарова против Российской Федерации от 4 декабря 2015 г. [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
101. Постановление Индустриального районного суда города Хабаровска от 07.12.2016 по делу № 1-863/2016 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».

102. Постановление Конституционного Суда Российской Федерации от 26 октября 2017 г. №25-П [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
103. Постановление Магаданского городского суда Магаданской области от 27.04.2018 № 1-213/2018 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
104. Постановление Президиума суда Ханты-Мансийского автономного округа - Югры от 22.02.2013 № 44Г-7/2013 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
105. Постановление Президиума суда Ханты-Мансийского автономного округа - Югры от 22 февраля 2013 г. № 44Г-7/2013 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
106. Постановление Федерального арбитражного суда Восточно-Сибирского округа от 10 сентября 2010 г. по делу № А33-17361/2009 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
107. Постановление Федерального арбитражного суда Восточно-Сибирского округа от 26 августа 2009 г. по делу № А78-7102/08 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
108. Постановление Федерального арбитражного суда московского округа от 12.03.2014 № Ф05-1622/2014 по делу № А40-56142/13-130-551 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
109. Постановление Федерального арбитражного суда московского округа от 15.01.2014 г. № Ф05-16359/2013 по делу № А40-56844/13-149-539 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
110. Постановление Федерального арбитражного суда московского округа от 23.03.2005, 16.03.2005 № КГ-А40/1704-05 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
111. Постановление Федерального арбитражного суда Московского округа от 12 марта 2014 г. по делу № А40-56142/13-130-551 (МТС и ЦБ РФ) [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
112. Постановление Федерального арбитражного суда Московского округа от 23 марта 2005 г. № КГ-А40/1704-05 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
113. Постановление Федерального арбитражного суда московского округа по делу № А40-56844/13-149-539 от 15 января 2015 [Электронный ресурс] // URL: https://kad.arbitr.ru/.
114. Постановление Федерального арбитражного суда Московского округа по делу № А40-56844/13-149-539 от 15 января 2015 г. (Рамблер и ЦБ РФ) [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
115. Постановление Федерального арбитражного суда Северо-Западного округа от 11 февраля 2014 г. № Ф07-10138/2013 по делу № А05-3725/2013 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
116. Постановление Федерального арбитражного суда Уральского округа от 31 октября 2011 г. № Ф09-6378/11 по делу № А50П-341/2011 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
117. Постановление 9 арбитражного апелляционного суда от 26 апреля 2018 г. по делу № А40-236273/16 [Электронный ресурс] // URL: https://kad.arbitr.ru/.
118. Апелляционное определение Самарского областного суда от 04.05.2016 по делу № 33-

5524/2016 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
119. Постановление 9 Арбитражного апелляционного суда от 6 августа 2014 г. по делу №А40-57559/14 [Электронный ресурс] // URL: https://kad.arbitr.ru/.
120. Определение Верховного Суда Российской Федерации от 27 ноября 2013 г. № 57-АПГ13-7 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
121. Постановление 9 Арбитражного апелляционного суда от 28 ноября 2014 г. по делу № А40-113991/13 – [Электронный ресурс] // URL: https://kad.arbitr.ru/.
122. Постановление 9 арбитражного апелляционного суда от 28 ноября 2013 г. по делу № А40-113991/2013 (Мегафон и ЦБ РФ) [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
123. Постановление Пленума Верховного Суда РФ от 31.10.1995 № 8 (ред. от 03.03.2015) [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
124. Постановление Арбитражного суда Московского округа от 17 апреля 2018 г. № Ф05-4142/2018 по делу № А40-186267/2017 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
125. Постановление Верховного Суда Российской Федерации от 20 апреля 2016 г. № 309-АД16-2859 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
126. Определении Конституционного суда Российской Федерации от 09.06.2005г. № 248-0 [Электронный ресурс] // URL: https://kad.arbitr.ru/.
127. Постановление Арбитражного суда Уральского округа от 17 августа 2016 г. № Ф09-8075/16 по делу № А50-17096/2015 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
128. Постановление Конституционного Суда РФ от 14.05.2003 № 8-П [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
129. Определение Конституционного Суда РФ от 02.10.2003 № 345-О [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
130. Определение Конституционного Суда РФ от 02.10.2003 г. № 345-О [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
131. Определение Конституционного Суда РФ от 14.12.2004 № 453-О [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
132. Определение Конституционного Суда РФ от 21.10.2008 № 525-О-О [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
133. Определение Конституционного Суда РФ от 21.10.2008 г. № 525-О-О [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
134. Постановление ФАС Поволжского округа от 28.04.2012 по делу № А06-3953/2011 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
135. Определение Верховного Суда РФ от 27.11.2013 № 57-АПГ13-7 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
136. Апелляционное определение Омского областного суда от 23.04.2014 по делу № 33-2579/2014 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
137. Постановление ФАС Северо-Западного округа от 29.04.2014 № Ф07-2577/2014 по делу № А66-3211/2013 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».

138. Постановление 9 Арбитражного апелляционного суда от 05 мая 2014 г. по делу № А40-153867/13 – [Электронный ресурс] // URL: https://kad.arbitr.ru/.
139. Постановление 9 Арбитражного апелляционного суда от 05 мая 2014 г. по делу № А 40-153867/13 [Электронный ресурс] // URL: https://kad.arbitr.ru/.
140. Постановление 9 арбитражного апелляционного суда от 05 мая 2014 г. по делу № А 40-153867/13 (Мэйл.Ру и ЦБ РФ) [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
141. Решение Арбитражного суда г. Москвы от 19 мая 2014 г. по делу № 40-28184/14 – [Электронный ресурс] // URL: https://kad.arbitr.ru/.
142. Решение Арбитражного суда г. Москвы от 19 мая 2014 г. по делу № А40-28184/14 [Электронный ресурс] // URL: https://kad.arbitr.ru/.
143. Определение Конституционного Суда РФ от 09.06.2015 № 1275-О [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
144. Постановление Верховного Суда РФ от 27.07.2015 № 305-АД15-7742 по делу № А40-60684/2014 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
145. Постановление Курганского областного суда от 10.08.2015 № 4А-178/2015 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
146. Постановление Курганского областного суда от 10.08.2015 № 4А-178/2015 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
147. Постановление Курганского областного суда от 10.08.2015 № 4А-178/2015 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
148. Проставление Курганского областного суда от 15 августа 2015 г. [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
149. Постановление Курганского областного суда от 18.09.2015 № 4А-255/2015 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
150. Постановление Курганского областного суда от 18.09.2015 № 4А-255/2015 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
151. Решение Хамовнического районного суда города Москвы от 22.03.2016 № 12-590/2016 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
152. Постановление Верховного суда РФ от 30 марта 2016 г. № 82-АД16-1 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
153. Постановление Арбитражного суда Поволжского округа от 31.03.2016 N Ф06-25874/2015 по делу № А65-26711/2014 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
154. Постановление Арбитражного суда Уральского округа от 31.05.2016 N Ф09-4708/16 по делу № А50-21341/2015 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
155. Постановление Верховного Суда РФ от 11.10.2016 № 82-АД16-5 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
156. Постановление Пленума Верховного Суда РФ от 01.06.2017 г. № 19 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
157. Постановление Конституционного Суда РФ от 26 октября 2017 г. № 25-П [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
158. Постановление Конституционного Суда РФ от 26.10.2017 № 25-П [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».

159. Постановление Верховного Суда Российской Федерации от 27 февраля 2013 г. № 32-АД12-4 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
160. Постановление Арбитражного суда Северо-Западного округа от 23 апреля 2018 г. № Ф07-3829/2018 по делу № А56-54459/2017 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
161. Определение Конституционного Суда Российской Федерации от 9 июня 2015 г. № 1275-О [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
162. Определение Конституционного Суда Российской Федерации от 27 июня 2017 г. № 1338-О [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
163. Определение Конституционного Суда Российской Федерации от 27 июня 2017 г. № 1337-О [Электронный ресурс]. –Доступ из справ.-правовой системы «КонсультантПлюс».
164. Апелляционное определение Ставропольского краевого суда от 10.10.2014 по делу № 33-5536/2014 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
165. Апелляционное определение Ставропольского краевого суда от 10.10.2014 по делу № 33-5536/2014 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс» .
166. Определение Верховного Суда Российской Федерации от 12 февраля 2018 г. № 308-КГ17-22368 по делу № А22-3929/2016 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
167. Апелляционное определение Московского городского суда от 16.09.2015 по делу № 33-30344/2015 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».
168. Постановление 8 Арбитражного апелляционного суда от 12 октября 2016 г. по делу № А70-5136/2016 [Электронный ресурс] // URL: https://kad.arbitr.ru/.

Книги

169. Алексеева Д.Г. Банковское право: Учебник. М.: Юристъ, 2007. – 357 С.
170. Волков Ю.В., Вахрушева Ю.Н. Комментарий к Федеральному закону от 7 июля 2003 г. N 126-ФЗ «О связи» [Электронный ресурс] // отв. ред. Л.К. Терещенко. – 2016. – Доступ из справ.-правовой системы «КонсультантПлюс»
171. Козырев А.Н., Макаров В.Л. Оценка стоимости нематериальных активов и интеллектуальной собственности. – М.: Интерреклама, 2003. — 398 С.
172. Либанова С.Э. Особенности возмещения убытков в различных отраслях права. Научно-практическое пособие. – Курган: КГУ, 2013. – 187 С.
173. Северин В.А. Коммерческая тайна в России. 2-е изд., перераб. и доп. — М.: ИКД «Зерцало-М», 2009. — 472 С.
174. Эрделевский А.М. Моральный вред и компенсация за страдания. Научно-практическое пособие. М.: Издательство Век, 1998. – 188 С.

Статьи

175. Arkhipov V., Naumov V., The Legal Definition of Personal Data in the Regulatory Environment of the Russian Federation: Between Formal Certainty and Technological Development // Computer Law and Security Review. Dorchester (UK), 2016. Volume 32. Issue 6. PP. 868-887.
176. Бабкин А.В., Буркальцева Д.Д., Костень Д.Г., Воробьев Ю.Н. Формирование цифровой экономики в России: сущность, особенности, техническая нормализация, проблемы развития // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. – 2017. – Т.10. – №3.
177. Белов А.В. Информационное общество и информационная культура в России: к постановке проблемы // Вестн. Волгогр. гос. Ун-та. Сер. 7, Филос. – 2009. - № 1 (9). – С. 198-199.
178. Вайпан В.А. Основы правового регулирования цифровой экономики // Право и экономика. – 2017. - № 11. – С. 5 – 18.
179. Маркелова К.А. Особенности банковской тайны как правовой категории // Банковское право. М.: Юрист, 2001. – С. 41 – 47.
180. Особенности банковской тайны как правовой категории // Банковское право. М.: Юрист, 2001. – С. 47 - 57.
181. Росенко А.П., Аветисов Р.С. Математическое моделирование вероятного ущерба от утечки конфиденциальной информации в автоматизированной информационной системе. // Доклады ТУСУРа. – 2009. – №1 (19), часть 2. – С. 33 – 35
182. Султанов А.Р. Комментарий к Постановлению Европейского суда по правам человека по делу «Авилкина и другие против Российской Федерации» // Международное правосудие. - 2013. - № 3. - С. 25 – 30.
183. Терещенко Л.К. Отдельные вопросы, возникающие в судебной практике при применении норм о тайне связи [Электронный ресурс] // Комментарий судебной практики / отв. ред. К.Б. Ярошенко. М.: Институт законодательства и сравнительного правоведения при Правительстве РФ, ИНФРА-М, 2016. – С. 127 – 137. – Доступ из справ.-правовой системы «КонсультантПлюс».
184. Федотов Н.Н. Тайна связи против технических средств защиты информации в Интернете [Электронный ресурс] / Н.Н. Федотов // «Форензика – компьютерная криминалистика» [Сайт]. – URL: http://forensics.ru/zi-ts.html#lit05.
185. Юшкевич А.В. Актуальные вопросы соблюдения тайны связи // Правовые вопросы связи. – 2008. – № 1. – С. 26 – 28.

Иные электронные ресурсы

186. Видеонаблюдение и «прослушка» в офисе: мнение Роструда [Электронный ресурс] URL: http://glavkniga.ru/elver/2012/9/640-videonabludenie_proslushka_ofise_mnenie_rostruda.html.
187. Врачебная тайна [Электронный ресурс] // Википедия — свободная энциклопедия [Сайт]. – URL: https://ru.wikipedia.org/wiki/%D0%92%D1%80%D0%B0%D1%87%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F_%D1%82%D0%B0%D0%B9%D0%BD%D0%B0.
188. Кля́тва Гиппокра́та — врачебная клятва, выражающая основополагающие морально-этические принципы поведения врача [Электронный ресурс] // Википедия — свободная энциклопедия [Сайт]. – URL:

https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8F%D1%82%D0%B2%D0%B0_%D0%93%D0%B8%D0%BF%D0%BF%D0%BE%D0%BA%D1%80%D0%B0%D1%82%D0%B0.
189. О некоторых вопросах в сфере трудовых отношений [Электронный ресурс] // Государственная инспекция труда в г. Санкт-Петербург – Доступ из справ.-правовой системы «КонсультантПлюс».
190. Сайт Банка России [Электронный ресурс]. – URL: http://www.cbr.ru/mcirabis/itest/.
191. Селивановский А.С. Банковская тайна: состояние и проблемы [Электронный ресурс] // Авторские курсы А.С. Селивановского [Сайт]. – URL: http://selivanovsky.ru/pages/bankovskaya_tajna/.

ИСТОЧНИКИ В ЧАСТИ СРАВНИТЕЛЬНО-ПРАВОВОГО ИССЛЕДОВАНИЯ ПО РАЗЛИЧНЫМ ЮРИСДИКЦИЯМ И ИНЫЕ ИСТОЧНИКИ

Нормативно-правовые акты и иные официальные документы

192. 15 U.S.C. § 6809(9) [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/uscode/text/15/6809
193. 15 U.S.C. §§ 6801–6809 [Electronic resource] // Legal Information Institute [Site] – URL: https://www.notarylearningcenter.com/pdf/GrammLeachBliley.pdf
194. 15 U.S.C. §1691n [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/uscode/text/15/1691
195. 15 U.S.C. §6802 (b) [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/uscode/text/15/6802
196. 15 U.S.C. §6809(4) [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/uscode/text/15/6809
197. 18 U.S. Code § 2703 - Required disclosure of customer communications or records [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/uscode/text/18/2703.
198. 18 U.S.C. 2511(4)(a) – Interception and disclosure of wire, oral, or electronic communications prohibited [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/uscode/text/18/2511.
199. 26 U.S. Code § 7213 - Unauthorized disclosure of information [Electronic resource] // Cornell Law School [Site]. – URL: https://www.law.cornell.edu/uscode/text/26/7213
200. 26 U.S. Code § 7431 - Civil damages for unauthorized inspection or disclosure of returns and return information [Electronic resource] // Cornell Law School [Site]. – URL: https://www.law.cornell.edu/uscode/text/26/7431
201. 45 CFR § 164.514 (e) [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/cfr/text/45/164.514
202. 45 CFR 160.103 - Definitions [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/cfr/text/45/160.103
203. 45 CFR 164.502(g) [Electronic resource] // Legal Information Institute [Site] – URL: https://www.law.cornell.edu/cfr/text/45/164.502
204. 50 U.S.C. §1861(k)(3) – Access to certain business records for foreign intelligence and international terrorism investigations [Electronic resource] // Legal Information Institute

[Site] – URL: https://www.law.cornell.edu/uscode/text/50/1861.
205. A Declaration on the Promotion of Patients' Rights in Europe. European consultation on the rights of patients. Prepared by WHO dated of 28 June 1994 [Electronic resource] // World Health Organization [Site]. – URL: http://www.who.int/genomics/public/eu_declaration1994.pdf
206. Act on Access to Information Held by Administrative Organs No. 42 of 1999 [Electronic resource]: Japanese Law Translation // Japanese Law Translation [Site]. – URL: http://www.japaneselawtranslation.go.jp/law/detail_main?id=99&vm=2&re=
207. Act on public Health Nurses, Midwives, and Nurses Review [Electronic resource]: adopted in Japan on 30 Jul.1948 // Japanese Law Translation [Site]. – URL: http://www.japaneselawtranslation.go.jp/law/detail/?id=2075&vm=04&re=02
208. Act on the Protection of Personal Information Held by Administrative Organs No. 58 of 2003 [Electronic resource] // Japanese Law Translation [Site]. – URL: http://www.japaneselawtranslation.go.jp/law/detail_main?re=&vm=02&id=131
209. Act on the Protection of Personal Information No. 57 of 2003 [Electronic resource] // Personal Protection Commission of Japan [Site]. – URL: https://www.ppc.go.jp/files/pdf/280222_amendedlaw.pdf
210. Adopting implementing rules concerning data protection at the European Central Bank [Electronic resource]: Decision of the European central bank – 17 April 2007. // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32007D0001(01)&qid=1532761299631.
211. Banking Act – Revised March 31, 2008 [Electronic resource] // Singapore Statutes Online [Site]. – URL: https://sso.agc.gov.sg/Act/BA1970#Sc3-
212. Basic Law for the Federal Republic of Germany [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: http://www.gesetze-im-internet.de/gg/GG.pdf.
213. BSI Act of 14 August 2009 (Federal Law Gazette I p. 2821) [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html.
214. Bundesgerichtshof Urteil vom 24.01.2006, XI ZR 384/03 [Electronic resource] // Bundesgerichtshof [Site]. – URL: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=35317&pos=0&anz=1
215. Cabinet Decision No. (36) of 2017 on the Executive Regulation of Federal Law No. (7) of 2017 on Tax Procedures [Electronic resource] // Federal Tax Authority [Site]. – URL: https://www.tax.gov.ae/pdf/Cabinet-Decision-36-of-2017-on-Executive-Regulation-on-Tax-Procedures.pdf
216. California Consumer Privacy Act of 2018 (CCPA) [Electronic resource] // California Legislative Information [Site]. – URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.
217. Commercial Code of February 15, 1995 (as revised October 26, 2017) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/519122017001/consolide
218. Commissioners for Revenue and Customs Act 2005 [Electronic resource] // Legislation.gov.uk [Site]. – URL: https://www.legislation.gov.uk/ukpga/2005/11/pdfs/ukpga_20050011_en.pdf
219. Competition Act of June 05, 2001 (as revised December 06, 2017) [Electronic resource] // Riigi Teataja [Site]. – URL:

https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/527122017001/consolide
220. Consumer Protection Regulations [Electronic resource]: Regulations by Telecommunications Regulatory Authority (TRA) of 10.01.2017 ver.1.3. // Telecommunications Regulatory Authority [Site]. – URL: https://www.tra.gov.ae/assets/8zJXhCkG.pdf.aspx
221. Credit Institutions Act of February 09, 1999 (as revised May 02, 2018) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523052018002/consolide.
222. Crime (International Co-operation) Act 2003 [Electronic resource] // Legislation.gov.uk [Site]. – URL: https://www.legislation.gov.uk/ukpga/2003/32/contents
223. Data Protection Law [Electronic resource] //: DIFC Law No. 2 of 2007. // Dubai International Financial Centre [Site]. – URL: https://www.difc.ae/files/3615/1739/8803/Data_Protection_Law_DIFC_Law_No._1_of_2007.pdf
224. Data Protection Regulation (DPR) [Electronic resource]: DIFC Consolidated Version No. 3 (in force on 31.01.2018) // Dubai International Financial Centre [Site]. – URL: https://www.difc.ae/files/4515/1745/7405/Data_Protection_Regulations.pdf
225. Declaration on the promotion of patients' rights in Europe – European consultation on the rights of patients Amsterdam 28 – 30 march 1994 – [Electronic resource] // World Health Organization [Site]. – URL: http://www.who.int/genomics/public/eu_declaration1994.pdf
226. Die elektronische Gesundheitskarte [Electronic resource] // Bundesministerium für Gesundheit [Site]. – URL: https://www.bundesgesundheitsministerium.de/themen/krankenversicherung/egk.html#c1058.
227. DIFC Court Law [Electronic resource] //:DIFC Law No. 10 of 2004. // Dubai International Financial Centre [Site]. – URL: https://www.difc.ae/files/1914/5448/9176/Court_Law_DIFC_Law_No.10_of_2004.pdf
228. Directive (EU) No. 2016/943 Of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, Strasbourg, 8.VI.2016 [Electronic resource] // Official Journal of the European Union [Site]. – // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0943&rid=1
229. Directive 95/46/EC - Scope - Publication of personal data on the internet - Place of publication - Definition of transfer of personal data to third countries - Freedom of expression - Compatibility with Directive 95/46 of greater protection for personal data under the national legislation of a Member State [Electronic resource]: Judgment of the court dated November 03, 2003 (Cases C-101/01) // The Court of Justice of The European Union [Site]. – URL: http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=741431.
230. EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation) [Electronic resource]: European Data Protection Supervisor. – Opinion 6/2017 // The European Data Protection Supervisor (EDPS) [Site]. – URL: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf.
231. Electronic Communications Act [Electronic resource]: Riigikogu, December 08, 2004 (as revised May 02, 2018) // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/530052018001/consolide.
232. Employment Contracts Act of December 17, 2008 (as revised June 06, 2018) [Electronic

resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/529062018003/consolide
233. Enterprise Act 2002 [Electronic resource] // Legislation.gov.uk. [Site]. – URL: http://www.legislation.gov.uk/ukpga/2002/40/contents
234. EPIC. Privacy and Human Rights Report 2006 [Electronic resource] // World Legal Information Institute [Site]. – URL: http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Republic-24.html.
235. Estonian Health Insurance Fund Act of June 14, 2000 (as revised December 06, 2017) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/505012018001/consolide
236. European charter of patients' rights – Rome, November 2002 – [Electronic resource] // European Commission [Site]. – URL: http://ec.europa.eu/health/ph_overview/co_operation/mobility/docs/health_services_co108_en.pdf.
237. Federal Data Protection Act (BDSG) of 30 June 2017 [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf
238. Federal Decree Law On Medical Liability [Electronic resource]: Federal Decree Law No.4 of 2016. // Dubai Health Authority [Site]. – URL: https://www.dha.gov.ae/Asset%20Library/MarketingAssets/20180611/(E)%20Federal%20Decree%20no.%204%20of%202016.pdf
239. Federal Law Concerning the Practice of human medicine profession [Electronic resource]: Federal Law No. 7 of 1975. // Dubai Health Authority [Site]. – URL: https://www.dha.gov.ae/Documents/Regulations/Federal%20laws/Federal%20Law%20No.%207-1975%20concerning%20the%20Practice%20of%20Human%20Medicine%20Profession.pdf
240. Federal Law No. (3) of 1987 Promulgating the Penal Code [Electronic resource] // LEGAL ADVICE MIDDLE EAST [Site]. – URL: https://legaladviceme.com/legislation/117/uae-federal-law-3-of-1987-promulgating-penal-code
241. Federal Law of the United Arab Emirates No. (7) of 2017 on Tax Procedures [Electronic resource] // Federal Tax Authority [Site]. – URL: https://www.tax.gov.ae/pdf/Federal-Law-No-7-of-2017-on-Tax-Procedures.pdf
242. Federal Trade Commission 16 CFR Part 314 Standards for Safeguarding Customer Information; Final Rule – May 23, 2002 [Electronic resource] // Federal Trade Commission [Site]. – URL: https://www.ftc.gov/sites/default/files/documents/federal_register_notices/standards-safeguarding-customer-information-16-cfr-part-314/020523standardsforsafeguardingcustomerinformation.pdf
243. Finance Companies Regulation (Central Bank of the UAE) Circular No. 112/2018 of 24.04.2018 [Electronic resource] // Central Bank of Arabian Emirates [Site]. – URL: https://centralbank.ae/en/pdf/notices/FinanceCompaniesRegulation.pdf
244. Financial Institutions and Customer Information: Complying with the Safeguards Rule [Electronic resource] // Federal Trade Commission [Site]. – URL: https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying
245. Financial Instruments and Exchange Act dated June 14, 2006 [Electronic resource]: Financial Services Agency [Site]. – URL: https://www.fsa.go.jp/common/law/guide/gaigin.pdf

246. Genetic Privacy and Non-discrimination Bill 1998 [2002] First Reading [Electronic resource] // Australian Government. The Federal Register of Legislation [Site]. – URL: https://www.legislation.gov.au/Details/C2004B01325
247. German Criminal Code of 13.11.1998 [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/englisch_stgb/.
248. Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen 20.07.200 [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: http://www.gesetze-im-internet.de/ifsg/index.html.
249. Health Data Protection Regulation [Electronic resource]: DHCA Regulation No. 7 of 2013. // Dubai Healthcare City Authority [Site]. – URL: https://dhcr.gov.ae/AboutDHCRDocuments/10-Health%20Data%20Protection%20Regulation.pdf
250. Health Services Organization Act of May 09, 2001 (as revised May 02, 2018) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523052018005/consolide.
251. Human Genes Research Act of December 13, 2000 (as revised February 19, 2014) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/518062014005/consolide.
252. Income Tax Act (Chapter 134) [Electronic resource] // Singapore Statutes Online [Site]. – URL: https://sso.agc.gov.sg/Act/ITA1947#pr6-
253. Internationale Kennungen für mobile Endeinrichtungen [Electronic resource] // Bundesnetzagentur [Site]. – URL: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/TechnischeNummern/IMEI/imei_node.html.
254. Law of Obligations Act of September 26, 2001 (as revised December 13, 2017) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/507022018004/consolide.
255. Ley 9/2014, de 9 de mayo, General de Telecomunicaciones [Electronic resource]: Jefatura del Estado «BOE» núm. 114, de 10 de mayo de 2014 // Agencia Estatal Boletin Oficial del Estado [Site]. – URL: https://www.boe.es/buscar/pdf/2014/BOE-A-2014-4950-consolidado.pdf.
256. Medical Care Act No. 205 of July 30, 1948 [Electronic resource] // Japanese Law Translation [Site]. – URL: http://www.japaneselawtranslation.go.jp/law/detail/?id=2199&vm=04&re=02
257. Medishield Life Scheme Act 2015 [Electronic resource] // Singapore Statutes Online [Site]. – URL: https://sso.agc.gov.sg/Act/MLSA2015#pr27-
258. Mental Health Act of February 12, 1997 (as revised December 09, 2015) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/501022016017/consolide.
259. Ministry of Health Singapore Reflection on Transition [Electronic resource] // Ministry of Health Singapore [Site]. – URL: https://www.moh.gov.sg/content/dam/moh_web/Legislations/Legislation%20And%20Guidelines/HBRA/Reflection%20on%20Transition.pdf
260. Ministry of Health Singapore Summary of Responses to Feedback Received During Public Consultation on Human Biomedical Research Bill [Electronic resource] // Ministry of Health Singapore [Site]. – URL:

https://www.moh.gov.sg/content/moh_web/home/Publications/Reports/2015/summary-of-responses-to-feedback-received-during-public-consult.html
261. Money Laundering and Terrorist Financing Prevention Act of October 26, 2017 [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/521122017004/consolide
262. New version of the law was accepted in 2001: Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10) 26.06.2001 [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/g10_2001/G_10.pdf.
263. Nummernplan Internationale Kennungen für Mobile Teilnehmer vom 06.04.2016 [Electronic resource] // Bundesnetzagentur [Site]. – URL: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/TechnischeNummern/IMSI/IMSI_NP.pdf?__blob=publicationFile&v=3.
264. Occupational Health and Safety Act of June 16, 1999 (as revised June 13, 2018) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/526062018002/consolide
265. On Combating Cybercrimes [Electronic resource]: Federal Decree-Law No. 5 of 2012 // Legal Portal of the United Arab Emirates [Site]. – URL: https://elaws.moj.gov.ae/UAE-MOJ_LC-En/00_PENALTIES%20AND%20CRIMINAL%20MEASURES/UAE-LC-En_2012-08-13_00005_Markait.html?val=EL1
266. On enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society [Electronic resource]: Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – April 25, 2018. // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0233&from=EN.
267. On Organizing The Telecommunications Sector [Electronic resource]: Federal Decree-Law No. 3 of 2003 // Legal Portal of the United Arab Emirates [Site]. – URL: https://elaws.moj.gov.ae/UAE-MOJ_LC-En/00_TELECOMMUNICATIONS/UAE-LC-En_2003-11-15_00003_Markait.html?val=EL1
268. On payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC – Directive (EU) of the European parliament and of the Council – No. 2015/2366 – November 25, 2015 – [Electronic resource] // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366.
269. On retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EC [Electronic resource]: the European parliament and of the Council Directive – № 2006/24/EC. – 15 March 2006 // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006L0024.
270. On the Protection of Medical Data [Electronic resource]: Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 adopted February 13, 1997 // University of Minnesota. Human Rights Library [Site]. – URL: http://hrlibrary.umn.edu/instree/coerecr97-5.html.
271. On the re-use of public sector information – the European parliament and of the Council

Directive – № 2003/98/EC – 17 November 2003 – [Electronic resource] // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:02003L0098-20130717
272. Open Government Data Strategy [Electronic resource] // Prime Minister of Japan and His Cabinet [Site]. –URL: https://japan.kantei.go.jp/policy/it/20120704/text.pdf
273. Personal Data Protection Act 616 SE Draft [Electronic resource] // Riigikogu [Site]. – URL: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/e14c5e2f-b684-4aa4-a7dd-ffb76f63f395/Isikuandmete%20kaitse%20seadus.
274. Personal Data Protection Commission, ADVISORY GUIDELINES FOR THE TELECOMMUNICATION SECTOR – May 16, 2014 [Electronic resource] // Personal Data Commission Singapore [Site]. – URL: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Sector-Specific-Advisory/finalised-advisory-guidelines-on-application-of-pdpa-to-telecom-sector.pdf.
275. Privacy and Human Rights [Electronic resource] // Global Internet Liberty Campaign [Site]. – URL: http://gilc.org/privacy/survey/surveylz.html.
276. Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005 [Electronic resource] // Legislation.gov.uk [Site]. – URL: http://www.legislation.gov.uk/uksi/2005/3181/contents/made.
277. Proposal for a regulation of the European parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC [Electronic resource] : Regulation on Privacy and Electronic Communications. – January 10, 2017 // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0010:FIN.
278. Public Information Act of November 15, 2000 (as revised June 14, 2017) [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/en/eli/514112013001/consolide
279. Regulating Data Dissemination and Exchange in the Emirate of Dubai [Electronic resource]: Dubai Law No. 26 of 2015 // The Supreme Legislation Committee [Site]. – URL: http://ogp.dubai.gov.ae/documants/pdf/ltiwndiymjezmdk.pdf
280. Regulation of Investigatory Powers Act 2000 [Electronic resource]: of the Parliament of the United Kingdom dated of 28.07.2000 // The National Archives [Site]. – URL: http://www.legislation.gov.uk/ukpga/2000/23.
281. Regulatory Framework For Stored Values and Electronic Payment Systems dated of 01.01.2017 [Electronic resource] // Central Bank of The United Arab Emirates [Site]. – URL: https://www.centralbank.ae/en/pdf/notices/Regulatory-Framework-For-Stored-Values-And-Electronic-Payment-Systems-En.pdf
282. Retail Banking Market Investigation Order 2017 [Electronic resource] // Gov.uk [Site]. – URL: https://assets.publishing.service.gov.uk/media/5893063bed915d06e1000000/retail-banking-market-investigation-order-2017.pdf
283. Retail banking market investigation. Final Report [Electronic resource] // Gov.uk [Site]. – URL: https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf.
284. Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung - (Artikel 1 des Gesetzes v. 20. Dezember 1988, BGBl. I S. 2477) [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/sgb_5/__291a.html.
285. Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S.

1074, 1319), die zuletzt durch Artikel 2 des Gesetzes vom 30. Oktober 2017 (BGBl. I S. 3618) geändert worden ist [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/stpo/StPO.pdf.

286. Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU on 6 October 2017 [Electronic resource] // EU2017.EE [Site]. – URL: https://www.eu2017.ee/node/4551.html
287. Telecommunication Business Law No. 25, 1984 [Electronic resource] // Ministry of Internal Affairs and Communications [Site]. – URL: http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/2001TBL.pdf
288. Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 10 Absatz 12 des Gesetzes vom 30. Oktober 2017 (BGBl. I S. 3618) geändert worden ist [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/tkg_2004/TKG.pdf.
289. Terrorism Act 2000 [Electronic resource] // Legislation.gov.uk. [Site]. – URL: http://www.legislation.gov.uk/ukpga/2000/11
290. The Armed Forces and Reserve Forces (Compensation Scheme), Schedule 3 "The tariff and supplementary awards" [Electronic resource] // Pension Appeal Tribunal Scotland [Site]. – // URL: https://www.patscotland.org.uk/sites/default/files/ruleandledg/AFRFCS_Order_2011.pdf
291. The Constitution of Japan [Electronic resource]: Promulgated on November 3, 1946. Came into effect on May 3, 1947 // Official Website of the Prime Minister and His Cabinet [Site] – URL: https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html
292. The Constitution of the Republic of Estonia [Electronic resource]: entered into force of June 28, 1992 (as revised May 06, 2015) // Vabariigi Presidendi Kantselei [Site]. – URL: https://www.president.ee/en/republic-of-estonia/the-constitution/index.pdf.
293. The Constitution of the Republic of Korea [Electronic resource] // WIPO [Site]. – URL: http://www.wipo.int/edocs/lexdocs/laws/en/kr/kr061en.pdf.
294. THE FAIR CREDIT REPORTING ACT [Electronic resource] // U.S. Government Publishing Office [Site]. – URL: https://www.gpo.gov/fdsys/pkg/CFR-2011-title16-vol1/pdf/CFR-2011-title16-vol1-chapI-subchapF.pdf
295. The Federal Financial Institutions Examination Council / Final Guidance on Response Programs Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice – April 1, 2005 [Electronic resource] // Federal Deposit Insurance Corporation [Site]. – URL: https://www.fdic.gov/news/news/financial/2005/fil2705.html
296. THE GRAMM–LEACH–BLILEY ACT [Electronic resource] // U.S. Government Publishing Office [Site]. – URL: https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf
297. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 No. 692 [Electronic resource] // Legislation.gov.uk. [Site]. – URL: http://www.legislation.gov.uk/uksi/2017/692/made#regulation-10-1
298. The Ordinance of the Ministry of Finance No. 10 of March 31, 1982 for Enforcement of the Banking Act. [Electronic resource] // Japanese Law Translation [Site]. – URL: http://www.japaneselawtranslation.go.jp/law/detail/?id=2691&vm=04&re=02
299. The Penal Code of Japan [Electronic resource] // Japanese Law Translation [Site]. – URL: http://www.japaneselawtranslation.go.jp/law/detail/?id=1960&re=02&vm=04
300. The Penal Code of United Arab Emirates [Electronic resource] // Abu Dhabi Judicial

Department [Site]. – URL: https://www.adjd.gov.ae/sites/Authoring/AR/ELibrary%20Books/E-Library/PDFs/Penal%20Code.pdf
301. The Personal Data Protection Act 2012 (PDPA) [Electronic resource] // Personal Data Commission Singapore [Site]. – URL: https://www.pdpc.gov.sg/Legislation-and-Guidelines/Enforcement-of-the-Act.
302. The Privacy, Data Protection and Cybersecurity Law Review, Edition 4. Privacy Law Review [Electronic resource] // The Law Reviews [Site]. – URL: https://thelawreviews.co.uk/edition/1001106/the-privacy-data-protection-and-cybersecurity-law-review-edition-4
303. THE RIGHT TO FINANCIAL PRIVACY ACT [Electronic resource] // U.S. Government Publishing Office [Site]. – URL: https://www.gpo.gov/fdsys/pkg/CFR-2011-title31-vol1/pdf/CFR-2011-title31-vol1-part14.pdf
304. Third Schedule Section 47 Disclosure of information Part I / Further Disclosure Not Prohibited [Electronic resource] // Singapore Statutes Online [Site]. – URL: /https://sso.agc.gov.sg/Act/BA1970?ProvIds=Sc3-#Sc3-
305. TRA Announcement [Electronic resource] // Telecommunications Regulatory Authority [Site]. – URL: http://www.tra.gov.ae/assets/3vyZ23hl.pdf.aspx
306. U.S. Code § 6103 - Confidentiality and disclosure of returns and return information [Electronic resource] // Cornell Law School [Site]. – URL: https://www.law.cornell.edu/uscode/text/26/6103
307. U.S. Code: Title 26 - Internal Revenue Code [Electronic resource] // Cornell Law School [Site]. – URL: https://www.law.cornell.edu/uscode/text/26
308. U.S. Department of Health and Human Services Office for Civil Rights. HIPAA Administrative Simplification – March 2013 – [Electronic resource] // U.S. Department of Health & Human Services [Site]. – URL: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf?language=es
309. Unfair Competition Prevention Act [Electronic resource]: Japanese Law Translation [Site]. – URL: http://www.japaneselawtranslation.go.jp/law/detail_main?id=83&vm=2&re=
310. Verfügung Nr. 33/2016, Amtsblatt Nr. 11/2016 vom 15.06.2016 [Electronic resource] // Bundesnetzagentur [Site]. – URL: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/TechnischeNummern/IMSI/IMSI_exterritNutzung.pdf?__blob=publicationFile&v=1.
311. Директива о конфиденциальности и электронных средствах связи [Электронный ресурс] // директива Европейского парламента и Совета Европейского Союза. – № 2002/58/ЕС – 12.07.2002. – Доступ из справ.-правовой системы «Консультант Плюс»
312. Закон «О налогообложении» Эстонской республики [Электронный ресурс] // Riigi Teataja [Сайт]. – URL: https://www.riigiteataja.ee/en/eli/523012015008/consolide
313. Закон Государства Израиль «Порядок налогообложения подоходным налогом» [Электронный ресурс] // International Center for Not-For-Profit Law [Сайт]. – URL: http://www.icnl.org/research/library/files/Israel/Ordinance.pdf
314. Закон Испании «Об общем налогообложении» [Электронный ресурс] // Agencia Estatal Boletin Oficial del Estado [Сайт]. – URL: http://www.boe.es/buscar/pdf/2003/BOE-A-2003-23186-consolidado.pdf
315. Конвенция о защите прав человека и основных свобод [Электронный ресурс]:

заключена – в г. Риме 04.11.1950 (с изм. от 13.05.2004). – Доступ из справ.-правовой системы «Консультант Плюс»
316. Конвенция о защите прав человека и человеческого достоинства в связи с применением достижений биологии и медицины: Конвенция о правах человека и биомедицине [Электронный ресурс]: заключена в г. Овьедо 04.04.1997 (с изм. от 27.11.2008) – Доступ из справ.-правовой системы «Консультант Плюс»
317. Конвенция о защите физических лиц при автоматизированной обработке персональных данных [Электронный ресурс]: заключена в г. Страсбурге 28.01.1981 (с изм. от 08.11.2001). – Доступ из справ.-правовой системы «Консультант Плюс»
318. Конвенция Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма [Электронный ресурс]: в г. Варшаве 16.05.2005. – Доступ из справ.-правовой системы «Консультант Плюс»
319. Лиссабонская декларация о правах пациента – принята 34-й Всемирной Медицинской Ассамблеей. Лиссабон, Португалия, сентябрь–октябрь 1981 года [Электронный ресурс] // Медицина и право [Сайт]. – URL: http://www.med-pravo.ru/Ethics/LisbonDecl.htm
320. Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения [Электронный ресурс]: Рекомендации ФАТФ – февраль 2012. // The Financial Action Task Force (FATF) [Сайт]. – URL: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Russian.pdf
321. Международный кодекс медицинской этики [Электронный ресурс] // Медицинский сайт MedLinks.ru [Сайт]. – URL: http://www.medlinks.ru/article.php?sid=1630
322. Налоговый кодекс Федеративной Республики Германия [Электронный ресурс] // Bundesministerium der Justiz und für Verbraucherschutz [Сайт]. – URL: https://www.gesetze-im-internet.de/englisch_ao/englisch_ao.html#p0175
323. О доступе к осуществлению деятельности кредитными организациями и пруденциальном надзоре за кредитными организациями и инвестиционными компаниями, вносящая изменения в Директиву 2002/87/ЕС и отменяющая Директивы 2006/48/ЕС и 2006/49/ЕС [Электронный ресурс]: директива Европейского парламента и Совета Европейского Союза. – № 2013/36/ЕС – 26.06.2013. – Доступ из справ.-правовой системы «Консультант Плюс».
324. О защите конфиденциальных ноу-хау и деловой информации (коммерческой тайны) от незаконного приобретения, использования и раскрытия [Электронный ресурс]: директива Европейского парламента и Совета Европейского Союза. – № 2016/943 – 08.06.2016. – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 30.07.2018).
325. 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) [Электронный ресурс]: регламент Европейского парламента и Совета Европейского Союза. – № 2016/679 – 27.04.2016. – Доступ из справ.-правовой системы «Консультант Плюс»
326. О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза [Электронный ресурс]: директива Европейского парламента и Совета Европейского Союза. – № 2016/1148 – 06.07.2016. – Доступ из справ.-правовой системы «Консультант Плюс».
327. О правах пациентов в трансграничном медицинском обслуживании [Электронный

ресурс]: регламент Европейского парламента и Совета Европейского Союза. – № 2011/24/ЕС – 09.03.2011 – Доступ из справ.-правовой системы «Консультант Плюс».
328. О предотвращении использования финансовой системы для целей отмывания денег или финансирования терроризма, об изменении Регламента (ЕС) 648/2012 Европейского парламента и Совета ЕС и об отмене Директивы 2005/60/ЕС Европейского парламента и Совета ЕС и Директивы 2006/70/ЕС Европейской комиссии [Электронный ресурс]: директива Европейского парламента и Совета Европейского Союза. – № 2015/849 – 20.05.2015. – Доступ из справ.-правовой системы «Консультант Плюс»
329. Об информации, сопровождающей переводы денежных средств, и об отмене Регламента (ЕС) 1781/2006 [Электронный ресурс]: регламент Европейского парламента и Совета Европейского Союза. – № 2015/847 – 20.05.2015 – Доступ из справ.-правовой системы «Консультант Плюс».
330. Проект Регламента по состоянию на 4 мая 2018: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC [Electronic resource] // The International Association of Privacy Professionals [Site]. – URL: https://iapp.org/media/pdf/resource_center/Draft-ePriv-Reg-May-2018.pdf.
331. Протокол об Уставе Европейской системы центральных банков и Европейского центрального банка (в редакции Лиссабонского договора от 13 декабря 2007 г.) [Электронный ресурс] // Право Европейского Союза [Сайт]. – URL: http://eulaw.ru/treaties/protoc/4.
332. Уголовный кодекс Испании [Электронный ресурс] // Agencia Estatal Boletin Oficial del Estado [Сайт]. – URL: https://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf
333. Хартия Европейского союза об основных правах [Электронный ресурс]: принята в г. Страсбурге 12.12.2007. – Доступ из справ.-правовой системы «Консультант Плюс»

Судебная практика

334. Barbulescu v. Romania [Electronic resource]: Judgement of the European Court of Human Rights dated September 05, 2017. // Marina Castellaneta [Site]. – URL: http://www.marinacastellaneta.it/blog/wp-content/uploads/2017/09/CASE-OF-BARBULESCU-v.-ROMANIA.pdf.
335. Beschluss des Entscheidungen des Bundesverfassungsgerichts vom. 27.07.2005 – 1 BvR 668/04 [Electronic resource] // Deutschsprachiges Fallrecht (DFR) [Site]. – URL: http://www.servat.unibe.ch/dfr/bv113348.
336. Bundesarbeitsgericht Urteil vom 27.7.2017, 2 AZR 681/16 [Electronic resource] // Bundesarbeitsgericht [Site]. – URL: http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=en&nr=19516.
337. Bundesgerichtshof Urteil vom 12.05.1958, II ZR 103/57 [Electronic resource] // Matthias Prinz Rechtsanwalt [Site]. – URL: https://www.prinz.law/urteile/bgh/II_ZR_103-57.
338. Bundesgerichtshof Urteil vom 21.10.2015 I ZR 51/12 [Electronic resource] // Bundesgerichtshof [Site]. – URL: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2015&anz=179&pos=0&nr=743 46&linked=urt&Blank=1&file=dokument.pdf.
339. BverfG of 11.06.1991 - 1 BvR 239/90 [Electronic resource] // Jurion [Site]. – URL:

https://www.jurion.de/urteile/bverfg/1991-06-11/1-bvr-239_90/?from=1%3A3191944%2C0.
340. BverfG of 13.06.2007 – 1 BvR 1550/03 [Electronic resource] // Jurion [Site]. – URL: https://www.jurion.de/urteile/bverfg/2007-06-13/1-bvr-1550_03_-1-bvr-2357_04_-1-bvr-603_05/.
341. BverfG of 15.12.1983 [Electronic resource] // Telemedicus [Site]. – URL: https://www.telemedicus.info/urteile/Datenschutzrecht/88-BVerfG-Az-1-BvR-209,-269,-362,-420,-440,-48483-Volkszaehlungsurteil.html.
342. Case No. 2-14-5025 [Electronic resource] // Riigi Teataja [Site]. – URL:https://www.riigiteataja.ee/kohtulahendid/otsingutulemus.html?aktiivneTab=KOIK&sort=LahendiKuulutamiseAeg&asc=false&kohtuasjaNumber=&lahendiKpvAlgus=&lahendiKpvLopp=&menetluseKpvAlgus=&menetluseKpvLopp=&kohus=&kohtunik=&annotatsiooniSisu=&menetluseLiik=&lahendiLiik=&ecliNumber=&lahendiTekst=pangasaladus.
343. Case No. 3-2-1-19-17 Swedbank AS-i v.Vladimir Kutšme [Electronic resource] // Riigi Teataja [Site]. – URL: https://www.riigiteataja.ee/kohtulahendid/otsingutulemus.html?aktiivneTab=KOIK&sort=LahendiKuulutamiseAeg&asc=false&kohtuasjaNumber=&lahendiKpvAlgus=&lahendiKpvLopp=&menetluseKpvAlgus=&menetluseKpvLopp=&kohus=&kohtunik=&annotatsiooniSisu=&menetluseLiik=&lahendiLiik=&ecliNumber=&lahendiTekst=pangasaladus.
344. Case number 1999 (Kyo) 2 dated 12 Nov. 1999 [Electronic resource] // Supreme Court of Japan [Site]. – URL: http://www.courts.go.jp/app/hanrei_en/detail?id=459.
345. Case number 2007(Kyo) 23 dated 11 Dec. 2007 [Electronic resource] // Supreme Court of Japan [Site]. - URL: http://www.courts.go.jp/app/hanrei_en/search.
346. Case number: 2006 (Kyo) 21 dated 27 Oct. 2006 [Electronic resource] // Supreme Court of Japan [Site]. – URL: http://www.courts.go.jp/app/hanrei_en/search.
347. Case number: 2008 (Kyo) 18 dated 25 Nov. 2008 [Electronic resource] // Supreme Court of Japan [Site]. – URL: http://www.courts.go.jp/app/hanrei_en/search.
348. Case of Kennedy v. The United Kingdom [Electronic resource]: Judgment of the European Court of Human Rights dated of 18.05.2010 // Council of Europe Portal [Site]. – URL: https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-98473&filename=001-98473.pdf.
349. Case of Liberty and Others v. The United Kingdom [Electronic resource]: Judgment of the European Court of Human Rights dated of 01.07.2008. // Centrum för rättvisa [Site]. – URL: http://centrumforrattvisa.se/wp-content/uploads/2011/03/CASE-OF-LIBERTY-AND-OTHERS-v.-THE-UNITED-KINGDOM.pdf.
350. Commissioner of Taxation v English, Scotishand Australian Bank Ltd dated of 1920 [Electronic resource] // Swarb.co.uk [Site]. – URL: https://swarb.co.uk/commissioners-of-taxation-v-english-scottish-and-australian-bank-limited-pc-2-jan-1920/.
351. Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others [Electronic resource]: Judgment of the Court (Grand Chamber) of April 8, 2014, ECR [2014] I-238 (Joined Cases C-293 & C-594/12) // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CC0293.
352. Judgment of the European court of justice dated July 16, 2015 - Coty Germany GmbH v Stadtsparkasse Magdeburg (C‑580/13) [Electronic resource] // The Court Of Justice Of The European Union [Site]. – URL:

http://curia.europa.eu/juris/celex.jsf?celex=62013CJ0580&lang1=en&type=TXT&ancre=.
353. Judgment of the European court of justice dated April 14, 2016 - Sparkasse Allgäu v Finanzamt Kempten (Case C‑522/14) [Electronic resource] // The Court Of Justice Of The European Union [Site]. – URL: http://curia.europa.eu/juris/document/document.jsf?text=banking%2Bsecrecy&docid=176343&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=173499#ctx1.
354. K LTD v. National Westminster Bank pls. [Electronic resource]: Judgment of Royal Courts of Justice Strand, London dated of 19 July 2006 // BAILII [Site]. – URL: http://www.bailii.org/ew/cases/EWCA/Civ/2006/1039.html.
355. Klass and Others v. Germany [Electronic resource]: Judgement of European Court of Human Rights dated of 6.09.1978 // European Court of Human Rights [Site]. – URL: http://hudoc.echr.coe.int/eng?i=001-57510.
356. La Sala Primera del Tribunal Constitucional [Electronic resource]: Sala Primera. SENTENCIA 26/2018, de 5 de marzo (BOE number 90, of 13 April 2018) // TRIBUNAL CONSTITUCIONAL DE ESPAÑA [Site]. – URL: http://hj.tribunalconstitucional.es/en/Resolucion/Show/25597.
357. La Sala Segunda del Tribunal Constitucional [Electronic resource]: Sala Segunda. SENTENCIA 145/2014, de 22 de septiembre (BOE number 261, of 28 October 2014) // TRIBUNAL CONSTITUCIONAL DE ESPAÑA [Site]. – URL: http://hj.tribunalconstitucional.es/es/Resolucion/Show/24106.
358. Lenz v. Universal Music Corp [Electronic resource]: Seoul High Court 2010 na 35260 (S Korea, October 13, 2010) // Harvard Law Review [Site]. – URL: https://harvardlawreview.org/2016/06/lenz-v-universal-music-corp/.
359. Opinion of Mr Advocate General Cruz Villalón delivered on 16.04.2015. Case C-580/13 Coty Germany GmbH v. Stadtsparkasse Magdeburg. [Electronic resource] // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CC0580.
360. Patrick Breyer v. Bundesrepublik Deutschland [Electronic resource]: Judgement of the Court of Justice of the European Union dated of 19.10.2016 No. C-582/14 // The Court Of Justice Of The European Union [Site]. – URL: http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1116945.
361. Primary Group (UK) Ltd and others v Royal Bank of Scotland Plc and another [2014] EWHC 1082 (Ch) [Electronic resource] // Rosling King [Site]. – URL: https://www.rkllp.com/2014/05/08/may-2014-banking-update/.
362. Radu v. the Republic of Moldova [Electronic resource]: Judgement of the European Court of Human Rights dated July 15, 2014 // European Court of Human Rights [Site]. – URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-142398%22]}.
363. Review of constitutionality of § 50(3) and § 461 (in the wording in force from 26 September 2008 until 9 January 2009) of the Minister of Justice regulation no. 72 of 30 November 2000 “Internal Rules of Prison” [Electronic resource]: Judgment of the Constitutional Review Chamber of the Supreme Court No. 3-4-1-3-09 of June 25, 2009 // Supreme Court of Estonia [Site]. – URL: https://www.riigikohus.ee/en/constitutional-judgment-3-4-1-3-09.
364. Review of the petition of the Chancellor of Justice, submitted under § 142(2) of the Constitution, for the declaration of invalidity of subindent 4 of Part II of the Republic of Estonia Police Act Amendment Act under § Article 152(2) of the Constitution [Electronic resource]: Judgment of the Constitutional Review Chamber of the Supreme Court No. III-

4/A-1/94 of January 12, 1994 // Supreme Court of Estonia [Site]. – URL: https://www.riigikohus.ee/en/constitutional-judgment-iii-4a-194.
365. Seoul Central District Court, 2014godan5110. [Electronic resource] // Supreme Court of Korea [Site]. – URL: https://eng.scourt.go.kr/eng/judiciary/organization/courts3.jsp.
366. Supreme Court of Connecticut. Emily Byrne v. Avery Center for Obstetrics and Gynecology, P.C. (SC 19873) [Electronic resource]: decided: January 16, 2018 // FindLaw for legal professionals [Site]. – URL: https://caselaw.findlaw.com/ct-supreme-court/1885827.html.
367. Supreme Court of Idaho. Peterson v. Idaho First National Bank No.9027 [Electronic resource] // Google Scholar [Site]. – URL: https://scholar.google.ru/scholar_case?case=13922878689066094550&q=Peterson+v.+Idaho+First+National+Bank&hl=en&as_sdt=2006&as_vis=1.
368. Supreme Court of Japan [Electronic resource] // Supreme Court of Japan [Site]. – URL: http://www.courts.go.jp/app/hanrei_en/detail?id=34.
369. Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others [Electronic resource] : Judgment of the European court of justice (Grand Chamber) dated December 21, 2016 (Joined Cases C-203/15 and C-698/15) // The Court Of Justice Of The European Union [Site]. – URL: http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=26020.
370. Tournier v. National Provincol and Union Bank of England [Electronic resource]: Judgment of the Court of Appeal dated of December 17, 1923 // United Settlement [Site]. – URL: http://www.uniset.ca/other/css/19241KB461.html.
371. United Pan-European Communications NV v Deutsche Bank AG [Electronic recourse]: [2000] EWCA Civ 166, [2000] 2 BCLC 461 // BAILII [Site]. – URL: https://swarb.co.uk/united-pan-europe-communications-n-v-v-deutsche-bank-ag-ca-19-may-2000/.
372. Weber and Saravia v. Germany. [Electronic resource]: Judgement of European Court of Human Rights dated of 29.06.2006 // European Court of Human Rights [Site]. – URL: http://hudoc.echr.coe.int/eng?i=002-3235.
373. X v Commission of the European Communities. - Appeal - Member of the temporary staff - Pre-recruitment medical examination - Repercussions of a refusal to undergo an Aids test - Breach of the right of secrecy as regards state of health. [Electronic resource]: Judgment of the Court of 5 October 1994. Case C-404/92 P. // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1533053077430&uri=CELEX:61992CJ0404.
374. Армонас против Литвы (Armonas v. Lithuania) (36919/02) Бирюк против Литвы (Biriuk v. Lithuania) [Электронный ресурс]: Постановление Европейского суда по правам человека от 25.11.2008 (23373/03) // Европейская конвенция о защите прав человека: право и практика [Сайт]. – URL: http://www.echr.ru/documents/doc/2468230/2468230-003.htm.

Книги

375. Booysen S., Neo D. Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres Around the World. - Cambridge University Press, 2017. – 450 P.
376. H. Helmchen, N. Sartorius. Ethics in Psychiatry: European Contributions. [Electronic

resource] // Google books library [Site]. – URL: https://books.google.ru/books?id=70h31egRm40C&pg=PA162&lpg=PA162&dq=European+Standards+on+Confidentiality+and+Privacy+in+Healthcare&source=bl&ots=dIJEFObHan&sig=slG8SHy6Sl9lE8mxviEDVDaJhxA&hl=ru&sa=X&ved=2ahUKEwiC1NLi48PcAhWixKYKHbeVAsAQ6AEwDHoECAcQAQ#v=onepage&q=European%20Standards%20on%20Confidentiality%20and%20Privacy%20in%20Healthcare&f=false.

377. Hao Wang. Protecting Privacy in China: A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China: Book. – Springer-Verlag Berlin Heidelberg, 2011. - P. 120.
378. Kent Roach Comparative Counter-Terrorism Law [Electronic resource] // Google Books Library [Site]. – URL: https://books.google.ru/books?id=0UzzCQAAQBAJ&pg=PA627&lpg=PA627&dq=Wiretapping+Law+singapore&source=bl&ots=VAVeZfSrL-&sig=g4LhzsDGGzEqJa-_BtplMFAuz0s&hl=ru&sa=X&ved=2ahUKEwi6t9DSweDcAhWHBZoKHXoBDdM4ChDoATACegQICRAB#v=onepage&q=Wiretapping%20Law%20singapore&f=false.
379. Yuet Ming Tham The Privacy, Data Protection and Cybersecurity Law Review – Edition 4 [Electronic resource] // The Law Reviews [Site]. – URL: https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151342/singapore.

Статьи

380. A. Barak. Proportionality. Constitutional Rights and their Limitations [Electronic resource]: International Journal of Constitutional Law, Volume 13, Issue 2, 1 April 2015 // Oxford Academic. International Journal of Constitutional Law [Site]. – URL: https://doi.org/10.1093/icon/mov028.
381. B. M. Knoppers. Protecting Data Privacy in Health Services Research [Electronic resource]: Institute of Medicine (US) Committee on the Role of Institutional Review Boards in Health. Services Research Data Privacy Protection. Washington (DC): National Academies Press (US). – 2000 // The National Center for Biotechnology Information [Site]. – URL: https://www.ncbi.nlm.nih.gov/books/NBK222816/.
382. C. Beckett. Big Data: Is the GCC ready? [Electronic resource] // Dentons [Site]. – URL: https://www.dentons.com/en/insights/alerts/2015/april/8/big-data-is-the-gcc-ready.
383. C. Kuner Regulation of Transborder Data Flows under Data Protection and Privacy Law. Past, Present and Future. OECD Digital Economy Papers No. 187. – 2011 [Electronic resource] // OECD [Site]. – URL: https://www.oecd-ilibrary.org/docserver/5kg0s2fk315f-en.pdf?expires=1532886032&id=id&accname=guest&checksum=E42C47589D17B131D70C6FB93AFC436B.
384. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward [Electronic resource] // Northumbria Research Link (NRL) [Site]. – URL: http://nrl.northumbria.ac.uk/34336/.
385. Deutsche Bahn on track for million Euro fine [Electronic resource] // A Trend Micro Blog by Rik Ferguson [Site]. – URL: http://countermeasures.trendmicro.eu/deutsche-bahn-on-track-for-million-euro-fine/.
386. Dr. Khaled El Elmam Health Data De-Identification [Electronic resource] // The

International Association of Privacy Professionals (IAPP) [Site]. – URL: https://iapp.org/media/pdf/knowledge_center/Perspectives_on_Health_Data_De-Identification_final.pdf.
387. E-Health-Gesetzentwurf ist für ULD enttäuschend 16.01.2015 [Electronic resource] // Das Unabhängige Landeszentrum für Datenschutz [Site]. – URL: https://www.datenschutzzentrum.de/artikel/861-E-Health-Gesetzentwurf-ist-fuer-ULD-enttaeuschend.html.
388. Es sind unzweifelhaft Straftaten geschehen 21.10.2009 [Electronic resource] // Suddeutsche Zeitung [Site]. – URL: https://www.sueddeutsche.de/wirtschaft/datenaffaere-bei-der-bahn-es-sind-unzweifelhaft-straftaten-geschehen-1.29461.
389. Fernández M.A. El secreto de las comunicaciones en el proceso penal [Electronic resource] // Universidad Pontificia. Facultad del derecho [Site]. – URL: https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/593/TFG000519.pdf?sequence=1.
390. G. Alahmad, K. Dierickx. What do Islamic institutional fatwas say about medical and research confidentiality and breach of confidentiality? [Electronic Resource] // Wiley Online Library [Site]. – URL: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1471-8847.2012.00329.x.
391. Gina Stevens Privacy Protections for Personal Information Online – April 6, 2011 [Electronic resource] // Federation of American Scientists [Site]. – URL: https://fas.org/sgp/crs/misc/R41756.pdf.
392. Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung Structure and enforcement of data privacy in South Korea [Electronic resource] // The Social Science Research Network [Site]. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2904896.
393. Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges [Electronic resource] // U.S. Department of Health & Human Services [Site]. – URL: https://ncvhs.hhs.gov/wp-content/uploads/2018/05/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf.
394. Islamic Medical Education Resources-03 0106-Medical Confidentiality. Lecture for Year 3 medical students on 25th June 2001 by Professor Omar Hasan Kasule [Electronic resource] // Islamic Medical Education Resources-03 [Site]. – URL: http://omarkasule-03.tripod.com/id695.html.
395. J. Clark Kelso California's Constitutional Right to Privacy [Electronic resource] // Barkeley Law University of California [Site]. – URL: https://www.law.berkeley.edu/wp-content/uploads/2016/12/Kelso-Californias-Constitutional-Right-to-Privacy.pdf.
396. Lee Soo Chye and Alvin Cheng Data protection in Singapore: overview [Electronic resource] // Thomson Reuters Practical Law [Site]. – URL: https://uk.practicallaw.thomsonreuters.com/6-579-6345?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1.
397. M. Telgheder, G. Brower-Rabinowitsch. Big-Data Fear Plagues German Healthcare. 24.04.2016 [Electronic resource] // Handelsblatt Global [Site]. – URL: https://global.handelsblatt.com/companies/big-data-phobia-plagues-german-healthcare-479373.
398. Morales M.R. El regimen constitucional del secreto de las comunicaciones. – Madrid: Civitas, 1995. P. 125 – 142.
399. N. O'Connell. Privacy in a UAE Healthcare Context. February 2014 [Electronic resource] //

AL TAMIMI & CO. [Site]. – URL: https://www.tamimi.com/law-update-articles/privacy-in-a-uae-healthcare-context/.
400. Nigel Cory Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? – May 1, 2017 [Electronic resource] // The Information Technology and Innovation Foundation (ITIF) [Site]. – URL: https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.
401. Orin S. Kerr, Applying the Fourth Amendment to the Internet: A General Approach [Electronic resource] // The Social Science Research Network [Site]. – URL: http://ssrn.com/abstract=1348322.
402. Rodriguez R.B. El secreto de las comunicaciones: tecnologia e intimidada. – Madrid: Mc Graw Hill, 1998.
403. Ruda-Gonzalez A. Who's Afraid of the Big Bad Data? Some Critical Reflections on the Programme to Open Access to Health Data (The Catalan Approach) // Asia Pacific Journal of Health Law & Ethics. – 2017. – Vol. 11. – No. 1. – pp. 61-82.
404. Ruth Plato-Shinar Bank Secrecy in Israel [Electronic resource] // Social Science Research Network [Site]. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427586.
405. Ryan L. Waggoner Privacy of Personal Information in the Financial Services Sectors of the United States and Japan: The Gramm-Leach-Bliley Act and the Financial Services Agency Guidelines [Electronic resource] // Moritz College of Law [Site]. – URL: http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Waggoner.pdf.
406. Urgell A.M. Analisis juriprudenceial del derecho al secreto de las comunicaciones (art. 18.3 C.E.) [Electronic resource] // Diposit de la Recerca de Catalunya [Site]. – URL: https://www.recercat.cat/bitstream/handle/2072/9115/treballrecerca.pdf;jsessionid=C6A2AE06E8DA7C4B7A127B7D6F2BE9A6.recercat1?sequence=1.
407. Vanessa Houlder, Jane Croft Supreme Court rules HMRC breached confidentiality [Electronic resource] / October 19, 2016. // Financial Times [Site]. – URL: https://www.ft.com/content/3db314c4-95f4-11e6-a80e-bcd69f323a8b.
408. Virginia Horniak PRIVACY OF COMMUNICATION - ETHICS AND TECHNOLOGY [Electronic resource] // Mälardalen University Sweden [Site]. – URL: http://www.idt.mdh.se/utbildning/exjobb/files/TR0390.pdf.
409. Vishnevskiy A. Bank Secrecy: a Look at Modern Trends from a Theoretical Standpoint [Electronic resource] / Vishnevskiy A. Право в современном мире. // Право. Журнал Высшей школы экономики [Сайт]. – URL: https://law-journal.hse.ru/data/2016/01/13/1134662079/%D0%B2%D0%B8%D1%88%D0%BD%D0%B5%D0%B2%D1%81%D0%BA%D0%B8%D0%B9.pdf.
410. Waltraut Ritter Open Data in Asia. Knowledge Dialogues, August 2014 [Electronic resource] // Knowledge Dialogues [Site]. – URL: https://knowledgedialogues.files.wordpress.com/2014/07/open-data-asia-09-2014.pdf.
411. Yohei Suda. The Japanese Law on Communications Interception During Criminal Investigations: Translator's Introduction [Electronic resource] // School of Law. University of Washington [Site]. – URL: https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/778/10PacRimLPolyJ067.pdf?sequence=1&isAllowed=y
412. Yuichiro Tsuji. Medical Privacy Issues in Ageing Japan // Australian Journal of Asian Law – 2017. - No.1. – P. 1-18.
413. Постникова Е.В. Некоторые аспекты правового регулирования защиты персональных данных в рамках внутреннего рынка Европейского союза [Электронный ресурс] / Постникова Е.В. Право в современном мире – 2018. // Право. Журнал Высшей школы

экономики [Сайт]. – URL: https://law-journal.hse.ru/data/2018/04/19/1150474169/%D0%BF%D0%BE%D1%81%D1%82%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2%D0%B0.pdf.
414. Султанов А.Р. Комментарий к Постановлению Европейского суда по правам человека по делу «Авилкина и другие против Российской Федерации» // Международное правосудие. – 2013. – № 3. – С. 25-30.

Иные электронные ресурсы

415. A Legal Guide To Privacy And Data Security [Electronic resource] // Minnesota.gov portal [Site]. – URL: https://mn.gov/deed/assets/legal-guide-to-privacy-and-data-security_tcm1045-133708.pdf.
416. About open data portal of Estonia [Electronic resource] // Open data portal of Estonia [Site]. – URL: https://opendata.riik.ee/en/about.
417. American Hospital Association. Statement on a patient's bill of rights [Electronic resource] // Illinois Institute of Technology [Site]. – URL: http://ethics.iit.edu/codes/AHA%201972.pdf.
418. American Society of Appraisers (ASA) Business Valuation Standards Glossary [Electronic resource] // American Society of Appraisers (ASA) [Site]. – URL: http://www.appraisers.org/docs/default-source/discipline_bv/bv-standards.pdf.
419. Anti-money laundering and counter terrorist financing [Electronic resource] // European Commission [Site]. – URL: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing_en.
420. Bank of Scotland's fax blunder leads to fine. [Electronic resource] // BBC News [Site]. – URL: https://www.bbc.com/news/business-23572574.
421. Banking Regulation 2018 Japan [Electronic resource] // Global Legal Insights [Site]. – URL: https://www.globallegalinsights.com/practice-areas/banking-and-finance-laws-and-regulations/japan.
422. Banking statistics. Deutsche Bundesbank [Electronic resource] // Bundesbank [Site]. – URL: https://www.bundesbank.de/Navigation/EN/Service/Reporting_systems/Banking_statistics/banking_statistics.html.
423. Bayanat.ae [Electronic resource] // Bayanat [Site]. – URL: http://data.bayanat.ae/en_GB/dataset?tags=health.
424. Building a European data economy [Electronic resource] // European Commission [Site]. – URL: https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy.
425. Bundesnetzagentur [Electronic resource] – URL: https://www.bundesnetzagentur.de/EN/Home/home_node.html.
426. Circular 10/2017 (BA): Supervisory Requirements for IT in Financial Institutions [Elecrtonic resource] // Bundesanstalt für Finanzdienstleistungsaufsicht [Site]. -URL: https://www.bafin.de/SharedDocs/Downloads/EN/Rundschreiben/dl_rs_1710_ba_BAIT_en.html;jsessionid=FAB34214A16E8EA7AB894DABC37F1AB3.1_cid298?nn=8249098.
427. Compliance with the anti-money laundering directive by cross-border banking groups at group level – Commission Staff Working Paper – Commission of the European Communities – Brussels, 30.6.2009 – [Electronic resource] // European Commission [Site].

– URL: http://ec.europa.eu/internal_market/company/docs/financial-crime/compli_cbb_en.pdf.
428. Comprehensive Guidelines for Supervision of Major Banks [Electronic resource]: Financial Services Agency [Site]. – URL: https://www.fsa.go.jp/common/law/guide/gaigin.pdf.
429. Consolidated FATF Standards on Information Sharing. Relevant excerpts from the FATF Recommendations and Interpretive Notes. Prepared by FATF (updated November 2017) [Electronic resource] // FATF [Site]. – URL: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Consolidated-FATF-Standards-information-sharing.pdf.
430. Court takes side with druggists despite leakage of personal info [Electronic resource] // Korea Biomedical Review [Site]. – URL: http://www.koreabiomed.com/news/articleView.html?idxno=1345.
431. David Case. “We’re Not Gonna Take It!” Significant Changes to Japan’s Trade Secret Protection Law [Electronic resource] // Orrick Blogs [Site]. – URL: https://blogs.orrick.com/trade-secrets-watch/2016/04/18/were-not-gonna-take-it-significant-changes-to-japans-trade-secret-protection-law/.
432. Deutsche Bank 'to pay €800 mln' in Kirch case 13.02.2012 [Electronic resource] // The Local [Site]. – URL: https://www.thelocal.de/20120213/40709.
433. Digital single market [Electronic resource] // European Commission [Site]. – URL: https://ec.europa.eu/commission/priorities/digital-single-market_en.
434. DLA Piper DATA PROTECTION LAWS OF THE WORLD [Electronic resource] // DLA Piper [Site]. – URL: https://www.dlapiperdataprotection.com/index.html#handbook/world-map-section.
435. Dubai Data Classification Framework [Electronic resource] // Dubai Data [Site]. – URL: http://www.dubaidata.ae/pdf/Classification-Framework.pdf.
436. Dubai Data Strategy. Strategic Objectives [Electronic resource] // Dubai Data [Site]. – URL: http://dubaidata.ae/dubai-data-strategy.html.
437. Dubai Open and Shared Data Framework [Electronic resource] // Dubai Data [Site]. – URL: http://dubaidata.ae/pdf/Dubai-Open-Shared-Data-Framework-20170427.pdf.
438. E-Health Law in Germany. March 2016. Taylor Wedding [Electronic resource] // Taylor Wessing [Site]. – URL: https://united-kingdom.taylorwessing.com/synapse/ti-ehealth-law-germany.html.
439. e-Patient portal [Electronic resource] // Patient Portal [Site]. – URL: https://www.digilugu.ee/login?locale=en.
440. EU Open Data Portal [Electronic resource] – URL: http://data.europa.eu/euodp/en/home
441. European Observatory on Counterfeiting and Privacy. Damages in Intellectual Property Rights [Electronic resource] // European Commission [Site]. – URL: http://ec.europa.eu/internal_market/iprenforcement/docs/damages_en.pdf.
442. Exploring Data-Driven Innovation as a New Source of Growth. Mapping the Policy Issues Raised by “Big Data”. Prepared by Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy of OECD dated of 18 June 2013 [Electronic resource] // OECD [Site]. – URL: https://www.oecd-ilibrary.org/docserver/5k47zw3fcp43-en.pdf?expires=1532885941&id=id&accname=guest&checksum=002E2D4F737B29719CBA621F48C50B3E.
443. FATF [Electronic resource] – URL: http://www.fatf-gafi.org/.
444. FCA fines five banks £1.1 billion for FX failings and announces industry-wide remediation

programme [Electronic resource] // Financial Conduct Authority [Site]. – URL: https://www.fca.org.uk/news/press-releases/fca-fines-five-banks-%C2%A311-billion-fx-failings-and-announces-industry-wide.
445. FCA fines former investment banker for sharing confidential information over WhatsApp. [Electronic resource] // Financial Conduct Authority [Site]. – URL: https://www.fca.org.uk/news/press-releases/fine-former-investment-banker-sharing-confidential-information-whatsapp.
446. FCA Handbook [Electronic resource] // FCA Handbook [Site]. – URL: https://www.handbook.fca.org.uk/.
447. Final Notice of FCA for HSBC Bank Plc. [Electronic resource] // Financial Conduct Authority [Site]. – URL: https://www.fca.org.uk/your-fca/documents/final-notices/2014/hsbc-bank-plc.
448. Final Notice of FCA for JPMorgan Chase Bank N.A. [Electronic resource] // Financial Conduct Authority [Site]. – URL: https://www.fca.org.uk/your-fca/documents/final-notices/2014/jpmorgan-chase-bank.
449. Final Notice of FCA for The Royal Bank of Scotland Plc. // Financial Conduct Authority [Site]. – URL: https://www.fca.org.uk/your-fca/documents/final-notices/2014/royal-bank-of-scotland.
450. Final Notice of FCA for UBS AG. [Electronic resource] // Financial Conduct Authority [Site]. – URL: https://www.fca.org.uk/your-fca/documents/final-notices/2014/ubs-ag.
451. Final notices: Citibank N.A. [Electronic resource] // Financial Conduct Authority [Site]. – URL: https://www.fca.org.uk/your-fca/documents/final-notices/2014/citibank-na.
452. Financial Ombudsmen Service. Issue 45. – April 2005. [Electronic resource] // Financial Ombudsmen [Site]. – URL: http://www.financial-ombudsman.org.uk/publications/ombudsman-news/45/45.pdf.
453. Financial Secrecy Index [Electronic resource] // Tax Justice Network [Site]. – URL: https://www.financialsecrecyindex.com/introduction/fsi-2018-results.
454. Financial Services Register [Electronic resource] – URL: https://register.fca.org.uk/.
455. Gematik. Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH [Electronic resource] // Gematik [Site]. – URL: https://www.gematik.de/telematikinfrastruktur/.
456. German State DPA Fines Payment Transaction Provider for Unlawful Transfer of Transaction Data. 12.09.2011 [Electronic resource] // HUNTON Andrews Kurth [Site]. – URL: https://www.huntonprivacyblog.com/2011/09/12/german-state-dpa-fines-payment-transaction-provider-for-unlawful-transfer-of-transaction-data/.
457. Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze vom 21.12.2015 [Electronic resource] // Bundesgesetzblatt [Site]. – URL: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s2408.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s2408.pdf%27%5D__1533657145850.
458. Gesetz über das Kreditwesen (Kreditwesengesetz - KWG) 10.07.1961 [Electronic resource] // Bundesministerium der Justiz und für Verbraucherschutz [Site]. – URL: https://www.gesetze-im-internet.de/kredwg/KWG.pdf.
459. GSMA [Electronic resource] – URL : http://www.gsma.com/.
460. GSME proposals regarding mobile theft and IMEI security dated of June 2003. [Electronic resource] // GSMA [Site]. – URL: https://www.gsma.com/gsmaeurope/wp-content/uploads/2012/03/gsme_proposals_mobile_thefts_imei_security.pdf.

461. Guideline of the Ministry on Internal Affairs On Protection of Personal Information in Telecommunication Business. [Electronic resource] // The Ministry of Internal Affairs and Communications [Site]. – URL: http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/others/110214_1.pdf.
462. Guidelines for cloud service customer data security [Electronic resource]: Prepared by International Telecommunication Union ITU-T X.1641 dated of 07.09.2016 // ITU [Site]. – URL : https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12853&lang=en.
463. Health information beyond HIPPA [Electronic resource] // U.S. Department of Health & Human Services [Site]. – URL: https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf.
464. HIPAA [Electronic resource] // U.S. Department of Health & Human Services [Site]. – URL: https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf.
465. Hiromi Hayashi, Rina Shimada. Data Protection 2018/Japan [Electronic resource]: International Comparative Legal Guides [Site]. – URL: https://iclg.com/practice-areas/data-protection-laws-and-regulations/japan#chaptercontent1.
466. Hogan Lovells, Trade Secrets Global Guide, 2018 [Electronic resource] // Hagan Lovells [Site]. – URL: http://www.hoganlovells.com/en/pdfdownload?page={6CCEEEF4-48E2-4D44-ACE9-A40280A3523D}&p=1.
467. How to report SARs. National Crime Agency [Electronic resource] // National Crime Agency [Site]. – URL: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu/how-to-report-sars.
468. HUGO [Electronic resource] // HUGO [Site]. – URL : http://www.hugo-international.org/.
469. Imagined Futures: Capturing the Benefits of Genome Sequencing for Society. Prepared by HUGO – 2013 [Electronic resource] // HUGO [Site]. – URL: http://www.hugo-international.org/Resources/Documents/CELS_Article-ImaginedFutures_2014.pdf.
470. Informatics and Telematics in Health. Present and Potential Uses. Prepared by WHO – 1988 [Electronic resource] // World Health Organization [Site]. – URL : http://apps.who.int/iris/bitstream/handle/10665/37201/9241561173-eng.pdf?sequence=1&isAllowed=y.
471. Information technology - Security techniques - Code of practice for personally identifiable information protection [Electronic resource]: prepared by International Telecommunication Union ITU-T X.1058 dated of 30.03.2017 // ITU [Site]. – URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13182&lang=en.
472. Inspection of a lawyer's bank account breached his right to professional confidentiality and private life. Press Release issued by the Registrar of the Court [Electronic resource] // European Court of Human Rights [Site]. – URL: https://hudoc.echr.coe.int/app/conversion/pdf?library=ECHR&id=003-5701328-7233297&filename=Judgment%20Sommer%20v.%20 Germany%20-%20inspection%20of%20a%20lawyer%27s%20bank%20account.pdf.
473. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations (amended February 2018) [Electronic resource] // FATF [Site]. – URL : http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.
474. IRS Publication No. 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information (Rev. 3/99) [Electronic resource] // IRS [Site]. – URL: https://www.irs.gov/pub/irs-utl/p1075.pdf.

475. Jail for relationship manager who sold details of bank clients [Electronic resource] // Caveat Emptor Singapore [Site]. – URL: http://caveat-emptor-singapore.blogspot.com/2011/03/jail-for-relationship-manager-who-sold.html.
476. Käsper K. On data retention and Estonia [Electronic resource] // Estonian Human Rights Centre [Site]. – URL: https://humanrights.ee/en/2017/12/data-retention-estonia/.
477. Keeping It Safe: The OECD Guide on the Protection of Confidentiality of Information Exchanged for Tax Purposes [Electronic resource] // OECD [Site]. – URL: http://www.oecd.org/ctp/exchange-of-tax-information/keeping-it-safe-report.pdf.
478. Know Your Customer: Quick Reference Guide [Electronic resource] / Pwc / January, 2013. // PWC [Site]. – URL: https://www.pwc.com/gx/en/financial-services/assets/pwc-kyc-anti-money-laundering-guide-2013.pdf.
479. Kwang Bae Park, Ju Bong Jang The Privacy, Data Protection, and Cybersecurity Law Review – Edition 4 – December, 2017 [Electronic resource] // The Law Reviews [Site]. – URL: https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151290/korea.
480. Legislation and Guidelines of the Financial Services Agency [Electronic resource] // Financial Services Agency [Site]. – URL: https://www.fsa.go.jp/en/refer/legislation/index.html.
481. Management of patient information. Trends and challenges in Member States. – Global Observatory for eHealth series – Volume 6 – 2012 [Electronic resource] // World Health Organization [Site]. – URL: http://apps.who.int/iris/bitstream/handle/10665/76794/9789241504645_eng.pdf?sequence=1.
482. Managing Digital Security and Privacy Risk. Background Report from 2016 Ministerial Meeting on the Digital Economy. Prepared by OECD – 2016 [Electronic resource] // OECD [Site]. – URL: https://www.oecd-ilibrary.org/docserver/5jlwt49ccklt-en.pdf?expires=1532886027&id=id&accname=guest&checksum=6DF302F57942A41C30109715E4BFB08B.
483. National Crime Agency [Electronic resource] // National Crime Agency [Site]. – URL: http://www.nationalcrimeagency.gov.uk/.
484. National eHealth Strategy Toolkit. Prepared by WHO and ITU – 2012 [Electronic resource] // World Health Organization [Site]. – URL : http://apps.who.int/iris/bitstream/handle/10665/75211/9789241548465_eng.pdf?sequence=1&isAllowed=y.
485. OECD [Electronic resource] – URL: https://www.oecd.org/.
486. Omer Tene Systematic Government Access to Private-Sector Data in Israel: Balancing Security Needs with Democratic Accountability [Electronic resource] // Oxford Academic. International Data Privacy Law [Site]. – URL: https://academic.oup.com/idpl/article/2/4/277/676924.
487. Open & Shared Data Framework [Electronic resource] // Dubai Data Manual [Site]. – URL: http://dubaidata.ae/open-and-shared-data-framework.html.
488. Open Banking [Electronic resource]– URL: https://www.openbanking.org.uk/.
489. Open Banking. Guidelines for Read/Write Participants. – March 2018. Version 3.1 [Electronic resource] // Open Banking [Site]. – URL: https://www.openbanking.org.uk/wpcore/wp-content/uploads/Open-Banking-Guidelines-for-ReadWrite-Participants-v3.1.pdf.
490. Open data [Electronic resource] // European Commission [Site]. – URL: https://ec.europa.eu/digital-single-market/en/open-data.

491. Open Knowledge International [Electronic resource] // Open data portal of Estonia [Site]. – URL: https://okfn.org/.
492. Overview of cybersecurity [Electronic resource]: prepared by International Telecommunication Union ITU-T X.1205 dated of 18.04.2008 // ITU [Site]. – URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136.
493. Personal Representatives [Electronic resource] // U.S. Department of Health & Human Services [Site]. – URL: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/personal-representatives/index.html.
494. Privacy in South Korea: overview by Kwang Bae Park and Sunghee Chae, Lee & Ko [Electronic resource] // Thomson Reuters Practical Law [Site]. – URL: https://uk.practicallaw.thomsonreuters.com/6-579-7825?transitionType=Default&contextData=(sc.Default).
495. Privacy Online. OECD Guidance on Policy and Practice. Prepared by OECD – 2003 [Electronic resource] // OECD [Site]. – URL: https://www.oecd-ilibrary.org/science-and-technology/privacy-online_9789264101630-en.
496. Promotion of Open Data Strategies [Electronic resource]: Ministry of Internal Affairs and Communications [Site]. – URL: http://www.soumu.go.jp/menu_seisaku/ictseisaku/ictriyou/opendata/eng/index_e.html.
497. Proposal for a directive of the European parliament and of the Council on the re-use of public sector information (recast) – April 25, 2018 – [Electronic resource] // EUR-Lex Access to European Union law [Site]. – URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0234:FIN.
498. Proposal for a regulation of the European parliament and of the Council on a framework for the free flow of non-personal data in the European Union – September 13, 2017 – [Electronic resource] // European Commission [Site]. – URL: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-framework-free-flow-non-personal-data.
499. R. Cash, D. Wikler, A. Saxena, A. Capron. Casebook on Ethical Issues in International Health Research. Prepared by WHO – 2009 [Electronic resource] // World Health Organization [Site]. – URL: http://apps.who.int/iris/bitstream/handle/10665/44118/9789241547727_eng.pdf?sequence=4&isAllowed=y.
500. Radio-Frequency Identification (RFID) A Focus on Information Security and Privacy. OECD Digital Economy Papers No. 138 dated of 14 January 2008 [Electronic resource] // OECD [Site]. – URL: https://www.oecd-ilibrary.org/docserver/230618820755.pdf?expires=1532885980&id=id&accname=guest&checksum=8C506A504953B560241DFB12428A26C2.
501. Reilly and Schweihs, Guide to Intangible Asset Valuation [Electronic resource] // Willamette [Site]. – URL: http://www.willamette.com/insights_journal/14/autumn_2014_4.pdf
502. Retail banking market investigation [Electronic resource] // Gov.uk [Site]. – URL: https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk#terms-of-reference.
503. Rundschreiben 09/2017 (BA) – Mindestanforderungen an das Risikomanagement – MaRisk [Electronic resource] // Bundesanstalt für Finanzdienstleistungsaufsicht [Site]. – URL: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1709_marisk_ba.html;jsessionid=FAB34214A16E8EA7AB894DABC37F1AB3.1_cid298?nn=8249098.

504. Safety, privacy and security across the mobile ecosystem. Key issues and policy implications. Prepared by GSMA 2017 [Electronic resource] // GSMA [Site]. – URL: https://www.gsma.com/publicpolicy/wp-content/uploads/2017/02/GSMA_Safety-privacy-and-security-across-the-mobile-ecosystem.pdf.
505. SCHUFA [Electronic resource] – URL: https://www.schufa.de/de/.
506. Shawn D. Fox, CPA "Calculating Damages in Misappropriation of Trade Secrets Matters" [Electronic resource] // Willamette [Site]. – URL: http://www.willamette.com/insights_journal/16/spring_2016_2.pdf
507. Smart Dubai [Electronic resource] // Smart Dubai [Site]. – URL: https://smartdubai.ae/en/Pages/default.aspx.
508. Statement on DNA Sampling: Control and Access. Prepared by HUGO Ethics Committee dated of February 1998 [Electronic resource] // HUGO [Site]. – URL: http://www.hugo-international.org/Resources/Documents/CELS_Statement-DNASampling_1998.pdf.
509. Statement on Human Genomic Databases. Prepared by HUGO Ethics Committee dated of December 2002 [Electronic resource] // HUGO [Site]. – URL : http://www.hugo-international.org/Resources/Documents/CELS_Statement-HumanGenomicDatabase_2002.pdf.
510. Statement on Personal Information Protection (Privacy Policy) [Electronic resource] // Bank of America Merrill Lynch [Site]. – URL: http://www.japan.ml.com/privacy/mljs_privacy_e3.asp.
511. Statement on the Principled Conduct of Genetics Research. Prepared by HUGO ELSIC dated of 21.12.1995 [Electronic resource] // HUGO [Site]. – URL : http://www.hugo-international.org/Resources/Documents/CELS_Statement-PrincipledConductofGeneticsResearch_1995.pdf.
512. Statistics [Electronic resource] // Bank of England [Site]. – URL: https://www.bankofengland.co.uk/statistics.
513. Strengthening Health Information Infrastructure for Health Care Quality Governance. Good Practices, New Opportunities and Data Privacy Protection Challenges. Prepared by OECD 2013 [Electronic resource] // OECD [Site]. – URL: https://www.oecd-ilibrary.org/social-issues-migration-health/strengthening-health-information-infrastructure-for-health-care-quality-governance/protection-of-privacy-in-the-collection-and-use-of-personal-health-data_9789264193505-9-en
514. Study on Trade Secrets and Confidential Business Information in the Internal Market. Prepared for the European Commission [Electronic resource] // European Commission [Site]. – URL: http://ec.europa.eu/DocsRoom/documents/27703/.
515. Sugano: International code of conduct for genomic and health-related data sharing. The HUGO Journal 2014 [Electronic resource] // HUGO [Site]. – URL: http://www.hugo-international.org/Resources/Documents/CELS_Article-InternationalCodeofConduct_2014.pdf.
516. The American Institute of Certified Public Accountants (AICPA) Practice Aid 06-4, "Calculating Lost Profits" [Electronic resource] // The American Institute of Certified Public Accountants [Site]. – URL: https://www.aicpa.org/InterestAreas/ForensicAndValuation/Resources/PractAidsGuidance/DownloadableDocuments/PA_064_Excerpt.pdf.
517. The Automatic Exchange of Information (AEOI) portal [Electronic resource] // The Automatic Exchange of Information (AEOI) portal [Site]. – URL: http://www.oecd.org/tax/automatic-exchange/international-framework-for-the-crs/exchange-

relationships/.
518. The Federal Statistical Office [Electronic resource] // Destatis [Site]. – URL: https://www.destatis.de/EN/Homepage.html.
519. The Lending Code. Setting standards for banks, building societies and credit card providers. – March 2011. [Electronic resource] // Landing Standards Board [Site]. – URL: www.lendingstandardsboard.org.uk.
520. The Network and Information Systems Regulations 2018 No. 506 [Electronic resource] // Legislation.gov.uk. [Site]. – URL: https://www.legislation.gov.uk/uksi/2018/506/made.
521. The OECD Privacy Framework – 2013 [Electronic resource] // OECD [Site]. – URL: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
522. The Payment Services Regulations 2017 "Financial Services and Markets" 2017 No. 752 [Electronic resource] // Legislation.gov.uk. [Site]. – URL: http://www.legislation.gov.uk/uksi/2017/752/pdfs/uksi_20170752_en.pdf.
523. The PPC Secretariat Report on Anonymously Processed Information [Electronic resource]: Personal Information Protection Commission of Japan // Personal Information Protection Commission of Japan [Site]. – URL: https://www.ppc.go.jp/en/legal/.
524. The Privacy, Data Protection and Cybersecurity Law Review, Edition 4. Privacy Law Review [Electronic resource] // The Law Reviews [Site]. – URL: https://thelawreviews.co.uk/edition/1001106/the-privacy-data-protection-and-cybersecurity-law-review-edition-4.
525. Third party providers. Open Banking [Electronic resource] // Open Banking [Site]. – URL: https://www.openbanking.org.uk/providers/third-party-providers/.
526. Threats and requirements for protection of personally identifiable information in applications using tag-based identification [Electronic resource]: Prepared by International Telecommunication Union ITU-T X.1171 dated of 20.02.2009 // ITU [Site]. – URL : https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9454&lang=en.
527. U.S. Economic Espionage Act (EEA) [Electronic resource] // Federation of American Scientists [Site]. – URL: https://fas.org/sgp/crs/secrecy/R43714.pdf.
528. UAE Ministry of Health & Prevention [Electronic resource] // Ministry of Health & Prevention. United Arab Emirates [Site]. – URL: http://www.mohap.gov.ae/en/OpenData/Pages/default.aspx.
529. Uniform Trade Secrets Act (UTSA) [Electronic resource] // Uniform Trade Secrets Act (UTSA) [Site]. – URL: http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.
530. What falls under the category of correspondence? [Electronic resource] // Japan Post [Site]. – URL: https://www.post.japanpost.jp/service/about_shinsyo_en.html.
531. WHO guidelines on ethical issues in public health surveillance. Prepared by WHO – 2017 [Electronic resource] // World Health Organization [Site]. – URL: http://apps.who.int/iris/bitstream/handle/10665/255721/9789241512657-eng.pdf?sequence=1&isAllowed=y.
532. World Health Organization [Electronic resource] // World Health Organization [Site]. – URL: http://www.who.int/.
533. А.А. Швец. Методические основы компенсации морального ущерба в Украине [Электронный ресурс] // УВЕКОН ИНТЕЛЛЕКТ [Сайт]. – URL: http://www.uvecon.in.ua/?mod=content&page=pub_5&lang=rus.
534. Банковская тайна и налоговое администрирование в странах Европы (часть 2). Законодательные регулирование института банковской тайны в ЕС и ряде других

европейских стран [Электронный ресурс] // Taurus Group [Сайт]. – URL: http://taurus-group.eu/ru/news/bankovskaya-tajna-i-nalogovoe-administrirovanie-v-stranax-evropy-chast-2/.
535. Глобальная программа кибербезопасности (ГПК) МСЭ. Основа для международного сотрудничества в области кибербезопасности от 04.2008 [Электронный ресурс] // ITU [Сайт]. – URL: http://www.ifap.ru/pr/2008/080908aa.pdf.
536. Кибербезопасность. Международный союз электросвязи [Электронный ресурс] // ITU [Site]. – URL : http://www.un.org/ru/ecosoc/itu/cybersecurity.shtml.
537. Отчет «Борьба с отмыванием денег и борьба с финансированием терроризма. Южная Корея» [Электронный ресурс] // Financial Action Task Force (FATF) [Site]. – URL: http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Korea.pdf.
538. Руководящие указания Международного союза электросвязи по защите информации, позволяющей установить личность, при применении технологии RFID. X.1275. от 17.12.2010 [Электронный ресурс] // ITU [Сайт]. – URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=10441&lang=ru.
539. Эстонский Генный фонд Тартуского Университета [Electronic resource] // Universitas Tartuenis [Site]. – URL: https://www.geenivaramu.ee/ru/estonskiy-gennyy-fond-tartuskogo-universiteta.