ИНСТИТУТ ИССЛЕДОВАНИЙ ИНТЕРНЕТА

ЗАРУБЕЖНЫЙ ОПЫТ

нормативно-правового регулирования деятельности операторов связи в области сбора и хранения данных пользователей телекоммуникационных услуг

(Telecommunications Data Retention Legislation)

в контексте деятельности государственных правоохранительных органов

Москва, 2017

Содержание

ВВЕДЕНИЕ

Сложность правового регулирования отношений в сфере использования интернета объясняется рядом факторов и ключевыми в ряду прочих являются:

- объективный характер технологической инфраструктуры интернета, которая является многоуровневой и именно это обеспечивает трансграничное функционирование и использование интернета;
- круг субъектов использования интернета, поскольку сторонами возникающих отношений являются лица различной юридической природы (физические/юридические лица, субъекты публичного и частного права, субъекты, относящиеся к различным правопорядкам).

В последнее десятилетие правовое регулирование использования интернета в национальном праве расширяется и изменяется, затрагивая, в том числе, сферу отношений, связанных со сбором и хранением данных пользователей телекоммуникационных услуг. При этом способы, формы, методы, порядок, содержание и т.д. правового регулирования отношений, связанных со сбором и хранением данных пользователей, в национальном праве государств – различны.

Различия подходов государств в формировании правового регулирования отношений (и соответствующего закрепления в действующем законодательстве), связанных со сбором и хранением данных пользователей телекоммуникационных услуг во многом обусловлено политико-правовыми приоритетами государств, отражая «разность» понимания природы и сущностных свойств самого интернета, как сложного технологического и социального феномена.

Существующий плюрализм правового регулирования использования интернета в национальном праве непосредственно выражается в закреплении ключевых и системообразующих понятий и терминов, определения их содержательных характеристик. Понятийно-категориальный аппарат правового регулирования формируется в конкретной правовой системе, а его

использование имеет прикладное значение. К примеру, разграничение понятий – «интернет» (*Internet*) и «доступ к интернету» (*Internet access*)[1], их правовая квалификация, – существенным образом влияет на правовое регулирование использования интернета, включая регулирование порядка сбора, использования, обработки и хранения данных пользователей телекоммуникационных услуг, а также их защиту (далее – «Сбор данных пользователей»).

АКТУАЛЬНОСТЬ ИССЛЕДОВАТЕЛЬСКОГО ПРОЕКТА

В настоящее время на развитие отрасли связи, в том числе ниши интернет-провайдеров в РФ оказывает существенное влияние разработка и применение законодательства в области сбора и хранения данных пользователей услуг связи, прежде всего – телекоммуникационных услуг, в том числе передачи данных в сети Интернет. Принятый 6 июля 2016 г. «пакет Яровой» (ФЗ №374, ФЗ №375) обязывает операторов связи и организаторов распространения информации (ОРИ) хранить не только метаданные, но и (до 6 месяцев) непосредственно данные, передаваемые пользователями в рамках телекоммуникационных услуг.

С момента внесения «пакета» в ГД РФ и его принятия операторы связи, крупнейшие ОРИ, иные игроки российской отрасли связи и ИТ, профессиональные объединения и ассоциации, а также представители Минкомсвязи РФ, интернет-омбудсмен и другие публичные фигуры неоднократно жестко критиковали нормы, предписывающие хранение метаданных и данных телекоммуникационных услуг. Многократно отмечалось, что суммарные инфраструктурные затраты операторов связи РФ, неизбежные при выполнении указанной нормы ФЗ-374, даже с учетом предложений по выведению из-под действия закона наиболее «тяжелых» форматов данных (видеоконтент) будут находится в диапазоне от 400 млрд. руб. до 4-5 трлн руб.,

[1] В праве большинства зарубежных государств (страны-члены Европейского Союза, США, Канада, Австралия и т.д.) понятия «интернет» и «доступ к интернету» закреплены, разграничиваются и имеют самостоятельное значение. В российском праве на законодательном уровне отражен иной подход: в законодательстве различного уровня предпочтение отдается использованию эвфемизмов понятия «интернет» – «сеть Интернет», «информационно-коммуникационная сеть», «информационно-коммуникаци-онная сеть Интернет»; понятие «доступ к интернету» не закреплено и используются такие понятия как «доступ к информации», «доступ к сайтам в сети «Интернет»» и т.д.

что сопоставимо либо превышает всю совокупную выручную российской отрасли операторов связи – и приведет к ее коллапсу либо серьезной деградации, а также кратному росту расценок на услуги связи для конечных пользователей.

Тем не менее, несмотря на интенсивную и последовательную работу игроков отрасли по доведению своей позиции до Правительства РФ и других государственных органов, включая законодательную ветвь власти, до сих пор лица, принимающие решения, всерьез не рассматривают возможность радикальной переработки соответствующих статей закона – либо их изъятия путем внесения в пакет изменений отдельным ФЗ. Предметом торга в части статей 13 и 15 ФЗ №374 служит лишь уточнение перечня форматов и сроков хранения данных пользователей телекоммуникационных услуг.

Обзор публичных заявлений лиц, принимающих решения, а также текстов документов, сопровождавших «пакет Яровой» на этапе его внесения и рассмотрения в ГД ФС РФ (пояснительные записки к проекту ФЗ и проч.), позволяет заключить, что тезис о принципиальной необходимости и целесообразности нормы о хранении данных опирается на два допущения:

1. Подобные механизмы являются опробованными и востребованными в мировой практике регулирования отрасли связи и рынка телекоммуникационных услуг в контексте деятельности правоохранительных органов. Например, автор «пакета», депутат ГД ФС РФ Ирина Яровая подчеркивала, что «в иностранном законодательстве то, что мы обсуждаем с точки зрения хранения информации, есть уже давно»[2].
2. Хранение операторами связи данных, передаваемых пользователями в рамках телекоммуникационных услуг, а также хранение метаданных о сеансах предоставления таких услуг эффективно помогает правоохранительным органам успешно решать задачи по борьбе с терроризмом, преступностью и экстремизмом. Так, в пояснительной записке к ФЗ-374 отмечалось, что «предлагаемые законопроектом изменения позволят обеспечить реализацию дополнительных мер по

[2] http://www.vestifinance.ru/articles/72602

защите гражданина и общества от терроризма, а также будут способствовать упреждению указанных преступлений»[3].

Парадоксальная ситуация, сложившаяся вокруг уже принятого «пакета Яровой», состоит в том, что на сегодняшний оба этих утверждения не опираются на доказательную базу и не имеют ни статистических, ни каких-либо иных проверяемых подтверждений в условиях РФ. Открытые источники не содержат информации о когда-либо проводившихся в России исследованиях международного опыта нормативно-правового регулирования в области сбора и хранения данных пользователей телекоммуникационных услуг в контексте деятельности государственных правоохранительных органов – т.е., в англоязычной терминологии, Telecommunications Data Retention Legislation. Какие-либо ссылки на изучение и источники данных по подобному опыту отсутствовали и на стадии рассмотрения законопроекта, и равным образом отсутствуют на сегодняшний день. Таким образом, ни отрасли связи, ни государственным регуляторам, ни законодателям в РФ неизвестно:

a. Применяется ли где-либо за рубежом регулирование, аналогичное «пакету Яровой» в части хранения данных и метаданных телекоммуникационных услуг?
b. В какой степени существующий международный опыт в области Telecommunications Data Retention сопоставим и сходен с российским?
c. Самое главное – насколько, судя по мировому опыту применения, Telecommunications Data Retention востребована и эффективна как метод обеспечения деятельности правоохранительных органов в области борьбы с терроризмом, преступностью и экстремизмом?
d. Какие выводы могут быть сделаны для РФ на основе изучения опыта юрисдикций, в которых регулирование в области Telecommunications Data Retention развивалось в течение относительно длительного периода (5 лет и более)?

Поиском ответов на указанные вопросы обосновывается актуальность настоящей работы.

---

[3] http://asozd2.duma.gov.ru/addwork/scans.nsf/ID/F7056CA18ADE1C1F43257F8E004A6E60/$File/1039149-6_07042016_1039149-6.PDF?OpenElement

СОДЕРЖАНИЕ НОРМАТИВНО-ПРАВОВЫХ ДОКУМЕНТОВ В ОБЛАСТИ СБОРА И ХРАНЕНИЯ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ ТЕЛЕКОММУНИКАЦИОННЫХ УСЛУГ ОПЕРАТОРАМИ СВЯЗИ

Австралия

Основные понятия, услуги и субъекты, подпадающие под законодательство о хранении данных

В Австралии нормативно-правовой режим, создающий требования по обязательному хранению метаданных пользователей телекоммуникационными операторами, включая операторов мобильной связи и интернет-провайдерами (общая категория «поставщики услуг», service providers) был создан в 2015 г. и формируется единственным НПА – Законом 2015 г. о поправках в части хранения данных в Закон о телекоммуникациях (перехвате и доступе) от 1979 г. (Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015, сокращенно TIAADR 2015). Закон TIAADR был принят 13 апреля 2015 г. после примерно годового процесса разработки и обсуждений, прежде всего в целях повышения возможностей и эффективности деятельности органов, уполномоченных в сфере безопасности, а также правоохранительных органов (LEAs) по борьбе с терроризмом и противодействию преступности. Закон формирует единую систему понятийного аппарата, определяет параметры и типы хранения данных, устанавливает сроки хранения, круг государственных органов, имеющих право получать доступ к хранимой поставщиками услуг информации и порядок такого доступа, определяет санкции за неисполнение норм TIAADR, очерчивает круг исключений, не подпадающих под нормы закона, и проч.

Примечательным моментом в разработке и принятии TIAADR 2015 стало параллельное формирование регуляторами (Генеральная Прокуратура, Офис

Координатора по коммуникациям и проч.) целой экосистемы документов, руководств, поясняющих справочных документов и инструкций, облегчающих интерпретацию и понимание норм Закона поставщиками услуг, а также самими правоохранительными органами. Кроме того, регуляторы активно использовали механизм грантов, частично компенсирующих поставщикам услуг расходы на имплементацию требований по хранению данных, и привлекли к разработке такого механизма частные консалтинговые компании (PWC). В результате, несмотря на продолжающуюся критику TIAADR правозащитным сообществом и отсутствие комплексной оценки эффективности внедряемой системы хранения данных, Австралия дает кейс гибкого и достаточно прозрачного регулирования, которое не создало критической нагрузки на бизнес-процессы и темпы развития национальной отрасли телекоммуникаций.

Ключевые понятия и определения в TIAADR 2015

TIAADR 2015 оперирует понятием *коммуникаций (communications)*, определение которого зафиксировано в *Законе о телекоммуникациях (перехвате и доступе) от 1979 г.* (Telecommunications (Interception and Access) Act 1979 (TIA), в который Закон 2015 г. вносит поправки). Согласно данному определению, коммуникации включают в себя «сеанс связи и обмен сообщениями, либо любую составляющую сеанса коммуникации и обмена сообщениями, которые осуществляются:

(a) в форматах:

(i) речи, музыки и иных звуков;

(ii) данных;

(iii) текста;

(iv) визуальных изображений, анимированных либо не анимированных; либо

(v) сигналов; либо

(b)в любом другом формате либо сочетании форматов.

Закон 2015 г. вводит в текст TIA 1979 статью 187A, которая устанавливает обязательства и требования по хранению данных для участников отрасли телекоммуникаций в рамках **3 четко определенных категорий услуг**.

В статье определены обязательства провайдеров услуг *(service providers)* по хранению определенной информации и документов в отношении следующих услуг:

a) услуг по осуществлению коммуникации либо обеспечению возможности для коммуникации, посредством направляемой или ненаправляемой энергии электромагнитного спектра.

b) услуг, предоставляемых поставщиком услуг связи (carrier) или интернет-провайдером (internet service provider).

c) услуг, предоставляемых лицом, которое на территории Австралии владеет либо является провайдером услуг инфраструктуры, обеспечивающей техническую возможность предоставления соответствующей услуги из перечисленных.

В тексте TIAADR 2015 не приводится какое-либо специальное определение понятия «провайдера услуг» (service provider), в отношении которого и действуют все вводимые им требования и обязательства в части хранения данных; также отсутствуют ссылки на какое-либо специальное определение этого термина в других национальных НПА. В свою очередь, в части определения интернет-провайдера (internet service provider) TIAADR 2015 дает отсылку к Дополнению 5 к Закону о службах вещания от 1992 г., согласно которому интернет провайдером признается[4]:

«лицо, которое предоставляет либо предлагает предоставить публичную услугу связи через Интернет (Internet carriage service)».

При этом отдельным пунктом уточняется, что под действие Закона могут подпадать и другие виды услуг, если нормы Закона прямо не исключают их из сферы его действия. Кроме того, устанавливается, что под действие Закона не подпадают услуги теле- и радиовещания, определяемые в соответствии с Законом о службах вещания от 1992 г.

Координатор по коммуникациям (CAC) полномочен заявить, что определенные виды под действие Закона подпадают и иные услуги помимо 3 вышеупомянутых, в том случае, если связанные с ними метаданные

[4] http://www.austlii.edu.au/au/legis/cth/consol_act/bsa1992214/sch5.html

«представляют значительную ценность для правоохранительных органов или государственных структур, уполномоченных в области обеспечения безопасности. По данным на начало 2017 г, прецедентов расширения списка услуг, охватываемых Законом, в рамках такого механизма не было зафиксировано.

Статья 187A.A «Информация, подлежащая хранению», раскрывает детальный перечень категорий и видов подлежащих хранению данных о подпадающих под нормы Закона услугах. Так, описываются **6 базовых категорий данных**:

1. Абонент и учетные записи, сервисы, телекоммуникационные устройства и другие сервисы, относящиеся к соответствующей услуге
2. Источник коммуникации.
3. Конечный адрес коммуникации.
4. Дата, точное время и продолжительность сеанса коммуникации, или подключения к соответствующей услуге.
5. Тип сеанса передачи данных и соответствующей услуги, использованной для подключения в ходе коммуникации.
6. Местонахождение оборудования или канала связи, задействованного для установления соединения в ходе коммуникации.

Наиболее полный и конкретный перечень услуг и соответствующих типов данных и метаданных, подпадающих под нормы Закона 2015 г., приведен на основе текста Закона в Руководстве по хранению данных для провайдеров услуг (Data Retention Guide for Service Providers), которое опубликовал офис Координатора по коммуникациям в июле 2015 г.[5] – **см. Приложение №1**: Сводная таблица категорий данных, подпадающих под требования Закона 2015 г. с детализацией и пояснениями на основе текста Закона. Принципиально важным моментом, однозначно прописанным в тексте Закона, является то, что его требования и нормы **не распространяются на содержание коммуникаций – речь идет исключительно о метаданных коммуникаций.**

[5] https://www.ag.gov.au/NationalSecurity/DataRetention/Documents/DataRetentionGuidelinesForServiceProviders.pdf

Требования к длительности хранения данных

Согласно Статье 187C «Срок хранения информации и документов», провайдеры услуг обязаны хранить обозначенные в Законе данные о коммуникациях в течение н**е менее двух лет**[6]**.** При этом Статьей вводится следующая интерпретация данного промежутка времени:

«начиная с момента, когда соответствующая информация или документ о коммуникациях были созданы; и

(ii) заканчивая истечением 2 лет *с момента закрытия учетной записи, к которой относится соответствующая информация или документ*; или

(b) в иных случаях – промежуток времени:

(i) начиная с момента, когда соответствующая информация или документ о коммуникациях были созданы; и

(ii) заканчивая истечением 2 лет с момента, когда соответствующая информация или документ о коммуникациях были созданы».

Изначально Законом был установлен срок вступления в силу его норм с 13 октября 2015 г. Однако для поставщиков услуг была предусмотрена опция запросить 18-месячную отсрочку, необходимую для обеспечения технической готовности их инфраструктуры к выполнению требований по хранению данных. Условием для предоставления такой отсрочки стала разработка поставщиками услуг Планов по имплементации норм Закона и согласование таких планов с Координатором по коммуникациям.

В итоге, обязательства провайдеров услуг, разработавших и согласовавших с госорганами Планы по имплементации TIAADR 2015 в части хранения данных, вступили в силу 13 апреля 2017 г. В Руководствах и документах, разъясняющих действие Закона для провайдеров услуг, подчеркивается, что Провайдеры услуг не обязаны иметь какие-либо данные, уже хранящиеся в течение 2 лет, на 13 апреля 2017 г. – обязательные сроки хранения начинают отсчитываться с этой даты.

[6] http://www.comlaw.gov.au/Details/C2015A00039, 187C Period for keeping information and documents.

Доступ к хранимым данным

Согласно Закону, правом запрашивать и получать доступ к данным, которые хранят поставщики услуг, наделены 22 государственных органа, включая правоохранительные органы и ведомства, уполномоченные в области обеспечения национальной безопасности, включая:

- Австралийскую службу безопасности и разведки (ASIO);
- Австралийскую федеральную полицию (AFP) и полицейские органы австралийских штатов;
- Австралийское налоговое управление (Australian Taxation Office);
- Австралийскую комиссию по преступности (ACC);
- Независимую комиссию по противодействию коррупции Нового Южного Уэльса (NSW Independent Commission against Corruption (ICAC))
- И другие ведомства.

При этом для указанных ведомств предусматривается механизм доступа к данным, не требующий получения и предоставления судебного ордера (**досудебный механизм**). Единственное исключение, пролоббированное оппозиционной Австралийской лейбористской партией, Закон предусматривает для доступа к данным лиц, осуществляющих профессиональную деятельность в качестве журналистов (либо работодателей таких лиц). Для получения доступа к метаданным таких лиц государственные органы, включая ASIO, должны будут запрашивать ордер у Генерального Прокурора.

Оценка расходов телекоммуникационных провайдеров услуг на хранение данных

Оценка затрат провайдеров услуг на выполнение требований Закона впервые осуществлялась параллельно с его внесением в парламент в 2014 г. в рамках Совместной рабочей группы по имплементации Закона с участием госорганов и отрасли (СРГ). Со-председателями СРГ были назначены секретарь Управления Генерального Прокурора, генеральный директор Австралийской службы безопасности и разведки (ASIO) и Комиссионер Австралийской

федеральной полиции (AFP); от госорганов в СРГ также участвовали секретарь Управления по коммуникациям, директор Австралийский комиссии по преступности. Отрасль телекоммуникаций представлял топ-менеджмент телекоммуникационных провайдеров услуг Telstra и Optus, а также директор Коммуникационного альянса, отраслевой организации, объединяющей более 150 австралийских телеком-провайдеров услуг.

Для выполнения оценки потенциальных затрат провайдеров услуг на имплементацию норм Закона в части хранения метаданных коммуникаций Управление Генпрокурора привлекло компанию Price Waterhouse Coopers (PWC). Ранее, в сентябре 2014 г., до внесения законопроекта в парламент, PWC уже выполняла первичную оценку расходов провайдеров услуг связи на выполнение прописанных в Законе требований в части хранения. По итогам выполнения задания СРГ PWC предоставила отчет 11 декабря 2014 г.

Согласно проведенным компанией расчетам, предварительные капитальные затраты имплементации Закона в части хранения метаданных оценивались в диапазоне ***от 188.8 до 319.1 млн долл.****.*

Параллельно с изучением отчета PWC на площадке Совместного парламентского комитета по разведке и безопасности (PJCIS) состоялись обсуждения вопроса оценки затрат на исполнение Закона с участием различных представителей отрасли, включая телекоммуникационных провайдеров услуг Optus и Vodafone, а также Австралийскую координационную сеть потребителей коммуникационных услуг (ACCAN). По итогам этих обсуждений PJCIS сформулировал и озвучил ряд рекомендаций:

- Федеральному правительству Австралии рекомендовалось обеспечить существенные взносы для покрытия расходов телеком-провайдеров на имплементацию норм Закона в части хранения данных.
- Особое внимание рекомендовалось уделить обеспечению калибровки и соблюдению баланса в линейке формируемых Законом требований с учетом различного размера, объема финансовых ресурсов и разных бизнес-моделей участников отрасли, подпадающих под действие Закона.

- В частности, отмечалась недопустимость создания вводимыми Законом требованиями чрезмерной финансовой нагрузки на деятельность малых провайдеров телекоммуникационных услуг и нарушения их бизнес-процессов.

По итогам оглашения рекомендаций Совместного парламентского комитета федеральный казначей Джо Хоки 12 мая 2015 г. заявил, что правительство Австралии выделит в общей сложности 131 млн долл. на поддержку телеком-провайдеров услуг в рамках имплементации последними требований Закона по хранению данных. При этом представители частной отрасли телеком-провайдеров неоднократно критиковали правительственные оценки и называли их заниженными.

Программа государственных грантов для отраслевых организаций для обеспечения хранения данных (DRIGP)

Систематизированным ответом австралийского правительства на отраслевую, правозащитную и медийную критику высокой стоимости исполнения норм Закона для провайдеров телекоммуникационных услуг стал запуск механизма финансовой поддержки отраслевых организаций. Таким механизмом стала *Программа грантов для отрасли на обеспечения хранения данных (DRIGP),* разработанная государственными регуляторами с учетом исследований и разработок частных консалтинговых компаний. В декабре 2015 г. Управление Генерального Прокурора опубликовало Руководство пользователя по *DRIGP*[7]. В январе 2016 г. Управление промышленности, инноваций и науки совместно с Управлением Генерального Прокурора также опубликовали Руководство пользователя по *DRIGP*[8].

Модель и основные параметры программы были разработаны Price Waterhouse Coopers в рамках исследования, также содержащего в себе

[7] https://www.ag.gov.au/NationalSecurity/DataRetention/Documents/DataRetentionIndustryGrantsProgrammeGuidelines.pdf

[8] https://webcache.googleusercontent.com/search?q=cache:HZ0sQfABbX8J:https://www.business.gov.au/~/media/Business/DRIGP/Data-Retention-Industry-Grants-Programme-Customer-Information-Guide-WORD.docx%3Fla%3Den+&cd=1&hl=en&ct=clnk&gl=ru

регрессионную систему баллов и коэффициентов для установления конкретных сумм возмещения расходов провайдера услуг в зависимости от:

- Масштаба бизнеса (Enterprise Scale) – до 25 баллов из 100.
- Анализа ожидаемой стоимости хранения данных и других параметров, указанных в заявке на участие в программе грантов – 75 баллов из 100, включая:
    - Число услуг, подпадающих под требования Закона в части хранения данных.
    - Виды и категории таких услуг.
    - Количество подписчиков (пользователей) соответствующих услуг.
    - Суммарная выручка компании за последний финансовый год.
    - Предполагаемый объем данных, подлежащих хранению, на момент вступления в силу нормы Закона (13 апреля 2017 г.).

Общая идеология регрессионной модели PWC состояла в том, чтобы повышать долю компенсируемых затрат прежде всего малым поставщикам, не обладающим серьезными финансовыми ресурсами.

Некоторые примечательные правила в части параметров финансирования, утвержденные в рамках программы:

- Максимальный размер гранта составляет ***80% от оценочной суммы расходов провайдера услуг***, указанной им в заявке на участие в грантовой программе, если такая сумма была одобрена регулятором в рамках рассмотрения заявки.
- Минимальный размер гранта составляет **10 тыс. долл.**[9]. При этом с целью поддержки малых провайдеров услуг в части имплементации норм Закона на минимальную сумму грантов не распространялось ограничение по процентной доле от оценки провайдером услуг суммы его расходов. Т.е в тех 3 случаях, когда были одобрены выплаты по программе грантов малым провайдера услуг на сумму 10 тыс. долл., доля этих средств от оценочной суммы расходов этих конкретных провайдеров услуг могла превышать (и превышала) 80%.

[9] https://www.ag.gov.au/NationalSecurity/DataRetention/Documents/data-retention-grant-allocation-methodology-report.PDF

- В процентном отношении минимальная доля оценочных расходов на хранение данных, компенсируемых провайдеру услуг в рамках грантовой программы, **составила 47%**.

Целью выделения средств провайдера услуг в рамках Программы **не является** полное возмещение затрат, связанных с имплементацией провайдера услуги требований Закона в части хранения данных. Задача формулируется иначе – обеспечение финансовых стимулов для провайдеров с целью обеспечить выполнение ими требований Закона в части хранения данных.

Программа была оформлена в виде единственного раунда финансирования телекоммуникационных провайдеров по итогам приема от них заявок на такое финансирование – опять же, в рамках единственного раунда подачи заявок. Прием заявок на получение грантов в рамках программы был открыт с 7 января по 23 февраля 2016 г. По состоянию на август 2016 г. в рамках программы было распределено 180 грантов, **общий утвержденный объем государственной поддержки отраслевым организациям составил 128,4 млн долл.**[10]. Средний размер гранта не превышает 300 тыс. долл., однако крупные телекоммуникационные провайдеры получили более значительные гранты. Крупнейшими по объему выделенных средств получателями грантов стали Telstra Corporation Ltd (39,915,538 долл.) и Vodafone Hutchison Australia Pty Ltd (28 848 519 долл.)[11].

По данным PWC, за все время действия программы помимо 180 поданных и одобренных заявок 15 заявок были забракованы Управлением Генпрокурора в процессе оценки, а еще 15 заявок были отозваны самими заявителями на разных этапах их подачи и рассмотрения. Таким образом, суммарное число заявок, поданных в рамках DRIGP, составило **2 1 0** – что достаточно точно совпадает с оценкой общего количества провайдеров услуг телекоммуникационных услуг в Австралии. При этом участие в программе грантов может накладывать на провайдеров услуг дополнительные требования согласно соглашению о финансировании (funding agreement). Провайдеры услуг обязаны были выполнить прописанные в соглашении условия к тому же сроку, к которому требовалось начать выполнение закона в части хранения данных – **13**

[10] https://www.ag.gov.au/NationalSecurity/DataRetention/Documents/DRIGP-recipients.pdf
[11] Там же.

апреля 2017 г. В условиях грантовой программы особо подчеркивается, что положения конкретных соглашений о финансировании не отменяют необходимость выполнить требования самого Закона к указанному сроку.

Сводная таблица категорий данных, подпадающих под требования Закона 2015 г. с детализацией и пояснениями на основе текста Закона

Общая категория подлежащей хранению информации	**Описание и категории подлежащей хранению информации**	**Пояснение**
1. Абонент и учетные записи, сервисы, телекоммуникационные устройства и другие сервисы, относящиеся к соответствующей услуге	Данная категория включает в себя: (a) любую информацию, которая относится к одной из нижеследующих категорий: i) любая информация об имени и адресе; ii) любая другая информация, используемая для целей идентификации; информация, относящаяся к соответствующей услуге, если такая информация используется провайдером услуги для идентификации ее подписчика; (b) любая информация, относящаяся к любому контракту, соглашению или договоренности в отношении соответствующей учетной записи, сервису или устройству; (c) любую информацию, которая включает какие-либо или все из нижеследующих категорий: (i) данные биллинга и	Данная категория включает в себя данные, идентифицирующие клиента услуги, в том числе его имя и адрес. Сюда также относятся контактные данные, такие как телефонный номер и адрес электронной почты. Эта информация позволяет государственным органам подтвердить идентичность подписчика услуги или соотнести с тем или иным конкретным пользователем сервис или учетную запись. Также к данной категории относятся данные о сервисах, закрепленных за учетной записью, такие как уникальный идентифицирующий номер, закрепленный за мобильным телефоном, или IP-адрес (или IP-адреса), присвоенные аккаунту или услуге доступа в Интернет. Эта категория также включает в себя данные биллинга и информацию о платежах. Информация о статусе услуги может включать в себя данные о том, когда была активирована и ли отключена соответствующая учетная запись, подключена, отключена или в конкретный момент времени находилась в роуминге соответствующая услуга, либо когда телекоммуникационное устройство было похищено. Под фразами «любая информация» и «любые идентификаторы» подразумевается информация, которую получает или создает провайдер услуги и которая подпадает под параметры, описываемые после этих фраз. Если провайдер услуги не обладает информацией, которая соответствует таким параметрам, в том числе в силу того, что такая информация не относится к соответствующей услуге, то хранения какой-либо информации не требуется. Например, если сервис-провайдер предлагает

Общая категория подлежащей хранению информации	Описание и категории подлежащей хранению информации	Пояснение
	информация о платежах; (ii) контактная информация, относящаяся к соответствующей услуге, если такая информация используется провайдером услуги при ее предоставлении; (d) любые идентификаторы, относящиеся к соответствующей услуге или любой связанной с ней учетной записи, сервисе или устройстве, если такая информация используется провайдером услуги в отношении такой услуги, либо любой связанной с ней учетной записи, сервиса или устройства. (e) статус соответствующей услуги или связанной с ней учетной записи, сервиса или устройства	бесплатную услугу и таким образом не получает данные биллинга, то от него не требуется обеспечивать хранение данных биллинга по соответствующей услуге. При этом провайдер услуги должен будет обеспечивать хранение данных о пользователе услуги и совершенных транзакциях. От провайдеров услуг не требуется обеспечивать сбор и хранение паролей, PIN-кодов, секретных вопросов и кодов токенов, которые используются в целях аутентификации и авторизации.
2. Источник коммуникации	Идентификаторы участвующего в сессии коммуникации аккаунта, сервис или устройство с которого осуществляется коммуникация или была предпринята попытка осуществить коммуникацию, должны быть переданы при помощи соответствующих технических средств	Идентификаторы источника коммуникации могут включать в себя, но не ограничиваются: • телефонный номер абонента, номер международного идентификатора мобильного абонента (IMSI), номер международного идентификатора мобильного оборудования (IMEI), с которого был осуществлен звонок или отправлено СМС. • идентифицирующие данные (такие как имя пользователя, адрес, номер) учетной записи, сервиса или устройства с которого осуществлялась коммуникация в форматах текстовых, голосовых или мультимедийных данных. Примеры включают сообщения электронной почты, данные VoIP, мгновенные сообщения или коммуникацию в видеоформате). • IP-адрес и номер порта, присвоенный подписчику услуги или устройству, подключенному к Интернету во время сеанса коммуникации.

Общая категория подлежащей хранению информации	Описание и категории подлежащей хранению информации	Пояснение
		• любой другой идентификатор сервиса или устройства, известный провайдеру услуги и позволяющий уникальным образом идентифицировать источник коммуникациих. Во всех случаях для определения точного адреса доставки коммуникации провайдеры услуг обеспечивают хранение только тех идентификаторов, которые непосредственно относятся к той или иной конкретной услуге.
3. Конечный адрес коммуникации	Идентификаторы учетной записи, телекоммуникационного устройства или соответствующего сервиса, на которые: a) была осуществлена коммуникация, или; b) были осуществлены перенаправление, маршрутизация или трансфер коммуникации, либо предпринята попытка таких действий.	Параграф 187A(4)(b) Закона однозначно определяет, что провайдеры услуги не обязаны хранить информацию по истории поиска своих абонентов в веб-браузерах. Конечным адресом коммуникации является получатель коммуникации. Идентификаторы конечного адреса коммуникации могут включать в себя (но не ограничиваться): • номер телефона, на который был осуществлен звонок или отправлено СМС • идентифицирующие параметры (имя пользователя, адрес или номер) аккаунта, сервиса или устройства, на которое доставляются текстовые, голосовые или мультимедийные данные. Примеры включают электронные письма, данные IP-телефонии (VoIP), мгновенные сообщения мессенджеров или данные в видеоформате) • IP-адрес, присвоенный подписчику или устройству, подключенному к Интернету на момент получения коммуникации, либо любой другой идентификатор сервиса или устройства известный провайдеру услуг и позволяющий обеспечить уникальную идентификацию конечного адреса коммуникации. В отношении услуг доступа, Закон однозначно исключает из перечня подлежащей хранению информации историю поиска в веб-браузере или любые данные, которые могут к ней приравниваться (например, URL-адрес или IP-адрес, к которому обращался пользователь в процессе поиска через браузер). Во всех случаях для определения точного конечного адреса коммуникации Провайдеры услуг обеспечивают хранение только тех идентификаторов, которые непосредственно относятся к тому или иному

Общая категория подлежащей хранению информации	Описание и категории подлежащей хранению информации	Пояснение
		конкретному сервису. Если конечный адрес коммуникации технически не может быть установлен провайдером услуги, провайдер только обеспечить хранение только последнего известного ему адреса коммуникации.
4. Дата, точное время и продолжительность сеанса коммуникации, или подключения к соответствующей услуге	Дата и точное время (включая временной пояс) следующих событий, характеризующих сеанс коммуникации (с достаточной точностью для однозначной идентификации сеанса коммуникации): a) Начало сеанса коммуникации b) Окончание сеанса коммуникации c) Подключение к соответствующей услуге d) Отключение от соответствующей услуги	В отношении телефонных звонков речь идет лишь о времени начала и завершения звонка. В отношении сеансов коммуникации через Интернет речь идет о временных характеристиках подключения устройства или учетной записи к сети коммуникации и отключения от нее по завершении сеанса. В данном случае временной промежуток между двумя событиями может варьироваться от нескольких часов до нескольких дней, недель, или более продолжительного периода времени, в зависимости от параметров и функциональных характеристик рассматриваемого сервиса.
5. Тип сеанса передачи данных и соответствующей услуги, использованной для подключения в ходе коммуникации.	Следующие категории: a) тип сеанса коммуникации; Примеры: голосовая связи, СМС, электронная почта, текстовый чат, онлайн-форум, социальные медиа. b) тип соответствующей услуги; Примеры: ADSL, Wi-Fi, IP-телефония (VoIP), кабельное соединение, GPRS, VoLTE, LTE. c) функции (режимы) соответствующей услуги, которые были использованы или которые были бы использованы для осуществления коммуникации. Примеры: ожидание звонка, переадресация	Тип средств связи и формат коммуникации (например, голосовой звонок или передача данных через Интернет). Тип соответствующей услуги (пункт 5(b)) обеспечивает больше технических подробностей об услуге. Например, в отношении услуги коммуникации в формате передачи мобильных сообщений, уточняется, используется ли услуга СМС или ММС. Объем потребления данных применительно к услугам доступа в Интернет характеризует объем данных, загруженных либо скачанных подписчиком услуги. Данная информация может измеряться для каждого сеанса коммуникации, либо в рамках системы метрик, применимой для оказания и биллинга соответствующей услуги, например ежедневно или ежемесячно. Примечание: Данный пункт применяется только в отношении провайдеров услуг, предоставляющих соответствующие услуги. Более подробно этот вопрос освещается в параграфе 187A(4)(c).

Общая категория подлежащей хранению информации	Описание и категории подлежащей хранению информации	Пояснение
	звонка, объем использованных данных	
6. Местонахождение оборудования или канала связи, задействованного для установления соединения в ходе коммуникации	Включаются следующие категории, относящиеся к оборудованию или каналам связи, используемым для отправки или получения коммуникации: a) местонахождение оборудования или канала связи, с которых инициируется передача данных; b) местонахождение оборудования или канала связи, которые выступаю конечной точкой коммуникации. Примеры: вышки сотовой связи, точки доступа к Wi-Fi.	Записи о местонахождении ограничены местонахождением устройства в момент начала и окончания сеанса коммуникации – например, телефонного звонка или СМС-сообщения. В отношении услуг фиксированной коммуникации (например, услуга ADSL) данное требование может быть выполнено путем хранения адреса подписчика услуги. Параграфом 187A(4)(e) Закона устанавливается, что записи о местонахождении ограничиваются той информацией, которую провайдер услуги использует при оказании соответствующей услуги. Например, данная формулировка включает в себя информацию о том, к какой вышке сотовой связи, точке доступа к WiFi или базовой станции подключалось устройство в момент начала и окончания сеанса коммуникации. Провайдеры услуг не обязаны хранить записи данных реального времени, записи данных в длящемся режиме, а также данные точного пространственного местонахождения, такие как длящиеся данные местонахождения устройства, определяемого по GPS. Подобные ограничения должны гарантировать, что записи данных местонахождения устройств, которые хранят провайдеры услуг, не будут использоваться для постоянного наблюдения либо отслеживания устройств.

США

Общие правовые особенности

В отличие от большинства других государств в выборке исследования, в США отсутствует единая политика и комплекс НПА, регулирующих хранение данных (в значении data retention). Отсутствует единый комплекс законодательных норм и подзаконных актов, который бы устанавливал обязательные требования государства к телекоммуникационным операторам в части записи и хранения тех или иных категорий данных и метаданных, в том виде, в котором аналогичные правовые механизмы существуют в европейских государствах и (до 2014 г.) существовали на уровне ЕС в рамках Директивы 2006/24/ЕС. Вместо этого имеет место практика ***со****хранения* данных (data preservation). В рамках data preservation провайдеры телекоммуникационных услуг, включая интернет-провайдеров, мобильных операторов и операторов услуг фиксированной телефонной связи самостоятельно определяют сроки, правила и процедуры хранения данных своих пользователей/клиентов, которые могут быть затребованы у них госорганами на основании административного постановления (administrative order) или иного механизма.

Важную роль в формировании такой схемы сыграл тот факт, что в США телекоммуникационные операторы являются компаниями частного сектора, т.е. субъектами частного права. При этом такие субъекты существуют в условиях законодательного федерализма и необходимости соблюдать одновременно федеральное законодательство США и законы штатов. При этом даже на федеральном уровне требования государства к субъектам частной отрасли носят «мозаичный» характер: существующие НПА, которые включают те или пункты, предписывающие раскрытие телекоммуникационными провайдерами данных об их пользователях, не сведены в единую систему и в ряде случаев развиваются (через механизмы поправок и проч.) де факто параллельно друг другу. Такая ситуация опять же способствует тому, что принятие решения о формировании единых правил и технических политик сохранения данных «выталкивается» в поле ответственности самого оператора.

Наконец, третья ключевая особенность американского подхода состоит в том, что параллельно политикам data preservation в отношении телекоммуникационных провайдеров долгое время (как минимум с 2001 г.) задачи сбора и раскрытия данных пользователей телекоммуникационных сервисов и Интернета решали сами спецслужбы за счет собственных ресурсов и технических возможностей. Наиболее ярким примером является деятельность Агентства национальной безопасности США (АНБ) по массовому сбору метаданных пользователей услуг телефонной связи в США на основании Статьи 215 Патриотического акта (USA PATRIOT Act). В рамках достаточно широкой интерпретации этой статьи и ряда других норм, принятых после терактов 11 сентября 2001 г., в США была развернута масштабная система программ спецслужб (прежде всего АНБ) по массовому неизбирательному сбору и перехвату данных (bulk data collection and data interception) как провайдеров телекоммуникационных услуг и интернет-сервисов, так и их пользователей (программы PRISM, MUSCULAR и проч.). Переломный этап в развитии таких спорных практик начался в 2014-2015 гг. и продолжается до сих пор. Важным процессом в этой связи является упразднение Патриотического акта и его замена Актом о свободе (FREEDOM Act) в 2015 г. Хотя часть положений USA PATRIOT Act в измененном виде были перенесен в текст FREEDOM Act, статья 215, дававшая АНБ основания для самостоятельного сбора метаданных по услугам телефонии, прекратила свое существование. Новые положения Акты о свободе как раз переносят деятельность по организации сбора метаданных пользователей услуг телефонии из компетенции государственных органов в компетенцию операторов таких услуг на основании предъявляемых государством нормативных требований.

Неудавшиеся попытки принять законодательство о хранении данных

Несмотря на то, что политика сохранения данных всегда оставалась основной моделью в США, в прошлом был предпринят ряд неудачных попыток принять нормы, укладывающиеся в концепцию хранения данных (data retention). Данные нормы были направлены прежде всего на интернет-провайдеров, а не на

провайдеров услуг мобильной и фиксированной телефонной связи, в отличие от большинства действующих НПА.

- В 2006 г. директор ФБР Роберт Мюллер призвал принят законодательство, обязывающее интернет-провайдеров в США обеспечивать хранение информации о действиях их пользователей (метаданные) **в течение 2 лет**. Конкретный перечень подлежащих хранению метаданных не уточнялся, в качестве основания для принятия закона указывалась необходимость доступа полиции и других правоохранительных органов к таким данным в рамках ведения расследований. Дальше идеи законопроекта ситуация не продвинулась, несмотря на озвученную поддержку представителей ряда других регуляторов[12]. Тогда же в 2006 г. Международной ассоциацией шефов полиции был озвучен аналогичный призыв принять закон, который бы обязывал интернет-провайдеров в течение «целесообразного срока» хранить данные об интернет-коммуникациях пользователей, включая информацию, идентифицирующую инициатора и адресата передачи данных.[13]
- В 2009 г. в Конгресс США был внесен пакет из двух законопроектов, акронимизированных как «Закон о безопасности в Интернете» (Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act, SAFETY Act)[14]. Законопроектом предлагалось обязать провайдеров электронных коммуникаций, а также провайдеров удаленных компьютерных сервисов хранить **в течение 2 лет** информацию, позволяющую идентифицировать пользователя, которому соответствующий провайдер в рамках предоставления своих услуг присвоил временный сетевой адрес[15]. Законопроект не был принят.

[12] https://www.cnet.com/news/fbi-politicos-renew-push-for-isp-data-retention-laws/
[13] https://www.cnet.com/news/fbi-wants-records-kept-of-web-sites-visited/
[14] https://www.govtrack.us/congress/bills/111/s436
[15] https://web.archive.org/web/20090319010704/http://www.crn.com/networking/214502232

Обязательства по сохранению данных в контексте принятия Акта о свободе (FREEDOM Act)

2 июня 2015 г. Бараком Обамой был подписан Закон об объединении и усилении Америки путем соблюдения прав и окончания прослушки, массового сбора данных и онлайн-слежки (Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act), более известный как Акт о свободе (USA FREEDOM). Закон был принят в качестве замены Патриотическому акту и был призван ограничить сложившуюся в рамках Статьи 215 последнего практику массового сбора и перехвата данных (прежде всего, данных о телефонных соединениях) АНБ США. В рамках Акта о свободе полномочия АНБ по сбору данных существенно ограничиваются за счет уточнения возможностей и порядка их применения, а также сужения перечня оснований для сбора данных и круга субъектов, в отношении которых допустим сбор данных. Ключевой момент в том, что функции по сохранению данных переходят от АНБ к самим телекоммуникационным провайдерам, которые обязаны предоставлять их АНБ на основании судебного ордера (включая метаданные телефонных коммуникаций).

Вместе с тем, сам Акт о свободе не вводит новых требований к провайдерам телекоммуникационных услуг по хранению данных. Вместо этого, его статьи частично «откатывают» систему американских НПА в состояние, которое имело место до принятия Патриотического акта 2001 г. При этом Акт о свободе не отменяет действия других законов и подзаконных актов отдельных регуляторов, принятых и вступивших в силу уже после принятия Патриотического акта. В результате, сохраняется гибкая политика сохранения данных (data preservation) телекоммуникационными провайдерами, которую они определяют и формируют самостоятельно в рамках набора требований в различных других законах и НПА.

Также USA FREEDOM вносит существенные уточнения в определения, используемые в нормативных актах других регуляторов, в том числе по вопросам сохранения данных провайдерами телекоммуникационных услуг. В частности, § 107 внес изменения в Статью 501 Кодекса законов США, содержащую в том числе определение подробных записей о вызове (Call Detail

Records, CDRs). Ранее такое определение в регуляторной практике Федеральной комиссии по коммуникациям (FCC) и тексте законов, регламентирующих деятельность FCC (в частности, Закон о коммуникациях 1934 г.) включало в себя данные о местонахождении пользователя услуг, в том числе данные GPS и данные местоположения ячеек сотовой связи, к которой (-ым) подключен мобильный телефон во время коммуникации. В параграфе 107 Акта о свободе приводится следующее определение подробных записей о вызове (CDR)[16]:

CDR означает информацию, позволяющую идентифицировать сеанс коммуникации, в том числе:

- телефонный номер, с которого был инициирована и завершена коммуникация;
- номер международного идентификатора мобильного абонента (IMSI); номер международного идентификатора мобильного оборудования (IMEI);
- номер телефонной карты, с использованием которой был осуществлен вызов; время и продолжительность звонка.

При этом прямо прописан, что CDR НЕ включает в себя:

- любое содержимое (данные) сеанса коммуникации;
- имя, адрес или платежную информацию подписчика или клиента;
- данные местоположения ячеек сотовой связи, к которой осуществлялось подключение во время коммуникации;
- данные системы глобального позиционирования (GPS).

В результате принятия Закона о свободе ожидалось, что исключение данных о местоположении устройств абонентов телекоммуникационных услуг из определения CDR приведет к тому, что телекоммуникационные провайдеры США, соответственно, исключат эти данные из своих политик хранения.

[16] https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf

Телефонная связь: нормативные требования по хранению метаданных абонентов

Одно из требований по сохранению метаданных пользователей услуг телефонной связи было введено Федеральной комиссией по коммуникациям США (FCC) еще в 1986 г. Согласно параграфу 42.6 «Хранение записей междугородних телефонных звонков»[17] Свода федеральных нормативных актов США (CFR), все провайдеры услуг магистральной (toll) телефонной связи обязаны хранить **в течение 18 месяцев** записи о совершенных звонках, необходимые для получения биллинговой информации о совершенных звонках. В частности, сохранению подлежат следующие данные:

1. Имя абонента.
2. Адрес абонента.
3. Вызывающий телефонный номер.
4. Вызываемый телефонный номер.
5. Дата и точное время звонка.
6. Продолжительность звонка.

Каждый провайдер услуг магистральной телефонной связи должен обеспечивать хранение таких данных вне зависимости от того, осуществляет ли он биллинг звонков собственных клиентов или же осуществляет биллинг звонков клиентов другого провайдера.

В августе 2015 г. Центр информации об электронной тайне частной жизни (Electronic Privacy Information Center (EPIC)) подал в FCC петицию с призывом отменить норму о хранении метаданных телефонных коммуникаций от 1986 г. Среди доводов в поддержку петиции ее авторы указывали низкую эффективность существующего механизма хранения таких данных для правоохранительных органов и его технологическую отсталость. Последний момент в том числе признавался Министерством юстиции США еще в прошлом десятилетии.[18]

Помимо нормы 1986 г., еще одним законодательным инструментом, который обязывает провайдеров хранить информацию о телефонных коммуникациях, является Закон о содействии правоохранительным органам в

[17] https://www.law.cornell.edu/cfr/text/47/42.6

[18] http://www.insidesources.com/privacy-groups-ask-fcc-to-repeal-bulk-phone-data-collection-rule/

области коммуникаций (Communications Assistance for Law Enforcement Act, CALEA), принятый в 1994 г. Закон обязывает провайдеров телефонной связи, а также операторов услуг беспроводного доступа в Интернет и VoIP-связи предоставлять правоохранительным органам свои технические возможности для осуществления перехвата или получения доступа к информации о телефонных коммуникациях на основании судебных ордеров. Согласно требованиям законодательства (пункт Кодекса федеральных нормативных актов США 47 C.F.R. § 1.20004(b), провайдеры услуг телефонной связи обязаны обеспечивать хранение информации (метаданных) обо всех перехваченных по запросам правоохранительных органов звонках **«на протяжении разумного срока».** Принципиальная размытость такой формулировки служит основанием для критики CALEA с момента принятия закона. Вместе с тем, провайдерам рекомендуется (но не предписывается в обязательном порядке) принят политику хранения информации по выполненным запросам **в течение двух лет**.

Конкретный перечень информации, подлежащей хранению провайдерами в рамках исполнения запросов органов правопорядка, может включать в себя, но не ограничивается:

- Телефонный номер, код идентификации канала (CIC) либо иная информация, позволяющая идентифицировать коммуникацию.
- Время и дата начала мероприятий оператора по осуществлению перехвата либо получению доступа к информации, позволяющей идентифицировать звонок.
- Время и дата окончания мероприятий оператора по осуществлению перехвата либо получению доступа к информации, позволяющей идентифицировать звонок.
- Личность сотрудника органов правопорядка, предъявившего документы, санкционирующие деятельность по перехвату / получению доступа к информации, позволяющей идентифицировать коммуникацию.
- Тип перехвата или получения доступа к телефонной коммуникации (например, перехват и отслеживание метаданных звонка, перехват полного содержимого звонка, перехват в рамках ордера на основании Закона FISA и проч.).
- И проч.

Телекоммуникационные провайдеры, предоставляющие услуги сервиса телекоммуникационного реле (Telecommunications Relay Service, TRS), обязаны обеспечивать хранение данные о об осуществленных в рамках сервиса звонках **в течение 5 лет** согласно 47 C.F.R. § 64.604. Сервис TRS представляет собой специальную систему, предназначенную для обеспечения возможности совершать телефонные звонки людям с нарушениями слуха и речи. В рамках сервиса участники коммуникации пользуются услугами ассистентов по коммуникации, которые обеспечивают переключение коммуникации в различные гибридные форматы (функция реле): Text-to-Voice, Voice Cary Over, Speech-to-Speech Relay Service и проч. Работу системы поддерживают американские частные телекоммуникационные операторы при координации Комиссии по коммуникациям (FCC).[19]

Политики хранения данных провайдеров телекоммуникационных услуг

Провайдеры телекоммуникационных услуг в США достаточно редко открыто публикуют свои политики в части сохранения данных пользователей в соответствии с требованиями законодательства. Доступная статистика в основном касается провайдеров фиксированной и мобильной телефонной связи и характеризует прежде всего их подход к соблюдению нормы FCC о хранении метаданных коммуникации по магистральным телефонным сетям от 1986 г. Среди телекоммуникационных операторов услуг телефонии практика публикации комплексных добровольных отчетов о прозрачности (transparency reports), в том числе в части имплементации требований по хранению данных, не развита так, как среди провайдеров услуг в Интернете.

- Verizon Wireless – крупнейший в США провайдер сервисов мобильной связи, осуществляет хранение телефонных CDR в течение **«примерно одного года»**[20].
- Второй по величине провайдер услуг мобильной связи AT&T не дает конкретных сроков хранения подробных записей о звонках, однако

[19] https://www.fcc.gov/consumers/guides/telecommunications-relay-service-trs

[20] https://www.usnews.com/news/articles/2015/05/22/how-long-cellphone-companies-store-your-call-records

представители компании заявляли, что для таких данных обеспечивается срок хранения **в 5 лет**.[21]

- Крупнейший в мире оператор связи и интернет-провайдер Level3 реализует следующие параметры в рамках корпоративной политики сохранения данных: хранение CDR в течение 2 лет, хранение иных данных по телефонным коммуникациям на основании запросов о сохранении от государственных органов (Preservation Requests) в течение 90 дней; текстовые сообщения (SMS, MMS и проч.) не хранятся.[22]
- Крупный провайдер услуг беспроводной связи T-Mobile US обеспечивает хранение CDR в промежутке от 7 до 10 лет[23].
- MetroPCS обеспечивает хранение данных о телефонных коммуникациях в течение двух лет. [24]
- Один из крупнейших телекоммуникационных провайдеров Sprint хранит CDR в течение 18 месяцев (минимально допустимый срок согласно норме 1986 г.)[25].
- U.S. Cellular хранит записи о телефонных коммуникациях в течение одного года (формально такой срок нарушает требования закона)[26].
- Credo Mobile, провайдер второго порядка, арендующий часть ресурсов телекоммуникационной сети у Sprint, обеспечивает хранение CDR в течение 3 лет.

[21] Там же.

[22] http://www.level3.com/-/media/files/legal_netsecurity/en_lea_portal_instructions.pdf

[23] http://www.msn.com/en-us/news/technology/how-long-cellphone-companies-store-your-call-records/ar-BBk8yxg

[24] https://www.usnews.com/news/articles/2015/05/22/how-long-cellphone-companies-store-your-call-records

[25] Там же.

[26] Там же.

Великобритания

Правительство Соединенного Королевства подготовило и представило на рассмотрение законодательного органа 1 марта 2016 г. проект – «Закон о хранении данных и правовом регулировании следственных полномочий» (*Data Retention and Investigatory Powers Act*), включая сопроводительные материалы для рассмотрения обеими Палатами Парламента (Палатой Лордов и Палатой Общин) Соединенного Королевства.

Поясним, что представленный законопроект был подготовлен в связи с утратой силы 31 декабря 2016 г. закона, принятого в июле 2014 г. и известного под аббревиатурой «DRIPA» (*Data Retention and Investigatory Powers Act*) 2014 г. (далее – «Закон DRIPA»). В свою очередь, принятие Закона DRIPA во многом (если не во всем) было обусловлено необходимостью имплементации Директивы 2006/24/ЕС Европейского Парламента и Совета 2006/24/ЕС «О сохранении данных, созданных или обработанных в связи с предоставлением общедоступных услуг электронной связи или сетей связи общего пользования», содержание которой было рассмотрено ранее.

Как отмечалось в предыдущем разделе настоящего исследования, названная Директива 2006/24/ЕС была отменена 8 апреля 2014 г. решением Европейского Суда Справедливости (*European Court of Justice Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland of 8 April 2014*).

Это решение Европейского Суда Справедливости, а также существенные замечания, высказанные законодательным органом в отношении значительного числа нормативных положений «Закона DRIPA», нарушающих, среди прочего конфиденциальность, порядок хранения данных, расширение компетенции правоохранительных органов, а также органов безопасности, привело к тому, что Закон DRIPA утратил силу в декабре 2016 г., и привел к необходимости подготовки нового законопроекта, уточняющего правовое регулирование порядка хранения данных, компетенции государственных органов (следственных, органов безопасности и т.д.) в не нарушающих частную жизнь, конфиденциальность и проч.

Соответственно, «Закон о хранении данных и правовом регулировании следственных полномочий» (далее – «Закон о хранении данных 2016 г.») в ноябре 2016 г. получил Королевскую санкцию (*Royal Assent*) и вступил в силу в день его принятия. Однако, следует пояснить ряд важных моментов, связанных с порядком вступления в силу Закона о хранении данных 2016 г. и его территориальным действием, поскольку речь идет о Соединенном Королевстве.

Закон о хранении данных 2016 г. достаточно значительный по своему объему документ (около 300 страниц), достаточно сказать, что он содержит 9 частей, распределенных по соответствующим главам и включающих 272 пункта, неотъемлемыми частями Закона являются 10 «тематических» таблиц.

Закон о хранении данных 2016 г. закрепляет, что ряд его нормативных положений вводятся в действие дифференцированно, т.е. в разный период времени. В соответствии с положениями (5-7), Закон о хранении данных 2016 г. распространяется на Англию и Уэльс, Шотландию и Северную Ирландию (*England and Wales, Scotland and Northern Ireland*) Соединенного Королевства; кроме того, он действует на территории любого из Нормандских островов (*Channel Islands*). При этом Ее Величество может, на основании соответствующего решения, распространить действие любого из положений Закона (с изменениями и без таковых) на остров Мэн (*Isle of Man*) или любую из Британских заморских территорий (*British overseas territories*).

Основные положения Закона о хранении данных 2016 г.

Закон о хранении данных 2016 г. направлен на осуществление надзора в сфере защиты и хранения данных, включая проведение следственных действий, определение полномочий компетентных органов, включая правоохранительные и разведывательные органы. Законом о хранении данных 2016 г. определены механизмы (организационные, процедурные и т.д.) деятельности органов, осуществляющие следственные мероприятия и, в этой связи, рассматриваемый Закон вносит изменения и поправки в иные действующие акты, связанные с правовым регулированием рассматриваемой сферы отношений. Закон о хранении данных 2016 г. применяется *в системе* действующих нормативных актов, регулирующих отношения защиты данных, конфиденциальности, охрану частной жизни и др.

Закон о хранении данных 2016 г. операционализирует основные понятия, используемые при регулировании рассматриваемого круга отношений применительно к каждому из соответствующих разделов.

Закон о хранении данных 2016 г.:

1) устанавливает какие органы, в каком порядке, в каком объеме своей компетенции могут осуществлять свою деятельность, которая связана с использованием конфиденциальной информации и данных (одним из основных контекстов Закона о хранении данных 2016 г. является четкое определение компетенции и круга полномочий следственных, правоохранительные и разведывательных органов);

2) закрепляет исходный принцип правового регулирования – обязанность органов государственной власти охранять частную жизнь и конфиденциальность, в целях его и определяется правовой и институциональный механизм, обеспечивающий конфиденциальность данных;

3) определяя меры, обеспечивающие конфиденциальность и порядок хранения (включая сбор, обработку, передачу) данных, классифицирует круг правонарушений и закрепляет соответствующие санкции в отношении: a) незаконного **перехвата сообщений** (*unlawful interception of communications*); b) незаконного **получения передаваемых данных** (*unlawful obtaining of communications data*);

4) отменяет и ограничивает сферу общей компетенции органов по поиску и получению передаваемых данных, делая акцент на специальной компетенции и установлении круга прав и обязанностей, а также четко определяет правовые условия, при которых может осуществляться **вмешательство в использование оборудования** (*equipment interference*); а также определяет требования, предъявляемые к перехвату сообщений (*interception of communications*);

5) вводит надзорные механизмы, применяемые в отношении осуществления деятельности компетентных органов в целях защиты частной жизни и конфиденциальности сообщений, которые включают, в частности:

a) определение конкретных режимов и процедур осуществления надзора (части 2-7 и 8 Закона), и b) обязанность соблюдать, наряду с прочими, следующие правовые акты и нормы общего права. Соблюдению подлежат: (i) Закон о правах человека 1998 г. (*Human Rights Act*); (ii) Закон о защите данных 1998 г. (*Data Protection Act*), в отношении защиты персональных данных и т.д.

(раздел 55); (iii) Закон о беспроводной телефонной связи 2006 г. (*Wireless Telegraphy Act*) в отношении незаконного перехвата сообщений или разглашения сообщений (раздел 48); (iv) Закон о неправомерном использовании компьютерных технологий (*Computer Misuse Act*) 1990 г. в отношении компьютерных преступлений (разделы 1- 3A); (v) нормы общего права (*Common Law*) в отношении преступлений, являющихся таковыми по нормам общего права, а также ненадлежащего поведения на государственной службе.

В связи с тем, что Закон о хранении данных 2016 г. направлен на осуществление надзора в сфере защиты и хранения данных, включая проведение следственных действий, определение компетенции и круга полномочий компетентных органов, включая правоохранительные и разведывательные органы, следует отметить, что предусмотрен комплекс норм, определяющих конкретный порядок и режим деятельности. В этой связи Закон о хранении данных 2016 г. регулирует:

1) порядок **правомерного перехвата сообщений** (*lawful interception of communications*), в рамках которого закрепляются обстоятельства, при которых перехват сообщений является законным, включая действия по перехвату сообщений, основанные **на ордере** (*under a warrant*); а также условия перехвата сообщений и последующее использование перехваченной информации и обработки материалов, полученных в связи с перехваченной информацией (части 2-7);

2) порядок правомерного **получения передаваемых данных** (*lawful obtaining of communications data*) в рамках которого закрепляются обстоятельства, при которых получение передаваемых данных является законным. Законность (правомерность) получения передаваемых данных основывается либо на соответствующем **разрешении** (*authorisation*) либо на **ордере** (*under a warrant*). Именно разрешение или ордер рассматриваются, в смысле нормативных положений Закона о хранении данных 2016 г., как законное (правомерное) основание осуществления *всех* действий, связанных с получением данных, а также с обработкой полученных данных;

3) порядок хранения конкретных передаваемых данных, в соответствии с уведомлением – **уведомление о сохранении данных** (*retention notice*);

4) порядок правомерного вмешательства в использование оборудования (*equipment interference*), осуществляемое на основании соответствующего ордера;

5) порядок получения ордеров на передачу персональных данных.

Закон о хранении данных 2016 г. определяет соответствующие механизмы надзора за названными выше «порядками», коррелирующих с иными действующими нормативными актами и нормами общего права (*Common Law*). Кроме того, Закон о хранении данных 2016 г. содержит различные нормативные положения, вносящие изменения и поправки в соответствующие действующие правовые акты. В частности, Закон о хранении данных 2016 г. изменяет разделы 3 и 5 Закон о разведывательной службе 1994 г. в отношении положений о национальной безопасности и т.д.

Закон о хранении данных 2016 г. исходит из того, что законность (правомерность) получения передаваемых данных основывается на соответствующем **разрешении** (*authorisation*), при этом строго определяя «целевой» характер таких разрешений.

Разрешения (*authorisation*) на получение **передаваемых данных** (*obtaining of communications data*) и полномочия выдавать разрешения для «целевого» получения данных (данных, получаемых в определенных целях) действуют при соблюдении определенных условии и если они выданы соответствующими уполномоченными должностными лицами соответствующего государственного органа, включая «местные» органы власти (с учетом особенностей административно-территориального устройства Соединенного Королевства).

1. Полномочия на выдачу разрешений (*authorisation*) , действуют при условии, если уполномоченное должностное лицо соответствующего государственного органа считает что:

a) получение **передаваемых данных** необходимо в целях, предусмотренных законом (7 b), а также в случае, если и такие данные необходимо получить:

i) для целей конкретного расследования или конкретной операции или

ii) для целей тестирования, поддержания или развития оборудования, систем или других средств связи;

c) выдача такого разрешения пропорциональна и адекватна для достижения соответствующих целей.

Получение данных является «целевым» если их предоставление требуется:

a) в интересах национальной безопасности;

в) в целях предотвращения или обнаружения преступления или предотвращения беспорядков;

c) в интересах экономического благосостояния Соединенного Королевства, поскольку эти интересы также связаны с интересами национальной безопасности;

d) в интересах общественной безопасности,

e) в целях оценки или сбора любых налогов, сборов, взносов иных платежей, подлежащих оплате государственным учреждениям;

(g) в целях предотвращения ущерба (смерть, увечье и т.д.) физическим лицам, а также ущераба психики, и психическому здоровью человека;

h) в целях содействия расследованию предполагаемых судебных ошибок;

i) когда физическое лицо умерло или не может быть идентифицировано;

j) в целях осуществления функций регулирования финансовых услуг и рынков, а также финансовой стабильности.

Закон о хранении данных 2016 г. «категорирует» условия, при которых круг полномочий и компетенция уполномоченных должностных ограничена в отношении **записей интернет-соединений** (*internet connection records*). В силу Закона о хранении данных 2016 г. такие условия «категорированы» по условиям – категорий «A», «B», «C».

Условия категории «A». Разрешения на получение данных с использованием записей интернет-соединений выдается при условии, если необходимо установить: a) какое лицо или устройство использует интернет-услугу; в) известны услуга и время ее использования, но невозможно идентифицировать лицо или устройство, с помощью которой услуга получена.

Условия категории «B». Разрешения на получение данных с использованием записей интернет-соединений выдается: a) если цели получения данных предусмотрены Законом (указаны конкретные нормы); в) для предупреждения или обнаружения преступления; c) если уполномоченное должностное лицо считает, что необходимо получить данные для определения

i) какая интернет-услуга используется, когда и как ее использует уже идентифицированное лицо или устройство ii) когда уже идентифицированное лицо или устройство, получает доступ к компьютерному файлу или компьютерной программе или запускает ее, которая полностью или в основном включает предоставление или приобретение материалов, владение которыми является преступлением; iii) какая интернет-услуга используется, а также когда и как она используется, уже идентифицированным лицом или устройством.

Условия категории «C». Разрешения на получение данных с использованием записей интернет-соединений выдается:

a) если цели получения данных предусмотрены Законом (указаны конкретные нормы);

в) для предупреждения или обнаружения преступления;

c) преступление, которое должно быть предотвращено или обнаружено, является серьезным преступлением; c) если уполномоченное должностное лицо считает, что необходимо получить данные записей интернет-соединений для определения того: i) какая интернет-услуга используется, когда и как ее использует уже идентифицированное лицо или устройство ii) когда уже идентифицированное лицо или устройство, получает доступ к компьютерному файлу или компьютерной программе или запускает ее, которая полностью или в основном включает предоставление или приобретение материалов, владение которыми является преступлением; iii) какая интернет-услуга используется, а также когда и как она используется, уже идентифицированным лицом или устройством.

Для целей Закона «**запись интернет-соединений**» (*internet connection record*) означает данные связи, которые:

a) могут использоваться для идентификации или содействовать идентификации телекоммуникационных услуг, которые передаются посредством телекоммуникационной системы в целях получения доступа к компьютерному файлу (или его запуска), либо к компьютерной программе; и

b) содержат данные, созданные или обработанные оператором телекоммуникационной сети в процессе предоставления телекоммуникационных услуг отправителю сообщения (независимо от того, относится ли это к лицу или нет).

Закон о хранении данных 2016 г. закрепляет обязанности операторов телекоммуникационных сетей в отношении разрешений (*authorisation*), и в их числе:

1) обязанность оператора телекоммуникационной сети, которому направлено требование, предпринимать все действия, предусмотренные в соответствующем разрешении.

2) обязанностью оператора телекоммуникационной сети является раскрытие коммуникационных данных согласно запросу или требованию, во исполнение предписаний, содержащихся в разрешении. При этом оператор телекоммуникационной сети обязан раскрывать данные таким образом, чтобы минимизировать объем раскрываемых данных и который необходимо обработать для достижения соответствующих целей, а также с учетом технических возможностей.

Хранение передаваемых данных (retention of communications data)

Часть 4 Закона о хранении данных 2016 г. непосредственно регулирует порядок хранения передаваемых данных.

Полномочия требовать сохранения конкретных данных входят в предметную и функциональную компетенцию Государственного секретаря (*Secretary of State*)[27], Судебного комиссара (*Judicial Commissioner*)[28], Комиссара по следственным полномочиям (*Investigatory Powers Commissioner*)[29].

Государственный секретарь (*Secretary of State*) вправе направить соответствующее уведомление – «**уведомление о сохранении данных**» (*retention notice*). Государственный секретарь вправе потребовать от оператора телекоммуникационных сетей сохранять соответствующие данные связи, если:

a) по его мнению такое требование является необходимым и соразмерным для достижения конкретной цели (целей), предусмотренных разделом 61(7), п a) – j Закона); и b) решение о направлении «уведомления о

[27] Закон о конституционной реформе 2005 г. (*Constitutional Reform Act 2005*) изменил статус ряда лиц, в настоящее время парламентские функции исполнительной власти переданы Государственному секретарю по делам юстиции.

[28] Судебный комиссар (*Judicial Commissioner*) – встречается иной перевод – Судебный специальный уполномоченный

[29] Комиссар по следственным полномочиям (*Investigatory Powers Commissioner*) – встречается иной перевод – Уполномоченный по следственным полномочиям

сохранении данных» было утверждено Судебным комиссаром (*Judicial Commissioner*).

«Уведомление о сохранении» **может**: a) относиться к конкретному оператору или любому типу операторов; в) требовать сохранения всех данных или любого типа данных; c) устанавливать период/периоды в течении которых такие данные должны быть сохранены; d) содержать иные требования или ограничения в отношении сохранения данных; e) закреплять различные положения для достижения различных целей, предусмотренных законом; f) относиться к данным, существовавшим или не существовавшим на момент подачи или вступившим в силу «уведомления о сохранении данных» .

«Уведомление о сохранении данных» **не должно** содержать требования о хранении каких-либо данных в течение ***более*** **12 месяцев**, при этом начало исчисления срока закрепляется дифференцированно. «Уведомление о сохранении» не должно требовать от оператора, который контролирует или предоставляет дистанционную передачу данных – «системный оператор» (*system operator*) – сохранения следующих данных:

a) данных, связанных с использованием телекоммуникационных услуг, предоставляемых другим оператором связи;

в) данных, которые обработаны (могут быть обработаны) системным оператором как присоединенное или логически связанное сообщение с использованием систем, указанных в предыдущем пункте;

c) данных, которые требуются для системного оператора для функционирования системы связи;

d) данных, которые не сохраняются или не используются системным оператором для какой-либо другой законной цели.

Закон о хранении данных 2016 г. предусматривает порядок вступления «уведомление о сохранении» в силу. «Уведомление о сохранении данных» вступает в силу: a) когда оно получено оператором, в адрес которого оно направлено; или b) в указанный в уведомлении момент или указанное время. При этом, в отношении уже сохраненных данных, срок их хранения зависит от срока вступления «уведомления о сохранении данных» в силу, и этот срок исчисляется с соответствующего момента вступления в силу такого уведомления.

В «уведомлении о сохранении данных»: должны быть указаны:

a) оператор (или тип операторов) к которому относится уведомление

b) данные, которые необходимо сохранять;

c) период или периоды, в течение которых данные должны быть сохранены;

d) любые иные требования или любые ограничения в отношении сохранения данных;

e) информация, требуемая, в том числе, по взносам на по расходы, понесенные в связи с направлением данного уведомления.

Требования или ограничения в отношении сохранения данных, могут, в частности, включать: a) требование сохранить данные таким образом, чтобы они могли быть своевременно переданы по соответствующему запросу; b) требования или ограничения в отношении получения данных, включая сбор, создание, обработку данных и т.д.

Закон о хранении данных 2016 г. закрепляет понятие **«зн*а*чимые передаваемые данные»** (*relevant communications data*), означающие данные, которые могут использоваться для идентификации или способствовать идентификации:

a) отправителя или получателя сообщения (независимо от того относится и это к лицу или нет);

b) времени или продолжительности коммуникации;

c) типа, способа, вида или факта коммуникации;

d) систем телекоммуникации (или любых их частей), с помощью, через, или посредством которых установлена коммуникация, или переданы данные;

e) местоположения любой системы телекоммуникации.

Важно обратить внимание, что понятие «зн*а*чимые передаваемые данные» охватывает также записи **интернет-соединений**

Закон о хранении данных 2016 г. закрепляет, что Государственный секретарь, прежде чем направить «уведомление о сохранении данных» должен, среди прочего:

1) учитывать: a) вероятную полезность такого уведомления; b) вероятное число пользователей (если известно) любых телекоммуникационных услуг, к которым относится такое уведомление; c) технические возможности соблюдения такого уведомления; d) вероятные расходы, которые могут быть связаны с соблюдением такого уведомления; e) любые иные последствия данного

уведомления для оператора телекоммуникаций (или типа операторов), к которому относится это уведомление;

2) до направления уведомления, Государственный секретарь должен предпринять разумные шаги для консультаций с любым оператором, к которому уведомление относится.

Закон о хранении данных 2016 г. предусматривает необходимость утверждения «уведомлений о сохранении данных» Судебным комиссаром (*Judicial Commissioner*). В компетенцию Судебного комиссара (*Judicial Commissioner*), относящуюся к этой сфере, входит следующее:

1) при принятии решения об утверждении «уведомления о сохранении данных» Судебный комиссар должен пересмотреть выводы Государственного секретаря относительно того, является ли требование, налагаемое в соответствующем «уведомлении о сохранении данных» необходимой и пропорциональной мерой и соответствует ли оно одной или нескольким целям, подпадающих под пункты (a) - (j) раздела 61 (7) Закона

2) при этом Судебный Комиссар обязан: a) применять те же принципы, которые будут применяться судом по ходатайству о пересмотре судебного решения; и b) принимать решения таким образом, чтобы не превысить свою компетенцию, вытекающую из Закона о хранении данных 2016 г., а также свои полномочия в части обеспечения соблюдения конфиденциальности;

3) если Судебный Комиссар отказывается утвердить решение о направлении «уведомлении о сохранении данных» он предоставляет соответствующее письменное обоснование Государственному секретарю.

4) если Судебный Комиссар, не считая Комиссара по следственным полномочиям (*Investigatory Powers Commissioner*), отказывается одобрить решение о направлении «уведомления о сохранении данных», Государственный секретарь может обратиться к Комиссару по следственным полномочиям с заявлением принять решение относительно одобрения решения о направлении «уведомления о сохранении данных».

Оператор телекоммуникационной сети, которому направлено «уведомления о сохранении данных», может обратиться к Государственному секретарю о его пересмотре. Такое обращение не освобождает оператора телекоммуникационной сети соблюдать направленное в его адрес уведомление.

Государственный секретарь обязан пересмотреть любое «уведомление о сохранении данных», направленное на его имя. До принятия решения о пересмотре «уведомления о сохранении данных», Государственный секретарь должен проконсультироваться, во-первых, с Техническим консультативным советом (*Technical Advisory Board*) и Судебным Комиссаром. При этом Технический консультативный совет должен учитывать технические требования и финансовые последствия для оператора телекоммуникационной сети, а Судебный Комиссар должен решить вопрос о соразмерности «уведомления о сохранении данных»

В свою очередь, Технический консультативный совет и Судебный Комиссар обязаны:

a) до принятия решения, предоставить заинтересованному оператору и Государственному секретарю возможность предъявить доказательства или сделать заявления в связи с «уведомлением о сохранении данных» ;

b) сообщить о принятом решении оператору телекоммуникационной сети и Государственному секретарю.

После рассмотрения выводов Технического консультативного совета и Судебного Комиссара решения, Государственный секретарь может либо изменить, либо отозвать «уведомление о сохранении данных», либо направить соответствующее уведомление оператору, подтверждающее действие «уведомления о сохранении данных».

Вместе с тем, Государственный Секретарь может изменить «уведомление о сохранении данных» или подтвердить его действие только если такое решение Государственного секретаря одобрено Комиссаром по следственным полномочиям (*Investigatory Powers Commissioner*). Закон о хранении данных 2016 г. подробно регламентирует компетенцию Комиссара по следственным полномочиям (*Investigatory Powers Commissioner*) в части порядка утверждения/одобрения «уведомления о сохранении данных», а также отказа в утверждении.

Закон о хранении данных 2016 г. предусматривает определенный круг обязанностей операторов телекоммуникационных сетей. К числе таких обязанностей относятся:

1) обеспечение целостности данных и их безопасности;

2) оператор телекоммуникационной сети должен: а) обеспечить, чтобы данные были защищены в той же мере, что и данные любых систем, из которой они получены; в) обеспечить с помощью соответствующих технических и организационных мер доступ к данным только специально уполномоченных лиц; с) защитить, посредством соответствующих технических и организационных мер, данные от случайного или незаконного уничтожения, случайной утраты или изменения или несанкционированного или незаконного хранения, сбора, обработки, доступа к таким данных или раскрытия данных;

3) оператор телекоммуникационной сети должен уничтожить данные, если сохранение данных перестает быть правомерным и иное не вытекает из Закона о хранении данных 2016 г. При этом уничтожение данных осуществляется в тот период времени и таким способом, которые оператор сочтет практически осуществимыми.

4) оператор телекоммуникационной сети обязан соблюдать требования или ограничения, содержащиеся в «уведомлении о сохранении данных» и не разглашать содержание третьим лицам.

Существенно важны положения Закона о хранении данных 2016 г. относительно экстерриториального действия «уведомления о сохранении данных». В практическом плане это означает, что любые требования или ограничения, налагаемые в силу «уведомления о сохранении данных (разделы 92, 93, 95 (1) – 95 (3)), могут относиться к действиям, осуществляемым за пределами Соединенного Королевства, а также к лицам, находящимся вне пределов Соединенного Королевства. При этом Закона о хранении данных 2016 г. совершенно четко определяет, что экстерриториальное применение относится к «уведомлению о сохранении данных». В силу нормативных положений раздела 95 (5), экстерриториальное применение не относится к действиям, осуществляемым в рамках гражданского судопроизводства возложенных на Государственного секретаря (*Secretary of State*) в отношении судебного запрета или для конкретного исполнения законных обязательств, вытекающих из положений Закона о Высшем суде по гражданским делам (Шотландия) 1988 г. (*Court of Session Act*).

Завершая общую характеристику Закона о хранении данных 2016 г., отметим еще раз, что понятийно-категориальный аппарат этого нормативного акта операционализирован применительно к соответствующему разделу. Вместе

с тем, целесообразно привести некоторые понятия, закрепленные в Законе о хранении данных 2016 г. и имеющие отношение к проанализированному контексту исследования.

Уведомление (*notice*) – означает уведомление, составленное в письменном виде;

Идентификация данных (*identifying data*) – означает:

a) данные, которые могут быть использованы для идентификации или помочь идентификации любых лиц, устройств, систем или услуг;

b) данные, которые могут быть использованы для идентификации или помочь идентификации любого события; или

c) данные, которые могут быть использованы для идентификации или помочь идентификации местонахождения (местоположения) любых лиц или вещей (*things*).

Данные, которые могут быть использованы для идентификации или помочь идентификации любого события (*data which may be used to identify, or assist in identifying, any event*) охватывают:

данные, имеющие отношение к сути события;

b) данные, имеющие отношение к виду, роду либо характеру события;

(c) данные, имеющие отношение ко времени или продолжительности события.

Коммуникация (*communication*) в отношении оператора телекоммуникационной сети, телекоммуникационных услуг, или телекоммуникационных систем включает:

a) все, что связано с речью, музыкой, звуками, визуальными изображениями или данные любого описания; b) сигналы, служащие либо для передачи чего-либо между людьми, между человеком и вещью или между вещами, либо для приведения в действие или управления любым оборудованием.

Оператор телекоммуникационной сети (*Telecommunications operator*) – означает лицо, которое:

a) предлагает или предоставляет телекоммуникационные услуги лицам в Соединенном Королевстве; либо

b) контролирует или обеспечивает телекоммуникационные сети, которые (полностью или частично) находятся в Соединенном Королевстве, или контролируются из Соединенного Королевства.

Китай

В июне 2017 г. вступает в силу Закон Китайской Народной Республики «О кибербезопасности» (*Cybersecurity Law*). Названный Закон (далее – «Закон о кибербезопасности») содержит 79 статей, 7 глав: Общие положения (Глава I); Поддержка и укрепление сетевой безопасности (Глава II); Безопасность операций в сети (Глава III), включающий 2 раздела – «Общие положения» и «Безопасность операций в критической информационной инфраструктуре»; Безопасность сетевой информации (Глава IV); Мониторинг, своевременное обнаружение и экстренное реагирование (Глава V); Юридическая ответственность (Глава VI); Дополнительные положения (Глава VII). С учетом специфики административно-территориального устройства Китая, важно обратить внимание, что действие Закона о кибербезопасности распространяется на «материковую» часть Китая.

Основополагающим для всех нормативных положений Закона о кибербезопасности является закрепление принципа суверенитета Китая в сфере киберпространства, и это определяет, с одной стороны, контекст порядка правового регулирования и содержание понятийно-терминологического аппарата этого Закона, с другой стороны, объясняет закрепление компетенции и круга полномочий органов государственной власти. Также следует напомнить, что в институциональном плане в Китае создана «многоуровневая» организационная система регулирования органами государственной власти телекоммуникационной сферы.

В контексте принципа суверенитета Китая в сфере киберпространства сформулированы: обязанности операторов сетей обеспечивать их безопасность; закреплены положения, относящиеся к защите личной информации; урегулирован сегмент «критической информационной инфраструктуры»; определены правила трансграничной передачи данных, а также определение и квалификацию правонарушений в этой сфере и закрепление соответствующих мер ответственности.

В общем плане, как отмечают многие аналитики и правоведы в Законе о кибербезопасности содержатся «обтекаемые» и «неясные» формулировки, а также положения, которые скорее всего будут урегулированы и уточнены в последующем соответствующими подзаконными актами[30].

Закон о кибербезопасности предусматривает, что государство устанавливает и совершенствует систему стандартов **безопасности сети** (*network security*) и основные вопросы в этой сфере решает Государственный Совет (*State Council*) Китая. Государственный Совет, прежде всего, в лице Административного департамента Государственного совета по стандартизации, а также других департаментов этого высшего органа власти Китая, в рамках своей компетенции, организуют разработку и своевременный пересмотр соответствующих национальных и отраслевых стандартов обеспечивающих **безопасность сети, безопасность сетевых продуктов** (*security of network products*) , **безопасность сетевых услуг** (*security of network services*) и функцинирования сети.

Закон о кибербезопасности раскрывает содержание понятия **«личная информация»** (*personal information*). Исходя из содержательных характеристик этого понятия, в контексте рассматриваемого Закона о кибербезопасности, целесообразен именно такой перевод на русский язык, а не – «персональные данные».

Закон о кибербезопасности определяет, что «личная информации» (*personal information*) относится ко всем видам данных, записанных в электронном виде или зафиксированных иным способом, и с помощью которых можно идентифицировать физическое лицо непосредственно или в сочетании с

[30] См. например, Overview China's Cybersecurity Law. IT Advisory KPMG China — February 2017. URL: https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf

иными данными, включая, но не ограничиваясь, имя физического лица, дату рождения, идентификационный номер, личные биометрические данные, адрес и номер телефона (статья 76 (5) Закона о кибербезопасности). Нормы названной статьи распространяются на «граждан» и на «физических лиц».

Для понимания регулирования порядка использования «личной информации» следует обратиться к содержанию еще одного ключевого понятия – «операторы сетей», к которым Закон о кибербезопасности относит: собственников (*owners*) и администраторов сетей (*administrators of networks*), а также и провайдеров сетевых услуг (*network service providers*).

«Операторы сетей» могут собирать и использовать «личную информацию» в порядке, установленным законом; при этом, осуществляя такие действия, операторы сетей, должны соблюдать принципы законности, приличий и необходимости, а также сообщать правила сбора и использования личной информации. Правила сбора и использования личной информации должны содержать: четкое указание целей, средств и возможностей использования, а получение согласия лица на сбор и использование личной информации является обязательным. Эти нормативные положения относятся к провайдерам сетевых продуктов и услуг, которые собирают личную информацию, включая персональные данные пользователей.

Закон о кибербезопасности закрепляет, что операторы сетей не должны собирать личную информацию, не связанную с предоставляемыми ими услугами; не должны нарушать положения законов, административных положений обработки личной информации, которую они хранят; не должны нарушать условия, предусмотренные в заключаемых договорах, о сборе или использовании личной информации.

Закреплена норма о том, что физические лица и организации не должны красть или использовать другие незаконные средства для получения личной информации, включая персональные данные. Закрепление такой нормы связано с тем, что граждане (лица) предоставляют личную информацию для многих целей и во многих сферах жизнедеятельности, в том числе в сфере образования, здравоохранения, общественного транспорта, следок, совершаемых с использованием телекоммуникационных сетей и т.д. Соответственно, Закон о кибербезопасности «стандартизирует» подходы и методы для предприятий и связанных с ними учреждений, по сбору и использованию личной информации.

«Операторы сетей» не вправе раскрывать, изменять или уничтожать собранную личную информацию. В случае, когда оператор сети нарушает порядок сбора и использования личной информации, Закон о кибербезопасности предусматривает право лица потребовать от оператора сети удалить свою личную информацию. Кроме того, если лицо обнаружит, что личная информация, собранная или хранящаяся у оператора сети, содержит ошибочные данные, лицо вправе потребовать от оператора сети внести соответствующие исправления.

«Специфическим» правилом является то, операторы сетей не должны предоставлять собранную ими личную информацию другим лицам, однако, это не относится к собранной личной информации, которая была обработана так, что конкретное лицо не может быть идентифицировано.

Операторы сетей обязаны предпринимать технические меры и иные необходимые меры для обеспечения безопасности собираемой ими личной информации, предотвращать утечку личной информации, ее уничтожение или потерю. В случаях утечки, уничтожения или потери личной информации, немедленно обязаны принять все меры по исправлению положения, и оперативно проинформировать пользователя, а также представить соответствующий отчет компетентным органам государственной власти.

С учетом роли государственных органов, обладающих широкими надзорными полномочиями в Китае, Закон о кибербезопасности закрепляет норму о том, что государственные органы «на законном основании» осуществляющие надзор и контроль над безопасностью сетей, а также сотрудники таких органов, обязаны хранить личную информацию, которая стала им известна в результате осуществления их профессиональных обязанностей, и способствовать тому, чтобы такая информация не была потеряна, а также не должны предоставлять такую информацию на незаконных основаниях другим лицам.

Закон о кибербезопасности предусматривает меры ответственности в отношении операторов сетей, провайдеров сетевых продуктов или услуг. Так, если названные операторы нарушают, в том числе нормы, связанные порядком сбора и хранения личной информации и защищаемую в соответствии с законом, в отношении них (независимо или одновременно):

– выносятся предупреждения;

– производится конфискация полученных незаконных доходов;

– и/или налагается штраф в размере от одного до десяти-кратного размера полученной незаконной прибыли;

– в случае отсутствия незаконных доходов, штраф составляет 1 000 000 юаней; кроме того штраф в размере от 10 000 до 100 000 юаней налагается на лиц, которые несут персональную ответственность;

В тех случаях, когда совершенные правонарушения квалифицируются как «серьезные нарушения», налагается штраф в размере от 50 000 до 500 000 юаней; при этом соответствующий компетентный орган государственной власти может потребовать:

– временного приостановления деятельности;

– приостановить деятельность для исправления возникших нарушений;

– закрыть веб-сайт;

– отменить соответствующие разрешения на работу:

– отозвать лицензию.

В случае хищения или использования иных незаконных средств для получения, незаконной передачи другим лицам личной информации и совершения иных действий, не являющихся преступлением, органы государственной безопасности изымают незаконные доходы и налагают штраф в размере от одного до десяти раз превышающую сумму полученных незаконных доходов; если незаконные доходы не получены, налагается штраф в размере до 1 000 000 юаней.

Закон о кибербезопасности закрепляет понятие «**операторы критической информационной инфраструктуры»** (*critical information infrastructure operators*) в отношении деятельности которых закреплен «специальный» комплекс норм. Применительно к рассматриваемой сфере отношений, следует отметить нормативные положения следующего содержания.

Личная информация, собираемая или создаваемая операторами критически важной информационной инфраструктуры, при эксплуатации критически важной информационной инфраструктуры на материковой территории Китая, должна храниться на материковой части Китае. В тех случаях, когда из-за потребностей бизнеса действительно необходимо предоставлять такую личную информацию его за пределами материковой части Китая, передача личной информации осуществляется в порядке соблюдения

условий безопасности. При этом непосредственно закреплена обязанность органов власти, а именно: Государственного департамента сетевой информации (*State network information departments*) и соответствующих департаментов Государственного Совета КНР (*State Council*), разработать порядок, предусматривающий комплекс мер для проведения такой оценки безопасности. (В настоящее время в Китае не приняты соответствующие акты).

В Китае были, в частности, Административные меры по предотвращению и профилактике и отражению компьютерных вирусов (*Administrative Measures for Prevention and Treatment of Computer Viruses*); Административные меры по многоуровневой защите информационной безопасности (*Administrative Measures for Hierarchical Protection of Information Security*) . Рассмотренный Закон о кибербезопасности выступает неким кодификационным законодательным актом, поскольку, по существу объединяет нормативные положения ранее принятых актов.

Бразилия

Федеративная Республика Бразилия (Бразилия) стала первым государством, которое на уровне закона закрепила правовые основы, принципы и порядок использования интернета, отразив фундаментальные технологические особенности многоуровневой инфраструктуры интернета, обеспечивающие трансграничное функционирование и использование интернета[31].

Бразилия 23 апреля 2014 г. приняла Законодательный акт – Закон № 12.965 «*Marco Civil da Internet*» (далее – «Закон Marco Civil»)[32] в котором

[31] В контексте существующих двусторонних отношений Россия-Бразилия, а также совместного участия этих государств в таком неформальном межгосударственном объединении как БРИКС, обращение к опыту Бразилии представляется полезным.

[32] Полный текст Закона № 12.965 «*Marco Civil da Internet*» на русском языке доступен на сайте Фонда содействия развитию интернета «Фонд поддержки интернет». URL:http://fondpi.ru/documents (Дата обращения: 09.04.2017).

закреплено, что «доступ к интернету» имеет первостепенное значение, является неотъемлемой частью прав пользователей и гарантировано законом (ст. 7 Закона Marco Civil). Таким образом, Бразилия относится к числу стран, разграничивающих ключевые понятия – «интернет» и «доступ к интернету» – и на законодательном уровне закрепляющих самостоятельное правовое значение этих понятий[33].

Следствием такого подхода и законодательного закрепления разграничения понятий «интернет» и «доступ к интернету», является последующее формирование понятийного аппарата рассматриваемого закона, а также содержательное определение целого ряда понятий, таких как:

«защита персональных данных»; «администратор автономной системы»; «интернет-соединение»; «интернет-приложения»; «запись о соединении/журнал соединений»; «регистрация доступа к интернет-приложениям»; «провайдер интернет-соединений»; «провайдер интернет-приложений» и др.

Законодательное закрепление понятийного ряда, несомненно, способствует правовой определенности правового регулирования отношения, связанных с использованием данных пользователей интернета.

Согласно Закону Marco Civil персональные данные, записи о соединениях и записи о доступе к интернет-приложениям, данные о частных интернет-коммуникациях пользователей носят конфиденциальный характер, и на интернет-провайдеров возлагается обязанность по обеспечению конфиденциальности данных. Законодательно закреплено, что сбор, хранение, обработка, передача данных пользователей (включая персональные данные), может осуществляться:

– в силу закона;

– может быть запрещен законом;

[33] В праве большинства зарубежных государств (страны-члены Европейского Союза, США, Канада, Австралия и т.д.) понятия «интернет» и «доступ к интернету» закреплены, разграничиваются и имеют самостоятельное значение. В российском праве на законодательном уровне отражен иной подход: в законодательстве различного уровня предпочтение отдается использованию эвфемизмов понятия «интернет» – «сеть Интернет», «информационно-коммуникационная сеть», «информационно-коммуникаци-онная сеть Интернет»; понятие «доступ к интернету» не закреплено и используются такие понятия как «доступ к информации», «доступ к сайтам в сети «Интернет»» и т.д.

– может быть предусмотрен договором о предоставлении услуг или является условием использования интернет-приложений.

В содержательном плане эти законодательные положения предполагают следующее.

Сбор, хранение, обработка, передача данных пользователей регулируется в силу действия нормативных положений Закона Marco Civil, который закрепляет правовые основания сбора, хранения, обработки, передачи данных пользователей, а также обязанность ведения и хранения:

– записей об интернет-соединениях пользователей,

– учетной документации о доступе при предоставлении соединения;

– учетной документации о доступе к интернет-приложениям (Подразделы I, II, III, ст.ст. 13-15 Закона Marco Civil).

При регулировании порядка сбора, хранения, обработки, передачи данных пользователей (далее – «Хранение данных пользователей») исходным является законодательное определение содержания следующих ключевых понятий:

«администратор автономной системы» (*autonomous system administrator*) – физическое или юридическое лицо, реализующее функцию администратора определенного блока IP-адресов и его уникальную автономную систему маршрутизации, зарегистрированный в установленном порядке государственным органом, ответственным за регистрацию и распределение IP-адресов в пределах географической территории, относящейся к данному государству;

«интернет-соединение» (*internet connection*) – наделение терминала способностью отправлять и получать пакеты данных по интернету, путем присвоения ему IP-адреса или его аутентификации;

«запись о соединении/журнал соединений» (*connection record/log*) – массив информации, относящийся к дате и времени начала и завершения сессии подключения к интернету, продолжительности такой сессии и использованию терминалом IP-адреса для отправки и получения пакетов данных;

«интернет-приложения» (*internet applications*) – набор функциональных средств, которые могут быть получены через подключенный к интернету терминал;

«регистрация доступа к интернет-приложениям» (*registrations of access to internet applications*) – «набор информации, о дате и времени использования конкретного интернет-приложения, осуществляемого с конкретного IP-адреса».

Хранение и ведение записей об интернет-соединениях осуществляет организация, отвечающая за управление автономной системой и предоставляющая интернет-соединение (провайдер интернет-соединений). Ведение учета таких записей о соединениях не может быть передано третьим лицам. Провайдер интернет-соединений ответственен за хранение записей и обеспечивает их конфиденциальность; учет записей **о б** интернет-соединениях хранится в течение **1 (одного) года,** с соблюдением конфиденциальности, в контролируемом безопасном месте.

Закон Marco Civil закрепляет право органов государственной власти, в круг которых входят административные и правоохранительные органы, а также Государственный Прокурор, требовать сохранять записи о соединениях в течение более длительного периода времени, т.е. **более одного года**. При этом Закон Marco Civil закрепляет обязанность соответствующего органа власти, потребовавшего сохранять записи о соединениях в течение более одного года, инициировать в течении 60 (шестьдесят) дней с момента первого запроса, соответствующее судебное разбирательство, с тем, чтобы получить решение суда на увеличение срока сохранять записей о соединениях.

Во всех случаях провайдер интернет-соединений предоставляет регистрационные журналы соответствующим государственным органам, и раскрывает иные данные о соединениях исключительно на основании решения суда.

Хранение учетной документации о доступе к интернет-приложениям возлагается на провайдера интернет-приложений, который обязан вести журналы записей о предоставлении услуг доступа к приложениям, с соблюдением конфиденциальности. Кроме того, провайдер интернет-приложений обязан хранить учетную документацию о доступе к интернет-приложениям в контролируемом и безопасном месте, **в течение 6 месяцев.**

В случае, если государственные органы (административные и правоохранительные органы, а также Государственный Прокурор) требуют

учетную документацию о доступе к интернет-приложениям, включая записи о предоставлении услуг доступа к приложениям, в течение более длительного периода, они обязаны инициировать соответствующее судебное разбирательство в течении 60 (шестьдесят) дней с момента первого запроса, для получения соответствующего решения суда. Провайдер интернет-приложений раскрывает данные записей регистрационных журналов а также данные учетной документации о доступе к интернет-приложениям, только на основании решения суда.

Провайдеры интернет-соединений и провайдеры интернет-приложений предоставляют информацию, подтверждающую, что Сбор данных пользователей осуществляется в соответствии с действующим законодательством Бразилии о защите персональных данных и конфиденциальности данных пользователей.

Закон Marco Civil закрепляет гарантии прав пользователей и такое законодательное закрепление гарантий прав обусловливает содержание функционирования органов власти. Закон Marco Civil гарантирует соблюдение, в частности: право на неприкосновенность личной и частной жизни; право на неприкосновенность и конфиденциальность потоков интернет-коммуникации пользователей; право на невозможность приостановки интернет-соединения (кроме случаев задолженности); право на получение ясной и полной информации об обеспечении сохранности записей о соединениях и записей о доступе к интернет-приложениям в договорах об оказании услуг, а также о практике управления интернет-трафиком, которые могут повлиять на качество предоставляемых услуг; право на неразглашение третьим лицам персональных данных пользователя, включая записи о соединениях и записи о доступе к интернет-приложениям (за исключением случаев, когда пользователь выразил свое согласие добровольно и осознанно, либо в случаях, предусмотренных законом); право на полное исключение персональных данных по требованию пользователя, предоставленных им для использования данного интернет-приложения, при прекращении взаимоотношений сторон; право на открытость и прозрачность любых условий использования, устанавливаемых провайдерами интернет-соединений и провайдерами интернет-приложений и др. (ст. 7 Закона Marco Civil).

Законодательное закрепление гарантий прав, по существу дела означает, что их ограничение запрещено, если иное не вытекает из решения суда и в порядке, установленном законом.

Закона Marco Civil устанавливает, что Хранение данных пользователей может основываться и регулироваться соответствующими договорами о предоставлении услуг доступа или закрепляться в качестве условия использования интернет-приложений. Законодательно гарантированному праву пользователей получать полную информацию о сборе, использовании, хранении, обработке и защите своих персональных данных (п.VIII ст. 7 Marco Civil) корреспондирует обязанность провайдеров закреплять в специальном пункте договора условие о Хранении данных пользователя (п.IX ст. 7 Marco Civil). Договоры провайдеров интернет-соединений и провайдеров интернет-приложений, которые не соответствуют этим условиям, не имеют юридической силы в силу закона.

Важное значение имеют те нормативные положения Закона Marco Civil, отражающие объективную трансграничную природу интернета. Речь идет о том, что Закон Marco Civil специфицирует отношения и круг субъектов, к которым в императивном порядке применяется право Бразилии. Законодательно закреплено, что в императивном порядке право Бразилии применяется:

- в отношении любой деятельности по сбору, накоплению, хранению и обработке персональных данных или данных относительно интернет-соединений, если такая деятельность осуществляется в пределах государственной территории Бразилии;
- в отношении данных, собранных в пределах государственной территории Бразилии;
- к определению содержания интернет-контента, если по крайней мере один из терминалов расположен на территории Бразилии (под «терминалом» понимается компьютер или иное устройство, подключенное к интернету);
- если деятельность по сбору, накоплению, сохранению и обработке персональных данных осуществляется юридическим лицом, расположенным за границей, но услуги оказываются

неопределенному кругу лиц в Бразилии, или по крайней мере один из членов какой-либо хозяйствующей группы учрежден в Бразилии.

Германия

Цели и принципы нормативно-правового регулирования

Нормы обязательного хранения данных пользователей телекоммуникационных услуг существовали в немецком законодательстве с 2008 по 2010 год (секция 113a и 113b Акта о телекоммуникациях) в соответствии с Европейской директивой о хранении данных. Согласно этим положениям, операторы связи были обязаны хранить информацию о фактах соединений в течение полугода и предоставлять ее правоохранительным органам (условия предоставления информации при обычной процедуре предполагали наличие судебного акта). В 2010 году Конституционный суд Германии признал данные нормы нарушающими конституционные права граждан на тайну переписки и конфиденциальность. Таким образом, немецкий процесс стал преамбулой к решению Европейского суда справедливости от 2014 года, которое отменило саму директиву ЕС.

Действующее федеральное законодательство содержит в себе несколько положений о предоставлении доступа к электронным коммуникациям пользователей правоохранительным органам. Так согласно Уголовно-процессуальному кодексу Германии (Secs. 100a и 100b Strafprozessordnung) правоохранительные органы могут получить доступ к коммуникациям подозреваемых в случае серьезных преступлений, запросив на это судебный ордер через Прокуратуру Германии (или налоговую службу в случае налоговых преступлений). Прокурор может также отдать приказ приступить к перехвату коммуникаций немедленно и получить в дальнейшем судебный ордер в течение трех дней. Дополнительные полномочия по аналогичному принципу определены для Федеральной службы расследований (Bundeskriminalamt) и региональных полицейских управлений (Polizeibehörden) в Законе о федеральной полиции (Bundeskriminalamtgesetz) и соответствующих региональных законах.

Разведслужбы и службы национальной безопасности (Bundesnachrichtendienst, Bundesamt für Verfassungsschutz могут получить доступ

согласно Акту о статье 10 (Artikel 10-Gesetz) в случае подозрений о подготовке преступлений, угрожающих национальной безопасности, с разрешения руководителя одной из ветвей государственной власти.

Закон о таможне (Zollfahndungsdienstgesetz) также позволяет таможенным следователям получать доступ к коммуникациям подозреваемых при наличии судебного ордера.

Немецкий закон о телекоммуникациях ("TKG") содержит требования для телекоммуникационных компаний, предоставляющих услуги гражданам, иметь технические возможности для перехвата электронных коммуникаций (голос, VoIP, SMS, почтовые сообщения) в случаях, предписанных законодательством Германии и сотрудничать с правоохранительными органами. Технические и организационные стандарты для организации перехвата, хранения, защиты и доступа к данным описаны в двух специальных директивах (TKÜV, TR-TKÜV). Данные мероприятия проводятся за счет операторов связи и на оборудовании операторов связи, вследствие чего малый бизнес, предоставляющий телекоммуникационные услуги, выведен из-под действия законодательства.

Для доступа к идентификационным данным абонента в большинстве случаев (за исключением, когда эти данные требуются для доступа к другим массивам персональных данных) судебный ордер не требуется.

В случае перехвата сообщений разведслужбами, он осуществляется, как правило, не в целенаправленно на физических лиц, а в определенных географических регионах целиком. Операторы связи обязаны устанавливать оборудование для перехвата в целях спецслужб (за счет государства) и организовать доступ к нему для сотрудников разведслужб. Тем не менее, с технической стороны, перехват сообщений ведется самим оператором связи, который в дальнейшем передает данные на оборудование спецслужб, позволяющее осуществлять поиск внутри массива данных по предопределенным категориям. После передачи копии, оператор связи обязан удалить массив данных.

При осуществлении физического доступа к хранимым данным количество лиц, которым предоставлен доступ, ограничивается законодательством до четырех человек – по два представителя оператора связи и правоохранительного органа.

Обязательства по передаче ключей шифрования в немецком законодательстве не предусмотрены.

В 2015 году был принят новый закон о хранении данных пользователей (в части информации о фактах соединения). Согласно новому закону операторы связи будут обязаны хранить геометки в течение 4 недель, другую информацию о фактах соединения, включая телефонные номера и IP-адреса, время и продолжительность сессий, текстовые сообщения в течение 10 недель. Хранение данных осуществляется за счет оператора связи, функции по хранению могут быть переданы третьей стороне, при условии соблюдения мер защиты. Законом предусмотрен механизм субсидирования или компенсаций данных расходов, однако пока непонятно, каким образом и в каких объемах

будут компенсироваться расходы. Закон должен вступить в силу 1 июля 2017 года, однако оспаривается в многочисленных судах в Германии и ЕС. Так решение Европейского суда справедливости от декабря 2016 года по делу Watson, признавшее несоответствующими законодательству ЕС законы о перехвате электронных коммуникаций Швеции и Великобритании, по мнению многих юристов относится и к новому немецкому закону. Кроме того, в октябре 2016 года Европейский суд справедливости вынес вердикт в деле Breyer против Германии, в котором признал, что динамические IP-адреса могут быть персональными данным, что также ставит под вопрос конституционность закона.

В апреле 2017 года Министерством юстиции был представлен законопроект о регулировании соцсетей(“NetzDG") для борьбы с фейковыми новостями. В рамках этого законопроекта «теле-медиа сервис-провайдеры, которые управляют коммерческой онлайн-платформой для обмена информацией между пользователями или ее публикации», с числом немецких пользователей более 2 млн будут обязаны не только блокировать или удалять контент, распространяющийся с нарушением законодательства, но и осуществлять хранение удаленного контента в течение 10 недель.

Наконец, весной 2017 года Министерство внутренних дел Германии выступило с инициативой распространить режим обязательного хранения информации о фактах соединений пользователей на интернет-сервисы, такие как Skype, WhatsApp, Facebook.

Осуществление надзора

Согласно УПК Германии и Закону о федеральной службе расследований, граждане должны быть уведомлены о фактах перехвата их коммуникаций, как можно скорее, в случае если это не повредит расследованию или безопасности самого гражданина. В течение двух недель с момента уведомления гражданин может подать иск в суд о проверке законности действий правоохранительных органов или жалобу на их действия. Аналогичные правила действуют и для решений региональных правоохранительных органов. Суды различных инстанций не пришли к единому выводу, может ли непосредственно сам оператор связи оспаривать решения о перехвате коммуникаций.

Судебный надзор в случае перехвата сообщений спецслужбами согласно Акту о статье 10 не предусмотрен, надзор осуществляется офисом Министра внутренних дел Германии и специальной Комиссией G10. Гражданин может быть уведомлен о проведении расследования в его отношении (и подать иск в суд) после его завершения, в случаях если это не представляет угрозу национальной безопасности.

Правоохранительные органы и спецслужбы не имеют права на прямой доступ к специальному оборудованию, установленному на объектах инфраструктуры операторов связи. При осуществлении доступа оператор связи

фиксирует информацию о должностных лицах, время доступа, массивы данных, к которым осуществлялся доступ и основание для него.

Понятийный аппарат

Оператор связи – компания, предоставляющая гражданам услуги в области телекоммуникаций на коммерческой основе.

Техники сбора данных – механизмы сбора голосовых и текстовых сообщений, интернет-трафика, доступа к идентификационным данным пользователей и информации о фактах соединения, для которых необходим судебный ордер или приказ высшего представителя одной из ветвей власти.

Информация об абонентах – собираемые в рамках законодательства данные, состоящие из

- Идентификаторы абонента;
- ФИО, адрес, день рождения абонента
- Дата и номер контракта
- Адрес проживания

Информация о фактах соединения – собираемые в рамках законодательства данные, состоящие из

- Идентификаторы коммуникационного оборудования;
- Технические характеристики, время, дата и длительность соединения;
- Сервисы, к которым обращался пользователь и поставщики этих сервисов;
- Получатель сообщений;
- Геометки

ETSI-ESB – технические интерфейсы для осуществления доступа к перехваченным электронным коммуникациям в соответствии с законодательством Германии.

TKÜV, TR TKÜV – законодательные, технические и организационные меры по осуществлению сбора электронных коммуникаций операторами связи для спецслужб.

Субъекты регулирования

Операторы связи:

- Обеспечивают сбор и хранение данных в соответствии с судебным или прокурорским ордером

- Обеспечивают технические и организационные меры по для осуществления перехвата и защищенного хранения электронных коммуникаций, доступа к ним правоохранительных органов и спецслужб
- Предоставляют доступ к сведениям об абоненте по законному запросу правоохранительных органов, в ручном и автоматическом режиме
- Устанавливают оборудование для осуществления перехвата и хранения электронных коммуникаций и осуществления доступа к ним на объекты собственной инфраструктуры за свой счет
- Исполняют предписанные меры технические и организационные меры по защите хранимых данных, включая шифрование и ограничение прав доступа, включая недоступность данных через телекоммуникационные сети.

Правоохранительные органы и спецслужбы

- Получают разрешения на доступ к собранным данным пользователей у судов, высших представителей ветвей власти, налоговой службы
- Соблюдают принципы пропорциональности и соответствие целям нормативного регулирования по сбору данных
- Уведомляют граждан о перехвате коммуникаций в целях осуществления надзора
- Сотрудничают с операторами связи для получения необходимых данных, не имеют права на прямой доступ к специальному оборудованию, установленному на объектах инфраструктуры операторов связи

Суды

- Выдают судебные ордера на сбор данных или перехват электронных коммуникаций
- Рассматривают иски граждан о законности и пропорциональности выданных ордеров на перехват коммуникаций

Комиссия G10

- Осуществляет надзор за спецслужбами в частности в области слежки за гражданами
- Уведомляют граждан о перехвате коммуникаций в целях осуществления надзора
- Проверяют законность и пропорциональность приказов о перехвате коммуникаций

Сбор и хранение данных пользователей телекоммуникационных услуг

Немецкий акт о телекоммуникациях (“TKG”) предписывает операторам связи хранить и предоставлять ручном и автоматическом режиме сведения об абонентах по запросу правоохранительных органов или спецслужб в целях, оговариваемых законодательством Германии. Данные об абонентах должны быть удалены незамедлительно после прекращения договорных отношений между оператором связи и абонентом.

Операторы связи обязаны осуществлять перехват и хранение электронных коммуникаций при наличии законного требования (судебного ордера) правоохранительных органов или прокуратуры. Сроки хранения информации о соединениях и содержания сообщений определяются судом в каждом конкретном случае.

Согласно закону о хранении данных пользователей, вступающему в силу с 1 июля 2017 года, операторы связи будут обязаны хранить следующую информацию о фактах соединения:

В течение 10 недель

- Идентификаторы пользователей и коммуникационного оборудования;
- Технические характеристики, время, дата и длительность соединения;
- Сервисы, к которым обращался пользователь и поставщики этих сервисов;
- Получатели сообщений;

В течение 4 недель – геометки.

Основания, меры и порядок ответственности операторов связи за нарушение порядка и правил сбора и хранения данных пользователей телекоммуникационных услуг

Нарушение правил сбора информации о пользователях, несанкционированный доступ к данным –

штраф в размере 38-58 тысяч евро, в случае несанкционированного доступа к данным – до 2 лет заключения.

Отказ от осуществления перехвата сообщений согласно судебному ордеру, отказ от хранения данных о пользователях согласно вступающему 1 июля 2017 года в силу закону – штраф до 500 тысяч евро.

Дания

Формирование национальной системы регулирования в области хранения данных

В Дании развитие законодательства и системы регуляторных мер в части хранения трафика осуществлялось и продолжает развиваться в русле политики Европейского Союза (ЕС) в этой области, включая Директиву 2006/24/ЕС «О сохранении данных, созданных или обработанных в связи с предоставлением общедоступных услуг электронной связи или сетей связи общего пользования» от 15 марта 2006 г., в 2014 г. отмененную решением Европейского Суда Справедливости

Однако основы правового режима хранения данных телекоммуникационными операторами в Дании были заложены ранее, еще в 2001 г. 6 июня 2002 г. был принят Закон №378 «О внесении поправок в уголовный кодекс, Закон об отправлении правосудия, Закон о рыночной конкуренции и правах потребителей услуг рынка телекоммуникаций, Закон о вооруженных силах и Закон об экстрадиции нарушителей правопорядка в Финляндию, Норвегию и Швецию»[34].

Закон был принят в рамках имплементации Международной конвенцией ООН о борьбе с финансированием терроризма от 9 декабря 1999 г., а также Решения Совета Безопасности ООН 1373 (2001) и других международных инициатив по борьбе с терроризмом на волне законодательной реакции на террористические атаки в 11 сентября 2001 г. Таким образом, первичным мотивом введения в национальное регуляторное поле механизмом хранения данных операторами отрасли телекоммуникаций в Дании, как и в большинстве стран мира, стала **борьба с терроризмом**.

Конкретно, Статьей 2 упомянутого закона были внесены поправки в Закон об отправлении правосудия, в том числе добавляющие в параграф 786 новый пункт, согласно которому операторы телекоммуникационных сетей и

[34] LOV nr 378 af 06/06/2002 Gældende. Lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige. https://www.retsinformation.dk/forms/r0710.aspx?id=1344

провайдеры телекоммуникационных услуг обязаны осуществлять запись и хранение **в течение одного года информации о телекоммуникациях (метаданных)** для содействия расследованию и судопроизводству по уголовным преступлениям[35].

Закон не вводил никакой системы уточняющих понятий и перечня информации подлежащей хранению, а также не уточнял круг правоохранительных органов, имеющих к ней доступ, порядок такого доступа и проч. Решение этой задачи в рамках той же Статьи 2 было делегировано на уровень подзаконных актов: так, указывалось, что министр юстиции, после консультаций с министром науки, технологий и развития, сформулирует подробные правила и требования в части записи и хранения данных и определит порядок взаимодействия провайдеров телекоммуникационных услуг с правоохранительными органами (LEAs) в части предоставления и раскрытия хранимой информации.

Закон №378 вступил в силу 1 июля 2002 г., однако разработка подзаконного акта, регламентирующего указанные вопросы, затянулась на четыре года. Задержка имела место по двум причинам[36]:

- Параллельно шел процесс разработки системы НПА, регулирующих обязательное хранение данных телекоммуникационными провайдерами, на уровне ЕС – датские регуляторы решили дождаться Директивы ЕС, чтобы иметь возможность принять национальные нормы, изначально адаптированные под нее.
- Национальные регуляторы столкнулись с техническими сложностями в процессе выработки концепции режима хранения данных, т.к. прежде не имели опыта в этой области.

В результате, 15 марта 2006 г. была принята Директива 2006/24/ЕС «О сохранении данных, которая вводила требования по хранению провайдерами телекоммуникационных услуг 6 категорий метаданных пользователей (категории A-F) в течение не менее шести месяцев и не более двух лет, начиная с даты коммуникации. Соответственно, датский режим хранения данных был

[35] Там же.

[36] https://ace-https://www.openrightsgroup.org/assets/files/legal/Data_Retention_status_table_updated_April_2015_uploaded_finalwithadditions.pdf

определен на уровне подзаконного акта уже в рамках этой «системы координат», заданных Директивой ЕС. 13 октября 2006 г. Министерство юстиции опубликовало Приказ о записи и хранении информации о телекоммуникационном трафике провайдерами электронных коммуникаций и услуг электронных коммуникаций (Приказ о хранении данных). Именно этот документ и определил основные моменты датского подхода к хранению данных телекоммуникационными провайдерами.

Категории информации, подлежащей хранению, в рамках Приказа о хранении данных 2006 г.

Согласно Приказу[37], провайдеры, предоставляющие конечным пользователям доступ к электронным коммуникациям и услуги электронных коммуникаций, обязаны осуществлять запись следующей информации в рамках коммуникаций **по стационарной или мобильной телефонной связи**, а также коммуникаций через сервисы передачи сообщений SMS, EMS и MMS:

1. Номер вызывающего абонента (номер A), а также имя и адрес зарегистрированного пользователя или подписчика соответствующей услуги.
2. Номер вызываемого абонента (номер B), имя и адрес зарегистрированного пользователя или подписчика соответствующей услуги.
3. Номер переадресации вызова (номер C), имя и адрес зарегистрированного пользователя или подписчика соответствующей услуги.
4. Отчеты о доставке сообщений.
5. Идентификаторы используемых для коммуникации устройств (номера идентификаторов IMSI иIMEI).
6. Ячейка(-и) сотовой связи, в соответствии с их меткой местоположения (идентификатор ячейки – Cell ID).
7. Данные, идентифицирующие географическое местоположение ячейки (ячеек) сотовой связи, к которой (-ым) подключен мобильный телефон на момент начала коммуникации.

[37] https://itpol.dk/sites/itpol.dk/files/TFR40200.pdf

8. Время начала и время окончания коммуникации.
9. Время первоначальной активации предоплаченной анонимной услуги и метка местоположения (идентификатор ячейки – Cell ID), с которого была активирована услуга.

Той же статьей Приказа определялся перечень подлежащей записи и хранению информации об инициировании и завершении сеансов передачи данных через Интернет:

1. IP-адреса, с которых осуществлялась отправка (передача) данных.
2. IP-адреса, на которые осуществлялась доставка (передача) данных.
3. Протокол передачи данных, задействованный в коммуникации (например, TCP или UDP).
4. Номер порта, с которого осуществлялась отправка интернет-трафика.
5. Номер порта, на который осуществлялась доставка интернет-трафика.
6. Метка времени начала и завершения сеанса коммуникации.

Первые 6 пунктов в совокупности формируют **режим регистрации IP-сессий (IP session logging)**, который является главной отличительной чертой датского подхода к хранению телекоммуникационных данных и с момента принятия Приказа вызвал бурные дискуссии в отрасли и гражданском обществе Дании (что позднее привело к отмене этого режима в 2014 г.).

Телекоммуникационным провайдерам предписывалось осуществлять запись и хранение данных **о первом и последнем пакете в каждой IP-сессии.** При этом в отношении режима регистрации IP-сессий в Приказе была предусмотрена альтернативная опция. В тех случаях, когда провайдер телекоммуникационных услуг по техническим причинам не может обеспечить выполнение требований по записи информации обо всех IP-сессиях конечных пользователей, в отношении него применяется механизм выборочной записи и хранения такой информации. Конкретно, устанавливается требование осуществлять запись и хранение **информации о каждом 500-м (1 из 500) пакете данных**, переданных в рамках сеанса коммуникации конечного пользователя. Де-факто большинство датских провайдеров 2007-2014 гг. использовали именно эту схему («1 из 500»).

Регистрация сессий должна была осуществляться **на границе сети провайдера**, где осуществляется обмен трафиком с другими интернет-провайдерами. Возможность осуществлять запись сессий именно на границе сети была важна для крупных провайдеров, так как позволяла сократить расходы на оборудование, необходимое для ведения регистрации IP-сессий. В частности, такая схема позволяла провайдерам обойтись без использования оборудования глубокой проверки сетевых пакетов (DPI).

Кроме того, в Приказе отдельно перечисляются подлежащие регистрации (записи) и хранению категории информации в отношении доступа конечного пользователя в Интернет:

1. Учетная запись пользователя.
2. Учетная запись и телефонный номер пользователя, осуществляющего коммуникацию в рамках публичной сети электронных коммуникаций.
3. Имя и адрес подписчика услуги или зарегистрированного пользователя, которому был присвоен соответствующий IP-адрес, идентификатор пользователя (User ID) или телефонный номер во время коммуникации.
4. Время начала и завершения коммуникации.

В дополнение к перечисленным категориям информации устанавливаются и другие специфические требования. Согласно секции 5.3. Приказа, в дополнение к информации о сеансах доступа в Интернет провайдер телекоммуникационных услуг должен обеспечить запись и хранение информации, которая позволяет идентифицировать точное географическое или физическое местонахождение точки доступа, через которую осуществлялся доступ, а также идентифицировать задействованное для обеспечения доступа коммуникационное оборудование. Данное требование, в частности, распространяется на точки доступа в публичных WiFi-сетях.

Сроки хранения информации в рамках определенных Приказом категорий не изменились и в соответствии с Законом №378 составляли1 год.

Соответствие режима хранения данных Директиве ЕС

Таким образом, Приказ от 13 октября 2006 г. сформировал весьма обширный режим записи и хранения данных о коммуникациях конечных пользователей провайдерами телекоммуникационных услуг. При этом можно по отдельным параметрам этот режим де-факто вышел за рамки режима, утвержденного Директивой 2006/24/ЕС «О сохранении данных, …». В частности, положения Приказа расширяют положения Директивы ЕС по крайней мере в следующих моментах:

- Режим регистрации IP-сессий, в том числе в выборочной модификации (информация об 1 пакете из 500) – не предусмотрен Директивой 2006/24/ЕС ни в какой части.
- Директива ЕС применяется в отношении «общедоступных услуг электронных коммуникаций или публичных коммуникационных сетей», тогда как действие Приказа от 13 октября 2006 г. распространялось на всех провайдеров услуг электронных коммуникаций, действующих на коммерческой основе, вне зависимости от того, являются ли их услуги общедоступными или нет. Исключения в части обязательств по хранению таких данных были сделаны лишь для 3 категорий субъектов:
    - Государственные учреждения;
    - Производственные помещения и прочие объекты работодателей, на которых предоставляется доступ к Интернету сотрудникам.
    - Государственные образовательные учреждения.

Все остальные виды учреждений, предоставляющих публичные услуги доступа к коммуникационной сети, должны были выполнять требования по записи и хранению данных – включая, например, кафе и рестораны, предоставляющие посетителям доступ по WiFi. Согласно комментариям Министерства юстиции к Закону №378 и Приказу 2006 г., требования по хранению данных были распространены на «непубличных провайдеров» с целью обеспечить необходимый уровень конкуренции между ними и провайдерами общедоступных услуг.

Оценки стоимости хранения данных

Регуляторный режим записи и хранения данных, введенный Приказом 2006 г., начал действовать в 2007 г. и частично был отменен лишь в 2014 г. после того как 8 апреля 2014 г. Европейский Суд Справедливости вынес решение[38], которое отменило действие Директивы 2006/24/ЕС «О сохранении данных, …». Т.е. датские телекоммуникационные операторы выполняли положения Приказа о хранении данных в течение 7 лет.

Комплексных и широко признанных датской телекоммуникационной отраслью и регуляторами оценок стоимости законодательства о хранении данных за этот период найти не удалось. По состоянию на 2013 г., совокупные (т.е. отслеживаемые с 2007 г. и вступления в силу Приказа о хранении данных) расходы телекоммуникационных провайдеров составили **порядка 250 млн датских крон (35-40 млн долл. США)[39].**

В отличие от Австралии и некоторых других стран, в Дании не была реализована какая-либо программа компенсации расходов телекоммуникационных провайдеров на выполнение требований регуляторов по записи и хранению данных.

Оценка эффективности режима записи и хранения данных

По экспертным оценкам на 2012 г., в рамках исполнения требований по хранению данных телекоммуникационные операторы Дании ежедневно генерировали порядка 400 записей по каждому пользователю, 90% из которых составляли записи регистрации IP-сессий[40]. По имеющимся данным на 2013 г. провайдерами в рамках исполнения законодательства было сделано в общей сложности **3,5 триллиона записей** (620 тыс. записей в пересчете на каждого гражданина Дании)[41].

При этом комплексная оценка эффективности механизмов записи и хранения данных в рамках Закона №378 и Приказа 2006 г. долгое время не осуществлялась. В 2012 г. новое правительство выдвинуло предложение о

[38] (European Court of Justice Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland of 8 April 2014)

[39] https://www.itpol.dk/notater/Danish-data-retention-evaluation-Feb13

[40] Там же.

[41] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26354.html

переносе ранее запланированного отчета об оценке регулирования в области хранения данных на 2014 г., однако такое предложение заблокировал национальный парламент.

В результате, в апреле 2012 г. правительство выпустило отчет, включавший в себя 10 примеров использования информации, записанной и хранимой в рамках требований к телекоммуникационным операторам, в деятельности органов правопорядка. Из 10 кейсов **записи данных о сеансах доступа в Интернет были использованы лишь в одном**, причем они ограничивались учетной записью, к которой был привязан IP-адрес. В остальных 9 кейсах использовались данные о коммуникациях по стационарной или мобильной телефонной связи, прежде всего данные географического местоположения ячеек сотовой связи, к которым подключен мобильный телефон на момент начала коммуникации. Эти данные использовались датской полицией в рамках расследования ряда преступлений, включая убийства и покушения на убийство.

В декабре правительство по запросу парламента опубликовало еще один отчет о выполнении законодательства по хранению данных, включавший новые описания кейсов использования полицией Дании информации о коммуникациях пользователей через Интернет. В отчете упоминаются 3 таких кейса[42]:

- Кейс с мошенничеством с сервисом электронных онлайн-платежей, описанный в предыдущем отчете правительства за весну 2012 г.
- Кейс с расследованием серии вооруженных ограблений. Однако де-факто кейс представляет собой пример использования записей о коммуникациях через мобильную телефонную связь, а не записей IP-сессий. Речь идет об идентификации личности правонарушителя, которая в итоге была осуществлена с использованием данных местоположения ячеек сотовой связи, к которым подключался его смартфон, в том числе для получения доступа в Интернет через мобильную сеть.
- Единственный кейс, когда ключевую роль в расследовании преступления сыграло использование записей регистрации IP-сессий, связан со случаем компьютерного мошенничества. Злоумышленники вывели через систему ДБО более 100 тыс. датских крон, взломав

[42] http://www.ft.dk/samling/20121/lovforslag/l142/bilag/2/1213533.pdf

устройство пользователя и инициировав транзакцию с него. Обнаружить факт неавторизованного доступа и совершения транзакции удалось как раз с помощью анализа данных регистрации IP-сессий.

В свою очередь, Служба безопасности и разведки Дании (PET), уполномоченная в области борьбы с терроризмом (что и являлось главной исходной целью принятия законодательства о хранении данных) в рамках отчета отметила, что механизм записи информации о коммуникациях через Интернет (включая регистрацию IP-сессий) использовался ей «в очень ограниченном количестве расследований»[43].

Таким образом, на данный момент публично был озвучен **только один случай реального применения механизма регистрации IP-сессий** (session logging) для расследования серьезного правонарушения. При этом, по различным оценкам, расходы на реализацию этого механизма (даже в формате «1 из 500») составляют значительную часть всех затрат телекоммуникационных провайдеров на выполнение требований законодательства по хранению данных.

Наконец, в отчете были отмечены значительные технические изъяны схемы по регистрации IP-сессий, связанные с ее осуществлением на границе сети провайдеров. По мере нарастающего внедрения технологий трансляции сетевых адресов на уровне провайдера (Carrier-Grade Network Address Translation (CG-NAT), прежде всего для организации услуг мобильного доступа в Интернет, разделять трафик индивидуальных клиентов по отдельным IP-адресам стало все более затруднительно, а во многих случаях невозможно. В итоге схема регистрации IP-сессий на границе сети, выгодная самим телекоммуникационным провайдерам, привела к серьезному снижению эффективности механизма хранения данных для использования его правоохранительными органами.

Отмены механизма регистрации IP-сессий и нынешняя ситуация

После принятия Европейским Судом Справедливости решения (European Court of Justice Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights

[43] Там же.

Ireland of 8 April 2014), отменившего действие Директивы 2006/24/ЕС «О сохранении данных…» датская система требований продолжала действовать в неизмененном виде в течение нескольких месяцев 2014 г.

2 июня 2014 г. правительство Дании представило 30-станичный правовой анализ Решения Европейского Суда Справедливости, в том числе включая интерпретацию Решения в отношении датских норм о хранении данных[44]. Согласно заключению правительства, Решение ЕСС, отменившее действие Директивы 2006/24/ЕС, в целом не затрагивало существующее в Дании законодательство о хранении данных и не являлось однозначным основанием для пересмотра либо отмены действующих в Дании НПА.

Однако 4 июня 2014 г. Министерство юстиции Дании в пресс-релизе[45] объявило о пересмотре действующих в стране правил хранения данных на уровне подзаконных актов. Конкретно, **были отменены положения Приказа о хранении данных от 2006 г.** в части регистрации IP-сессий (включая как механизм записи данных о первом и последнем пакете в сессии, так и схему «1 из 500»). При этом сам Приказ отменен не был и продолжает действовать в обновленном виде.

В пресс-релизе Министерства юстиции особо подчеркивалось, что решение о частичной отмене режима хранения данных никак не связано с Решением Европейского Суда Справедливости и упразднением Директивы 2006/24/ЕС, и обусловлено недостаточной эффективностью механизма регистрации IP-сессий и его низкой полезности для органов безопасности и охраны правопорядка.

Тем не менее, с 2015 г. представители правительства периодически озвучивают планы по повторному введению в датское законодательство новой, более совершенной с технической точки зрения схемы записи данных об IP-сессиях пользователей. Пересмотр подзаконных НПА в этой связи планировался на 2016 г., однако в итоге был отложен до разработки и принятия нового документа уровня ЕС, который бы заменил упраздненную Директиву 2006/24/ЕС.

---

[44] http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2014/Notat%20om%20logningsdirektivet.pdf

[45] http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2014/justitsministeren-oph%C3%A6ver-reglerne-om-sessionslogning

Нидерланды

Цели и принципы нормативно-правового регулирования

Обязательства по хранению данных пользователей впервые появились в законодательстве Нидерландов в 2009 году с принятием Telecommunications Data Retention Act (TDRA), в соответствии с европейской директивой по хранению данных, и ушли из законодательства, когда директива была признана несоответствующей законодательству о защите персональных данных Европейским судом справедливости в 2014 году, то было подтверждено местным судом в Гааге.

TDRA и Telecommunications Act 2009 года предписывали операторам связи хранить информацию о фактах соединения на телефонных, фиксированных и мобильных сетях в течение года, а информацию о фактах интернет-соединений – в течение 6 месяцев. Основная цель данных положений – борьба с серьезными преступлениями (согласно законодательству страны, это преступления с минимальным сроком заключения в 4 года). Тем не менее, одной из причин, по которым данный закон был признан не соответствующим конституции местным судом стало несоответствие реальной практики заявленным целям. Например, правоохранительные органы пользовались законом в случаях кражи велосипедов, что вряд ли можно считать серьезным преступлением. При этом для доступа к хранимым данным не требовалось разрешение суда или независимой комиссии, что нарушало статьи 7 и 8 Декларации о фундаментальных правах ЕС (право на частную жизнь и на защиту персональных данных). Более того, TDRA не содержал положений о способах защиты хранимых данных и разрешал передачу данных за пределы ЕС, в частности обмен данными между спецслужбами.

Результатом данного судебного процесса стало создание в 2015 году нового проекта закона, учитывающего замечания суда. Так появились прямо прописанные условия доступа к хранимым данным (серьезность преступления, судебный ордер), а хранимая информация была разделена на два типа:

информация о фактах соединения (дата и время, продолжительность, геометка) и информация о пользователях (имя, идентификаторы). Законопроект был внесен в парламент в феврале 2017 года (Intelligence and Security Services Act). Вместе с тем, далеко не все обещания по изменению законодательства были выполнены. Так законопроект позволял спецслужбам передавать данных пользователей за пределы ЕС и разрешал доступ к различным базам данных правительственных и финансовых организаций без наличия судебного ордера. Сроки хранения данных операторами связи остались неизменными (6 и 12 месяцев), но появилось право спецслужб требовать у компаний ключи шифрования. Впрочем, законопроект не требовал хранить содержание сообщений пользователей.

По результатам обсуждения в парламенте закон был признан спорным, и его дальнейшая судьба была отложена до следующих выборов в стране.

Таким образом, действующее законодательство Нидерландов (Dutch Code of Criminal Procedure, 1994 и Intelligence and Security Services Act 2002) не предполагает обязательств по обязательному хранению пользовательских данных операторами связи. Однако, они должны обеспечивать возможность перехвата электронных коммуникаций в случае наличия судебного ордера, выдаваемого по запросу прокуратуры в случае расследований серьезных преступлений. При этом сбор и хранение данных происходит за счет операторов связи.

Министр внутренних дел также может авторизовать перехват электронных коммуникаций Агентством национальной безопасности Королевства (General Intelligence and Security Agency “AIVD”), а Министр обороны – военной разведке (Military Intelligence and Security Agency “MIVD”) в целях национальной безопасности. В случае если данные зашифрованы, компании обязаны помогать спецслужбам в их расшифровке. При этом подобные приказы Министров не могут быть оспорены в суде. Максимальный срок перехвата коммуникаций по судебному ордеру или приказу министра составляет три месяца, с возможностью продления на дополнительные три месяца. Для перехвата электронных коммуникаций некоторых категорий граждан, таких как журналисты или адвокаты, требуется авторизация специального суда в Гааге.

Сбор и хранение данных пользователей телекоммуникационных услуг

Действующее законодательство не содержит положений об обязательном сборе и хранении данных пользователей телекоммуникационных услуг.

Основания, меры и порядок ответственности операторов связи за нарушение порядка и правил сбора и хранения данных пользователей телекоммуникационных услуг

Отказ от перехвата электронных сообщений в соответствии с ордером суда приравнивается к вмешательству в законные действия полиции, что предполагает уголовное наказание в виде штрафа и заключения сроком до трех месяцев.

Незаконный перехват электронных сообщений карается штрафом в размере до 20 тысяч евро.

Франция

Цели и принципы нормативно-правового регулирования

Система перехвата электронных коммуникаций была создана в качестве меры по борьбе с серьезными преступлениями и терроризмом. При этом существующее регулирования является результатом нескольких волн законов, причиной принятия которых служили громкие террористические акты (такие как теракты в США 9/11, взрывы поездов в Мадриде в 2004, убийства в редакции Шарли Эбдо 2015, теракт в клубе Батаклан 2016).

Режимы сбора, перехвата и хранения данных пользователей можно разделить на две части: **судебные и внесудебные**.

Уголовный кодекс Франции позволяет судам выдать ордера на перехват электронных сообщений, включая голосовые, текстовые, видео и интернет-трафик с 1991 года (Закон №91-646). Впрочем, перехват сообщений практиковался и до 1991 года без каких-либо законных оснований, пока Европейский суд по правам человека не вынес решение против Франции (CEDH, 24 April 1990, Huvig and Kruslin c/ France). С 2011 (указ №2011-21) возможен сбор информации о фактах соединения у интернет-провайдеров и хостингов. При этом суд может разрешить использование специальных технических средств, spyware, на устройствах подозреваемых (закон №2011-267). В 2014 году (закон №2014-1353 в список видов коммуникаций для перехвата были добавлены VoIP-сервисы. Наконец, в 2016 году (Закон № 2016-731) полномочия судов в части использования специальных технических средств были расширены до установки оборудования для перехвата данных подозреваемых, подключаемого к информационным системам операторов связи. Ордера на перехват выдаются сроком до четыре месяцев и могут быть продлены на срок до года (два года при серьезных преступлениях).

Внесудебный перехват коммуникаций также подвергся реформе благодаря решению суда от 1990 года. Так закон №91-646 1991 года позволяет Премьер-министру выдавать приказы на перехват под контролем независимой комиссии (CNCIS). Закон № 2004-669, принятый вскоре после терактов в Мадриде расширил действие приказов на все электронные коммуникации.

Закон № 2006-64 разрешил доступ полиции к хранимым электронным коммуникациям операторов связи (а с 2011 года – хостинг-провайдеров) в рамках антитеррористических расследований, ранее доступной только судебным властям. С 2013 года (закон № 2013-1168) доступ к информациям о фактах соединений, включая историю соединений и геометки, получили несколько правительственных агентств, связанных с обеспечением национальной безопасности. Закон №2015-912 сделал законными различные методы и технические средства массовой слежки, фактически применявшиеся различными французскими спецслужбами. Более того, закон установил обязанности для операторов связи по установке «черных ящиков» для сбора и

анализа метаданных в реальном времени (и перехвата коммуникаций в случае возникновения подозрений террористической угрозы) и прямого доступа спецслужб к этим данным. Несмотря на серьезные протесты и возможное несоответствие законам ЕС, данные меры были подтверждены Государственным советом Франции. Наконец, закон №2015-1556 расширил полномочия спецслужб по перехвату международных электронных коммуникаций.

Несмотря на то, что сразу после принятия закона 2015 года, президент Олланд обратился за подтверждением в Государственный совет Франции (как правило, верховная судебная инстанция в этой стране выносит решения о соответствии конституции по еще не вступившим в действие законам), и вступил в действие, с небольшими изменениями. Так появилась обязательное подтверждение приказов о перехвате электронных коммуникаций независимой комиссией.

Против принятия закона выступил Совет ООН по правам человека (United Nations committee for human rights)[46].

Тем не менее, созданная во Франции система перехвата и хранения данных пользователей оспаривалась в судах нескольких инстанций, и ее легальный статус находится под вопросом.

Так несколько представителей гражданского общества оспаривают положения закона в Высшем административном суде Франции на несоответствие Европейской директиве по защите персональных данных, используя решение Европейского суда справедливости по процессу Digital Rights Ireland, приведшему к отмене общеевропейской Data retention directive и решения Европейского суда по правам человека, уже приведшие к отмене многих похожих национальных законов по всему ЕС. Представители истцов требуют, как минимум, чтобы власти Франции обратились в Европейский суд справедливости для проверки соответствия национального законодательства законам ЕС, как предписывает, в частности, Декларация фундаментальных прав граждан ЕС. Решение Европейского суда справедливости по делу *Watson* в декабре 2016 года, признавшее несоответствующими законодательству ЕС законы о перехвате электронных коммуникаций Швеции и Великобритании, также привели к усилению судебного давления на Францию. Впрочем, до сих

[46] http://tbinternet.ohchr.org/_layouts/treatybodyexternal/SessionDetails1.aspx?SessionID=899&Lang=en

пор французские исполнительные и судебные власти предпочитали игнорировать решения судов ЕС по этому вопросу. Основными претензиями со стороны властей ЕС в настоящий момент является отсутствие необходимости судебного ордера, крайне ограниченные возможности пользователей по опротестованию решения о перехвате коммуникаций и отсутствие ограничений по сбору данных и их защите, в том числе для иностранных официальных лиц, журналистов, адвокатов, врачей и других особых категорий граждан. На текущий момент Государственный совет постановил рассмотреть необходимость изменения законодательства к декабрю 2017 года.

В действующем законодательстве выделяются следующие цели для внесудебного перехвата и хранения данных пользователей:

- Обеспечение национальной безопасности, независимости и территориальной целостности;
- Важные интересы во внешней политике, имплементация европейских и международных обязательств Франции, предотвращение всех форм иностранного вмешательства во внутренние дела государства;
- Важные экономические, промышленные и научные интересы Франции (т.е. экономический и промышленный шпионаж);
- Борьба с терроризмом;
- Борьба с насильственным изменением конституционного строя;
- Борьба с организованной преступностью и деятельностью запрещенных организаций;
- Борьба с массовыми беспорядками;
- Борьба с распространением оружия массового поражения.

Осуществление надзора

Надзор за исполнением функций по перехвату и хранению электронных коммуникаций осуществляется Национальной комиссией по надзору за техниками по сбору данных (CNCTR). Комиссия состоит из четырех членов парламента, по выбору президента; четырех судей из обоих ветвей суда, по выбору Государственного совета и Кассационной коллегии; одного технического

эксперта, по выбору Национального регулятора в области связи и коммуникаций. CNCTR обязана в течение 24 часов вынести решение относительно приказов премьер-министра, однако это решение не является обязательным к исполнению. Комиссия также имеет доступ для аудита ко всем хранимым в рамках исполнения законодательства данным, и может выносить рекомендации премьер-министру по результатам аудита.

Возмещение ущерба

Граждане Франции, кого коснулись меры по перехвату электронных коммуникаций, могут подать жалобу в CNCTR, а в случае отклонения жалобы комиссией – иск в Государственный совет Франции. Однако истец не получает доступа к документам, приведшим к открытию расследования в его отношении; режим секретности распространяется и на заседания Государственного совета по делу истца.

Понятийный аппарат

Техники сбора данных – механизмы сбора голосовых и текстовых сообщений, интернет-трафика, доступа к идентификационным данным пользователей и информации о фактах соединения, для которых необходим судебный ордер или приказ премьер-министра.

Устройства для сканирования телекоммуникационных сетей – «черные ящики», устанавливаемые на объекты инфраструктуры операторов связи и хостинг-провайдеров в целях обнаружения террористической активности путем автоматизированного сбора и анализа метаданных пользователей в реальном времени с использованием технологии DPI.

Эксплуатация компьютерных сетей – использование специальных технических и программных средств для доступа, сбора, хранения и передачи данных с устройств подозреваемых, для которых необходим судебный ордер или приказ премьер-министра.

Наблюдение за международными коммуникациями – техники сбора данных для коммуникаций, исходящих из иностранных государств или

передаваемых заграницу, то есть с использованием иностранных технических идентификаторов.

Информация о фактах соединения – собираемые в рамках законодательства данные, состоящие из следующих компонентов:

- идентификаторы пользователей;
- идентификаторы коммуникационного оборудования;
- технические характеристики, время, дата и длительность соединения;
- сервисы, к которым обращался пользователь и поставщики этих сервисов;
- получатель сообщений;
- геометки.

Круг субъектов, которые принимают участие в исполнении закона

1. Операторы связи:
   - обеспечивают сбор и хранение данных в соответствии с судебным или прокурорским ордером, приказом премьер-министра сроком, устанавливаемым законодательством;
   - назначают квалифицированный персонал для осуществления перехвата электронных коммуникаций;
   - устанавливают устройства для сканирования телекоммуникационных сетей на объекты собственной инфраструктуры за свой счет.

2. Хостинг-провайдеры
   - обеспечивают сбор и хранение данных в соответствии с приказом премьер-министра сроком, устанавливаемым законодательством;
   - назначают квалифицированный персонал для осуществления перехвата электронных коммуникаций;
   - устанавливают устройства для сканирования телекоммуникационных сетей на объекты собственной инфраструктуры за свой счет.

3. Интернет-компании
    - обеспечивают сбор и хранение данных в соответствии с приказом премьер-министра сроком, устанавливаемым законодательством;
    - назначают квалифицированный персонал для осуществления перехвата электронных коммуникаций.

4. Комиссия по надзору за сбором данных (CNCTR)
    - выносит решения о соответствии приказов по сбору данных или перехвату коммуникаций законодательству страны
    - проводит аудит по результатам исполнения приказов
    - подает жалобы в Государственный совет в случае несогласия с приказами

5. Правоохранительные органы и спецслужбы
    - получают разрешения на доступ к собранным данным пользователей у судов, премьер-министра, CNCTR
    - соблюдают принципы пропорциональности и соответствие целям нормативного регулирования по сбору данных.
6. Суды
    - выдают судебные ордера на сбор данных или перехват электронных коммуникаций;
    - выдают ордера на предоставление ключей шифрования при необходимости для проведения расследования.

Сбор и хранение данных пользователей телекоммуникационных услуг

Обязательства по хранению данных об электронных коммуникациях появились в 2001 году (закон № 2001-1062). Так операторам связи *было разрешено* хранить информацию о фактах соединений в течение одного года в

целях биллинга, исследовательских целях или устранения нарушений законодательства.

В 2006 году антитеррористический закон расширил обязательства по хранению, предоставив доступ полиции к данным и обязал хранить информацию о фактах соединения все организации, обеспечивающие доступ в интернет, включая интернет-кафе, отели, рестораны и пр. Сбор содержания сообщений был строго запрещен. Затраты на хранение метаданных компенсируются государством.

В 2015 году срок хранения метаданных был увеличен до 5 лет, а срок хранения содержания сообщений, собираемых согласно законодательству, был установлен в один месяц с момента сбора информации (в случае, если содержание зашифровано – до 6 лет). Данные, собранные с помощью устройства для сканирования телекоммуникационных сетей хранятся в течение двух месяцев (срок хранения может быть продлен приказом премьер-министра. В случае иностранных коммуникаций, содержание сообщений хранится сроком до года, метаданные – сроком до 6 лет, зашифрованная информация – сроком до 8 лет.

Основания, меры и порядок ответственности операторов связи за нарушение порядка и правил сбора и хранения данных пользователей телекоммуникационных услуг

Разглашение информации о проводимых мерах по сбору или перехвату электронных коммуникаций: штраф до 75 тысяч евро и тюремное заключение сроком до года

Отказ от сотрудничества с правоохранительными органами по сбору или перехвату электронных коммуникаций или осуществлению доступа к хранимым данным: штраф до 750 тысяч евро и тюремное заключение сроком до года.

Отказ от предоставления ключей шифрования суду: штраф до 270 тысяч евро и тюремное заключение сроком до трех лет, 450 тысяч евро и пяти лет в случае если отказ не позволил предотвратить преступление или уменьшить его последствия.

Европейский Союз

Анализ правового регулирования защиты данных в рамках Европейского Союза целесообразно предварить комментариями общего характера[47].

Европейский Союз является интеграционным региональным образованием и его следует рассматривать как международную организацию, несмотря на то, что Европейский Союз «выходит за рамки» легитимного понятия международной организации. Это связано с тем, что формально-юридически в организационном плане Европейский Союз представляет собой объединение двух международных организаций – Европейское сообщество и Европейское сообщество по атомной энергии (Евратом).

Договор о Европейском Союзе и Договор об учреждении Европейского Сообщества 2007 г. (2007/C 306/01) – Лиссабонский Договор – закрепил исходное положение о том, что Европейский Союз рассматривается как правопреемник Европейского сообщества и признает параллельное существование Евратома, и, таким образом рассматривает Европейский Союз как *единую* организацию. Соответственно, Европейский Союз, согласно его учредительными документам (учредительный договор, устав), в институциональном плане – правомерно считать международной межгосударственной организацией. Европейский Союз в настоящее время объединяет 28 государств-членов (включая Великобританию).

Европейский Союз является «наднациональной» международной организацией и объем суверенных прав, которые государства-члены передали Европейскому Союзу, не имеет аналогов в истории международных организаций. В практическом плане «наднациональный» характер Европейского Союза означает, что:

- руководящие органы этой международной организации вправе принимать решения (юридические акты), обязательные для государств-членов, т.е. наделены правотворческими функциями;

[47] ДИРЕКТИВА (ЕС) 2016/1148 ЕВРОПЕЙСКОГО ПАРЛАМЕНТА И СОВЕТА От 6 июля 2016 года Касающиеся мер по обеспечению высокого общего уровня безопасности сетевых и информационных систем http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

- государства-члены интегрируют в национальные правопорядки юридические акты, принятые в рамках Европейского Союза;
- акты Европейского Союза обязательны для правоприменительных органов государств-членов (административные органы, суды);
- лица (физические/юридические) государств-членов вправе ссылаться на юридические акты Европейского Союза, как в рамках своих национальных органов, так и в рамках Суда справедливости Европейского Союза (*Court of Justice of the European Union, CJEU*), при этом решения Суда справедливости Европейского Союза носят прецедентный характер.

Суд справедливости Европейского Союза (далее – «Европейский Суд Справедливости») в одном из своих основополагающих решений установил, что Европейское сообщество является «новым правопорядком международного права, субъектами которого являются не только государства-члены, но и лица», а в случае коллизии права Европейского Союза и национального права государства-члена, право Европейского Союза имеет приоритет и применяется в *конкретном случае* вместо национального права. Вместе с тем право Европейского Союза в целом не отменяет национальное право государства-члена[48].

Таким образом, Европейский Союз – международная организация, деятельность которой основана на «уникальном объединении государств», поскольку государства-члены предоставили правотворческие и правоприменительные полномочия органам Европейского Союза, согласились на приоритетное применение права Европейского Союза. Обобщенно, совокупность именно этих характеристик означает *наднациональность* Европейского Союза.

Для настоящего исследования важно отметить, что правовое регулирование сферы защиты данных в Европейском Союзе фактически насчитывает более 20 лет. Основными правовыми актами Европейского права в рассматриваемой сфере являются Директивы и Рекомендации Европейского Парламента и Совета в соответствующей сфере отношений.

[48] EuGH, Slg 1963, 1, 24f (van Gend & Loos)

Условно можно сказать, что правовое регулирование сферы защиты данных в Европейском Союзе сформировало некую «европейскую модель», которую, несомненно, следует рассматривать как «стандарт защиты данных». Однако этот стандарт применим в рамках этого регионального интеграционного объединения, хотя и обладающего «наднациональными» характеристиками.

Во многих странах мира действуют законы о защите данных, вместе с тем в настоящее время не существует некоего «глобального стандарта» или «международной модели» защиты данных. В этом смысле гармонизация национального законодательства в сфере защиты данных в ближайшей перспективе вряд ли достижима. Гармонизация национального законодательства в сфере защиты данных усложнена тем, что «национальные модели» во многом находятся в стадии формирования, а полная или частичная рецепции существующих «моделей» сопряжена, прежде всего с тем, что понятийно-терминологический аппарат нормотворческого процесса – различен.

Ключевые понятия: «защита данных», «конфиденциальность информации», «конфиденциальность данных», «сбор, обработка, хранение данных», «передача данных» и т.д., в различных юрисдикциях содержательно определены по-разному. Более того, правовое значение обозначенных понятий нередко существенно различается, что во многом обусловлено политико-правовыми «предпочтениями» того или иного государства в конкретный исторический период.

Важно обратить внимание, что «защита данных» – это система, которая не может и не должна быть разбита на некие «составные части», к примеру, «конфиденциальность данных» – «сбор данных»; «сбор и обработка данных» – «хранение и передача данных»; «защита данных – «хранение данных» и т.д. Именно в этом контексте следует подчеркнуть значение (прежде всего правовое) сформированной системы «европейской модели» защиты данных.

Система «европейской модели» защиты данных основана на нормативно-правовом комплексе, включающего набор базовых принципов обработки данных (принципы справедливой информации) и набор основных прав защиты данных (персональные данные, информация, доступ, исправление данных и т.д.). Кроме того, регуляторный механизм этого нормативно-правового комплекса, с одной стороны, закреплен в международных нормативных актах, директивных

документах органов Европейского Союза, с другой стороны, имплементирован в национальное законодательство стран-членов Европейского Союза.

8 апреля 2014 г. Европейский Суд Справедливости вынес решение (*European Court of Justice Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland of 8 April 2014*), которое фактически привело существенному изменению подходов в регулировании сферы защиты данных, а также их сбора, хранения и обработки[49]. Речь идет о том, что Европейский Суд Справедливости отменил Директиву 2006/24/ЕС «О сохранении данных, созданных или обработанных в связи с предоставлением общедоступных услуг электронной связи или сетей связи общего пользования» (*Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks*), принятую 15 марта 2006 г. Европейским Парламентом и Советом.

Европейский Суд Справедливости счел несовместимым с правом Европейского Союза, что для борьбы с преступностью закреплено общее и неизбирательное хранение всех данных о трафике и местоположении абонентов и зарегистрированных пользователей, связанных со всеми средствами электронной связи.

В настоящее время анализируются последствия приятого решения, и соответствующие органы Европейского Союза комплексно решают вопросы, относительно того, каким образом право Европейского Союза будет регулировать отношения в сфере хранении данных. Целый ряд нормативно-правовых актов на уровне Европейского Союза уже принят в настоящее время. Однако, прежде чем обратиться к их рассмотрению, целесообразно рассмотреть основные положения Директивы 2006/24/ЕС «О сохранении данных, созданных или обработанных в связи с предоставлением общедоступных услуг электронной связи или сетей связи общего пользования» (далее – «Директива 2006/24/ЕС»), поскольку важно понять причины ее отмены Европейским Судом Справедливости.

Директива 2006/24/ЕС дополнила ранее принятую Директиву Европейского Парламента и Совета 12 июля 2002 г. связанную с обработкой

[49] European Court of Justice Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland of 8 April 2014

персональных данных и защитой конфиденциальности в секторе электронных коммуникаций (*Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications*). Кроме того Директива 2006/24/ЕС была направлена на гармонизацию законодательства государств-членов относительно правового регулирования оказания общедоступных услуг электронной связи или сетей связи общего пользования в контексте сохранении данных, созданных или обработанных в связи с предоставлением таких услуг.

Директива 2006/24/ЕС предусматривала, что сохранение данных, созданных или обработанных в связи с предоставлением обозначенных услуг, осуществляется в целях обеспечения расследования, обнаружения и судебного преследования за серьезные преступления, в соответствии с порядком, установленным в национальном праве каждого государства-члена Европейского Союза. Директива 2006/24/ЕС относилась к данным о трафике, данных о местоположении, а также информации, связанной с такими данными и распространялась на юридические и физические лица в целях идентификации абонента или зарегистрированного пользователя. Директива 2006/24/ЕС не распространялась на содержание электронных сообщений (контент), включая информацию, полученную с использованием сети электронной связи.

В Директиве 2006/24/ЕС были операционализированы следующие понятия:

- «данные» (*data*) – означают данные о трафике и данные о месторасположении, а также связанные с ними данные необходимые для идентификации абонента или пользователя;
- «пользователь (*user*) – означает любое юридическое или физическое лицо, использующее общедоступные услуги электронной, для частных или предпринимательских целей, при использовании которых нет необходимости быть подписчиком таких услуг.
- «телефонные услуги» (*telephone service*) – означают вызовы (включая голосовые, голосовые сообщения, телеконференцсвязь и данные о вызовах), дополнительные услуги, включая переадресацию звонков и перевод соединения на телефон третьего абонента (переадресация вызовов типа «call transfer») и услуги обмена сообщениями и услуги

мультимедийных сервисов (включая услуги коротких сообщений, расширенные медийные услуги и мультимедийные услуги);

- «идентификатор пользователя» (*user ID*) – означает уникальный идентификатор, присвоенный лицам, когда они подписываются или регистрируются для доступа к интернету или услуг интернет-комуникаций;
- «идентификатор ячейки» (*cell ID*) – означает идентификатор ячейки, с которой был инициирован вызов мобильной телефонной связи или в которой он завершен;
- «неудачная попытка вызова (*unsuccessful call attempt*) – означает связь, при которой телефонный звонок успешно подключен, но не отвечает, или было вмешательство в управление сетью которой звонок завершен;

Директива 2006/24/ЕС предписывала, что государства-члены принимают меры для обеспечения того, чтобы данные, хранящиеся в соответствии с этой Директивой, предоставлялись только компетентным национальным органам в конкретных случаях и в соответствии с национальным законодательством. Процедуры, которым необходимо следовать, и условия, которые должны быть выполнены для получения доступа к хранящимся данным (в соответствии с требованиями необходимости и соразмерности), определяются каждым государством-членом в его национальном праве. При этом следовало учитывать соответствующие положения права Европейского Союза или международных договоров и, в частности, толкования Европейского суда по правам человека[50].

Ключевое значение имеют нормативные положения **статьи 5** Директивы 2006/24/ЕС в которой закреплены следующие нормативные положения.

Все данные, подлежащие хранению, распределены по соответствующим категориям. Предусмотрено, что государства-члены должны обеспечить сохранение всех «категорированных» данных. Закреплено 6 категорий.

К **категории «А»** отнесены данные, необходимые для обнаружения и идентификации источника сообщения:

[50] Европейский суда по правам человека, созданный для регулировании отношений, вытекающих и связанных с реализацией Конвенции Света Европы «О защите прав человека и основных свобод» (Заключена в г. Риме 04.11.1950, с изм. от 13.05.2004).

1) в отношении стационарной телефонной сети и мобильной телефонии: (i) номер вызывающего телефона; (ii) имя и адрес абонента или зарегистрированного пользователя;

2) в отношении доступа к интернету, электронной почты в интернете и интернет-телефонии: (i) присвоенный идентификатор пользователя (ID(s) allocated); (ii) присвоенный идентификатор пользователя и номер телефона, предназначенный для любой связи, входящей в общую телефонную сеть; (iii)

имя и адрес абонента или зарегистрированного пользователя, которому был присвоен IP-адрес, идентификатор или номер телефона, использованного во время связи.

К **категории «B»** отнесены данные, необходимые, для идентификации адресата коммуникации:

1) в отношении стационарной телефонной сети и мобильной телефонии: (i) номер (номера), набранный номер (номер телефона), а также, в случаях, связанных с дополнительными услугами, такими как переадресация вызова или перевод соединения, номер или номера, на которые направлен вызов; (ii) имя и адрес абонента (абонентов) или зарегистрированного пользователя (пользователей), а также присвоенный идентификатор пользователя (ID);

2) в отношении электронной почты в интернете и интернет-телефонии: (i) присвоенный идентификатор пользователя или номер телефона предполагаемого получателя (получателей) телефонного интернет-вызова; (ii) имя (имена) и адрес (адреса) абонента (абонентов) и присвоенный идентификатор пользователя (ID) пользователя предполагаемого получателя сообщения.

К **категории «C»** отнесены данные, необходимые, для идентификации даты, времени, длительности коммуникации:

1) в отношении стационарной телефонной сети и мобильной телефонии – дата, время начала и конца коммуникации;

2) в отношении доступа к интернету, электронной почты и интернет-телефонии: (i) дата и время входа в интернет и выхода из интернета по услугам доступа в интернет с учетом определенного часового пояса и с IP-адреса, динамически, или статически определенном провайдером услуг доступа в интернет для коммуникации, а также присвоенный идентификатор пользователя (ID) абонента или зарегистрированного пользователя; (ii) дата и время входа в

интернет и выхода из интернета по услугам электронной почты или инетрнет-телефонии с учетом определенного часового пояса.

К **категории «D»** отнесены данные необходимые, для идентификации типа коммуникации:

1) в отношении стационарной телефонной сети и мобильной телефонии: использованная служба телефонной связи;

2) в отношении электронной почты и интернет-телефонии: использованные интернет-услуги.

К **категории «E»** отнесены данные необходимые, для идентификации коммуникационного оборудования пользователей или того, что подразумевается под таким оборудованием:

1) В отношении стационарной телефонной сети – вызываемые телефонные номера и вызывающие телефонные номера;

2) в отношении мобильной телефонии: (i) вызываемые телефонные номера и вызывающие телефонные номера; (ii) Международная идентификация мобильного абонента (IMSI) вызывающей стороны; (iii) Международный идентификатор мобильного оборудования (IMEI) вызывающей стороны; (iv) Международная идентификация мобильного абонента (IMSI) вызываемой стороны; (v) Международный идентификатор мобильного оборудования (IMEI) вызываемой стороны; (vi) в случае предоплаченных анонимных услуг – дата и время первоначальной активации услуги и метка местоположения (идентификатор ячейки – Cell ID), с которого была активирована услуга;

3) в отношении доступа к интернету, электронной почты в интернете и интернет-телефонии: (i) номер вызывающего телефона для коммутируемого доступа (доступ по телефонной линии); (ii) цифровая абонентская линия (DSL) или другая конечная точка отправителя сообщения;

К **категории «F»** отнесены данные необходимые, для идентификации местоположения оборудования мобильной связи:

1) метка местоположения (идентификатор ячейки – Cell ID) начала связи;

2) данные, идентифицирующие географическое местоположение ячеек, в соответствии с их меткой местоположения (идентификатор ячейки – Cell ID) в течение периода, для которого сохраняются данные связи.

Обязательства государств-членов ЕС по хранению данных охватывает хранение всех обозначенных выше данных (статья 5), а также хранение данных

«неуспешных попыток вызова», если эти данные создаются или обрабатываются и сохраняются (в отношении телефонных данных) или регистрируются (в отношении интернет-данных) провайдерами общедоступных услуг электронной связи или сетей связи общего пользования в пределах юрисдикции соответствующего государства-члена в процессе предоставления соответствующих услуг связи.

Директива 2006/24/ЕС обязывала хранить данные, касающиеся несвязанных вызовов; учитывая, что обязательства провайдеров услуг электронных коммуникаций должны быть пропорциональными. Директива 2006/24/ЕС также предусматривала, чтобы провайдеры услуг электронных коммуникаций хранили только такие данные, которые создаются или обрабатываются в процессе предоставления ими услуг связи. Если данные не создаются или не обрабатываются провайдерами услуг электронных коммуникаций, у них не возникает обязательств по хранению этих данных. При этом Директива 2006/24/ЕС не ставила цели гармонизировать «технологии хранения данных», и этот выбор должен быть осуществлен на национальном уровне.

Директива 2006/24/ЕС устанавливала, что государства-члены Европейского Союза обеспечивают хранение всех данных, предусмотренных в статье 5, т.е. входящих в шесть вышеперечисленных категорий и определяла срок – все эти данные должны храниться в течение не менее шести месяцев и не более двух лет, начиная с даты коммуникации.

Защита данных и безопасность данных, согласно Директиве 2006/24/ЕС, должна осуществляться без ущерба действующих Директив Европейского Союза, связанных с рассматриваемой сферой отношений, и обеспечиваться государством-членом Европейского Союза. При этом каждое государство-член должно обеспечить, чтобы поставщики общедоступных услуг электронной связи или сетей связи общего пользования связи соблюдали следующие принципы безопасности подлежащих хранению данных:

а) хранящиеся данные должны быть того же качества и обладать той же степени безопасности и защиты, что и данные в сети;

в) данные должны быть подвергнуты соответствующим техническим мерам и структурированы для их защиты от случайного или незаконного

уничтожения, случайной утраты или изменения или несанкционированного или незаконного хранения, обработки, доступа или раскрытия;

c) данные должны быть подвергнуты соответствующим техническим мерам и структурированы, так, чтобы доступ к ним был возможен только для уполномоченным лиц;

d) данные, за исключением тех, которые были доступны и сохранены, должны быть уничтожены в конце периода удержания.

Директива 2006/24/ЕС закрепляла, что государств-членов Европейского Союза обязаны обеспечить хранение данных, предусмотренных в Статье 5, и эти данные должны храниться таким образом, чтобы данные и любая другая необходимая информация, касающаяся таких данных, могли быть переданы по запросу компетентным органам без неоправданной задержки.

Принятия Директивы обосновывалось, в том числе тем, что во многих европейских странах на протяжении многих лет данные удалялись как только они теряли свое предназначение для целей выставления счетов. После усиления террористических нападений в европейских странах органы власти стали рассматривать такие данные как информацию, необходимую для борьбы с преступностью. Таким образом, Директива 2006/24/ЕС пересматривала «презумпцию уничтожения данных».

По-видимому, нет необходимости анализировать все правовые аргументы Европейского Суда Справедливости, приявшего решение об отмене Директивы 2006/24/ЕС. Достаточно отметить следующее.

Европейский Суд Справедливости постановил, что законодательный орган Европейского Союза превысил пределы принципа пропорциональности в отношении ряда фундаментальных положений Хартии основополагающих прав Европейского Союза (2000/C 364/01), в частности нормы ст.ст. статьи 7, 8 и 52(1), в частности, права на неприкосновенность частной жизни, защиту данных, свободу выражения мнений[51]. Европейский Суд Справедливости отметил, что обязательства, налагаемые Директивой 2006/24/ЕС по хранению данных, представляет собой вмешательство в право на неприкосновенность частной жизни, т.к. предусматривает доступ компетентных органов к этим данным; нарушает право на защиту данных.

[51] Charter of Fundamental Rights of the European Union (2000/C 364/01)

Европейский Суд Справедливости фактически исходил из двуединого критерия соразмерности: меры должны соответствовать достижению целей, но не быть чрезмерными для достижения цели. В этой связи была отмечена важность защиты персональных данных для обеспечения конфиденциальности, но меры и степень вмешательства в сферу «фундаментальных прав» фактически ограничивали эти права.

Европейский Суд Справедливости счел, что порядок хранения данных, в соответствии с Директивой 2006/24/ЕС, предоставляет национальным органам власти, дополнительные возможности в расследовании серьезных преступлений и являются важным инструментом в этой сфере и, Директива 2006/24/ЕС в этой части не противоречит цели ее принятия. Вместе с тем, ограничения основных прав должны осуществляться только в той степени, насколько это «абсолютно необходимо» и что для права Европейского Союза важны четкие и точные правила, регулирующие сферу ограничения прав и гарантий прав лиц. Европейский Суд Справедливости отметил, что Директива 2006/24/ЕС не устанавливает четкие и точные правила относительно мер ограничения основных прав и степени вмешательства национальных органов власти. В частности, применение Директивы 2006/24/ЕС ко всему трафику, всех пользователей, всех средств электронных коммуникаций – влечет «вмешательство национальных органов власти в основные права» практически всего населения Европейского Союза и, при этом не устанавливает четкую связь между данными, хранящимися в связи с тяжкими преступлениями (или общественно опасными) и иными сохраняемыми данными.

Кроме того, Директива 2006/24/ЕС не определяет существенных условий (к примеру, критерии по числу лиц, имеющих доступ к данным, порядок деятельности административных органов и т.д.) использования хранящихся данных, полученных компетентными национальными органами. Европейский Суд Справедливости также заметил, что Директива 2006/24/ЕС не устанавливает четкие гарантии защиты сохраненных данных, включая риски незаконного доступа к этим хранящимся данным, фактически позволяя провайдерам исходить из «экономических соображений» при использовании технических и организационных средств обеспечения безопасности хранения данных.

Выше обозначенные причины, наряду с прочими, дали основание Европейскому Суду Справедливости признать Директиву 2006/24/ЕС

недействительной и ее отметить. Для последующего изложения важно обратить внимание, что решение, вынесенное Европейским Судом Справедливости 8 апреля 2014 г. об отмене Директивы 2006/24/ЕС (*European Court of Justice Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland of 8 April 2014*), по-разному оценивается и экспертами и правоведами.

Обобщенно существующие оценки решения, вынесенного Европейским Судом Справедливости, можно определить как своеобразное напоминание названия известного фильма: «*The Good, the Bad and the Ugly*» («*Il Buono, il Brutto, il Cattivo*»).

Тот факт, что Директива 2006/24/ЕС отменена, принципиально важно, прежде всего, для поддержания конфиденциальности частной жизни, защиты персональных, сохранения свободы выражения мнений и т.д. Содержание Директивы 2006/24/ЕС лишний раз подтверждает, что частная жизнь лиц «находится под постоянным наблюдением». Кроме того, существенным аспектом хранения данных, в смысле нормативных положений Директивы 2006/24/ЕС, является «рост» сводных мета-данных. В этой связи «положительный эффект» отмены Директивы 2006/24/ЕС Европейским Судом Справедливости – не оспаривается большинством аналитиков, экспертов-правоведов.

Однако, не стоит не учитывать те «правомерные аспекты» Директивы 2006/24/ЕС, которые в том числе были отмечены Европейским Судом Справедливости, относящиеся к тому, что Директива 2006/24/ЕС, наряду с тем, что она имела «надлежащие правовые основания принятия и введения в действие», одна из важных целей ее принятия состояла в сохранение данных, созданных или обработанных в связи с оказанием общедоступных услуг электронной связи или сетей связи общего пользования, осуществляемых для обеспечения расследования, обнаружения и судебного преследования за серьезные преступления.

Обращаясь к текущему периоду регулирования защиты и хранения данных в Европейском Союзе, следует отметить, что «этапным» стал 2016 г. и это определяется рядом причин.

В апреле 2016 г. была принята новая структура защиты данных Европейского Союза, закрепленная в документе – «Регламент (ЕС) 2016/679 Европейского Парламента и Совета от 27 апреля 2016 года о защите физических

лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46 / ЕС (Общие положения о защите данных)» (*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation*). В аналитических материалах этот документ чаще называют – «Общие положения о защите данных» (далее – «Регламент о защите данных») и в отношении него важно подчеркнуть его правовую природу и значение. Прежде всего это связано с тем, что в праве Европейского Союза Директивы (*Directive*), принимаемые Европейским Парламентом и Советом, имеют общенормативное значение, что в формально-юридическом плане означает, что Директивы должны быть имплементированы в национальное право государств-членов. Регламенты (*Regulation*) Европейского Парламента и Совета обладают иной правовой силой. Документы Европейского Союза, принятые в форме Регламента, непосредственно применяются в государствах-членах Европейского Союза, что, в свою очередь, предполагает гармонизацию национального права государств-членов. (Первые законодательные проекты, принятые в национальных юрисдикциях в связи с Регламентом о защите данных, опубликованы в Германии, Нидерландах и Польше).

Подчеркнем, что Регламент о защите данных, во-первых, заменяет Директиву 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных», во-вторых, вступил в силу 25 мая 2016 г. и будет применяться с 25 мая 2018 г., в третьих, его принятием и вступлением в силу *de facto*, «гармонизируется» право Европейского Союза в сфере защиты данных и механизмов регулирования.

Регламент о защите данных устанавливает общие правила для защиты физических лиц в отношении обработки личных данных и о свободном передвижении персональных данных в рамках Союза.

Одновременно с Регламентом о защите данных была принята Директива (ЕС) 2016/680 Европейского Парламента и Совета 2016/679 от 27 апреля 2016 г. «О защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, обнаружения

или преследования уголовных наказаний и о свободном перемещении таких данных и отмене Рамочного Решения Совета ЕС 2008/977/ JHA» (*Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*).

Директива «О защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования уголовных наказаний и о свободном перемещении таких данных» (далее – «Директива 2016/680») вступила в силу 5 мая 2016 г., и до 25 мая 2018 г. нормативные положения Директивы 2016/680 должны быть имплементированы государствами-членами Европейского Союза в свое национальное право.

Приятие Директивы 2016/680 обусловлено рядом важным причин соеди которых следует отметить следующие.

1. Директива 95/46/ЕС Европейского парламента и Совета («О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных»), которая действует в настоящее время но, как отмечалось ранее, будет заменена в связи с применением с 25 мая 2018 г. Регламента о защите данных, распространяется на всю обработку персональных данных в странах-членах в государственном и частном секторах. Вместе с тем, Директива 95/46/ЕС «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных» *не* распространяется на обработку персональных данных в ходе осуществления деятельности, которая выходит за рамки законодательства Европейского Союза, таких как деятельность в области судебного сотрудничества по уголовным делам и сотрудничества правоохранительных органов.

2. В настоящее время в рамках Европейского Союза действует Рамочное Решение Совета ЕС 2008/977/ JHA, связанное с судебным сотрудничеством по уголовным делам и сотрудничеством правоохранительных органов и сфера применения которого ограничивается обработкой персональных данных, передаваемых между государствами-членами Европейского Союза. Директива

2016/680 отменяет это Рамочное Решение Совета ЕС 2008/977/ JHA, т.е. его действие ограничивается сроком – 25 мая 2018 г., когда нормативные положения Директивы 2016/680 должны быть имплементированы государствами-членами в национальное право.

Директива 2016/680 направлена на обеспечение последовательной защиты персональных данных физических лиц и упрощения обмена персональными данными между компетентными органами государств-членов, которое, по смыслу Директивы 2016/680 имеет решающее значение для обеспечения эффективного судебного сотрудничества по уголовным делам и взаимодействия правоохранительных органов.

В связи со значительным объемом Регламента о защите данных и Директивы 2016/68, а также в связи с тем, что обозначенные документы регламентируют достаточно большой круг отношений, определяя подробный перечень процессуальных и организационных механизмов и т.д., – эти документы приложены к настоящему исследованию в русскоязычной версии (автоматический перевод, с некоторыми редакторскими правками. Целесообразность адекватного перевода на русский язык Регламента о защите данных и Директивы 2016/680 – очевидна)[52].

В завершении упомянем еще один документ, который в настоящее время находится в процессе рассмотрения в Европейском Союзе. Это Директива (ЕС) 2016/681 Европейского Парламента и Совета 2016/679 от 27 апреля 2016 г. «по использованию данных номера бронирования (*passenger name record*) по предотвращению, обнаружению, расследованию и преследованию преступлений, связанных с терроризмом и серьезными преступлениями» (*Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*)[53].

[52] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation URL: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

[53] http://eclan.eu/en/eu-legislatory/directive-eu-2016-681-of-the-european-parliament-and-of-the-council-of-27-april-2016-on-the-use-of-passenger-name-record-pnr-data-for-the-prevention-detection-investigation-and-prosecution-of-terrorist-offences-and-serious-crime

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ДЕЙСТВУЮЩЕГО И ФОРМИРУЮЩЕГОСЯ (ПРЕДЛАГАЕМЫЕ ПРОЕКТЫ) РОССИЙСКОГО ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ СБОРА И ХРАНЕНИЯ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ ТЕЛЕКОММУНИКАЦИОННЫХ И ЗАКОНОДАТЕЛЬСТВА ДРУГИХ СТРАН

Часть I

Страна	**Состав данных для хранения**	**Период хранения данных**	**Порядок использования хранимых данных (кто и при каких условиях имеет доступ и каким образом может использовать данные)**	**Наличие обязательств по информированию субъектов, данные которых собираются о фактах использования собранных данных**	**Основные участники механизма хранения**
Россия	Операторы связи обязаны хранить на территории Российской Федерации: 1) информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи - в течение трех лет с момента окончания осуществления таких действий; 2) текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи - до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. *Порядок, сроки и объем хранения устанавливаются Правительством Российской Федерации – до настоящего времени не установлены.*	Информация о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи - в течение трех лет с момента окончания осуществления таких действий Период хранения текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео-, иных сообщений пользователей услугами связи – до 6 месяцев, но до настоящего времени однозначно не определён и должен быть детализирован в подзаконных актах.	Операторы связи обязаны предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, указанную информацию, информацию о пользователях услугами связи и об оказанных им услугах связи и иную информацию, необходимую для выполнения возложенных на эти органы задач, в случаях, установленных федеральными законами. В настоящее время такие случаи предусмотрены: ФЗ «Об оперативно-разыскной деятельности»; ФЗ «О федеральной службе безопасности»; ФЗ «О полиции». В части случаев, предусмотренных законами, запросы на такую информацию не требуют судебного решения.	Не предусмотрены.	Операторы связи (юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии) – более 36 тысяч выданных лицензий в России; Организаторы распространения информации (лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети "Интернет") – неопределённый круг субъектов.

Страна	Состав данных для хранения	Период хранения данных	Порядок использования хранимых данных (кто и при каких условиях имеет доступ и каким образом может использовать данные)	Наличие обязательств по информированию субъектов, данные которых собираются о фактах использования собранных данных	Основные участники механизма хранения
Австралия	1. Абонент и учетные записи, сервисы, телекоммуникационные устройства и другие сервисы, относящиеся к соответствующей услуге 2. Источник коммуникации. 3. Конечный адрес коммуникации. 4. Дата, точное время и продолжительность сеанса коммуникации, или подключения к соответствующей услуге. 5. Тип сеанса передачи данных и соответствующей услуги, использованной для подключения в ходе коммуникации. 6. Местонахождение оборудования или канала связи, задействованного для установления соединения в ходе коммуникации.	Не менее двух лет, «начиная с момента, когда соответствующая информация или документ о коммуникациях были созданы; и (ii) заканчивая истечением 2 лет с момента закрытия учетной записи, к которой относится соответствующая информация или документ; или (b) в иных случаях – промежуток времени: (i) начиная с момента, когда соответствующая информация или документ о коммуникациях были созданы; и (ii) заканчивая истечением 2 лет с момента, когда соответствующая информация или документ о коммуникациях были созданы». Т.е, **более кратко**: а) В большинстве случаев – в течение не менее 2 лет с момента коммуникации; б) В отдельных случаях - в течение всего срока активности учетной записи пользователя и течение 2 лет с момента закрытия учетной записи.	Согласно Статье 110A TIAADR 2015, доступ имеют 22 органа, включая правоохранительные органы и ведомства, уполномоченные в области обеспечения национальной безопасности, в том числе: • Австралийская служба безопасности и разведки (ASIO); • Австралийская федеральная полиция (AFP) и полицейские органы австралийских штатов; • Австралийское налоговое управление (Australian Taxation Office); • Австралийская комиссия по преступности (ACC); • Комиссия по вопросам коррупции и преступности (CCC); • Независимая комиссия по противодействию коррупции Нового Южного Уэльса (NSW Independent Commission against Corruption (ICAC)); • Австралийская комиссия по поддержанию целостности правопорядка (ACLEI); • Комиссия по поддержанию целостности полиции (PIC); • Управление иммиграции и защиты границ (IBPD); • Австралийская комиссия по ценным бумагам и инвестициям (ASIC); • Австралийская комиссия по уголовной разведке (ACIC); • И другие ведомства.	Закон TIIADR 2015 не обязывает государственные органы уведомлять пользователей о получении доступа к данным их коммуникаций чеез провайдеров услуг. Более того, Статья 182A устанавливает, что разглашение информации о выдаче судом ордера на получение доступа к данным коммуникаций лица, осуществляющего профессиональную журналистскую деятельность, общем случае является уголовным преступлением и карается заключением на срок до 2 лет. Статья 182B описывает ряд частных случаев, при которых разглашение такой информации допустимо либо прямо предписано и не является уголовно наказуемым.	Поставщики 3 категорий услуг: a) услуги по осуществлению коммуникации либо обеспечению возможности для коммуникации, посредством направляемой или ненаправляемой энергии электромагнитного спектра (carriage service). b) услуги, предоставляемые поставщиком услуг связи (carrier) или интернет-провайдером (internet service provider). c) услуги, предоставляемые лицом, которое на территории Австралии владеет либо является провайдером услуг инфраструктуры, обеспечивающей техническую возможность предоставления соответствующей услуги из перечисленных.

Страна	Состав данных для хранения	Период хранения данных	Порядок использования хранимых данных (кто и при каких условиях имеет доступ и каким образом может использовать данные)	Наличие обязательств по информированию субъектов, данные которых собираются о фактах использования собранных данных	Основные участники механизма хранения
			Для указанных ведомств доступ к данным не требует получения и предоставления судебного ордера (досудебный механизм). Единственное исключение, пролоббированное оппозиционной Австралийской лейбористской партией, Закон предусматривает для доступа к данным лиц, осуществляющих профессиональную деятельность в качестве журналистов (либо работодателей таких лиц). Для получения доступа к метаданным журналистов госорганы, включая ASIO, должны запрашивать ордер у Генерального Прокурора.		
Европейский союз	Персональные данные, данные в рамках конкретного расследования, данные, в отношении которых лицо дало согласие на их сбор, обработку, хранение и т.д. Запись и хранение осуществляются с оговоркой о технических возможностях.	Сроки зависят от типа персональных данные которые подлежат обработке, целей хранения и иных мер, обеспечивающих законное и справедливое рассмотрение дел. Хранение данных осуществляется в течение одного месяца со дня получения соответствующего «запроса». Этот срок может быть продлен на два месяца. Срок хранения данных зависит от того какие органы вовлечены в эту сферу: контрольные или надзорные.	Согласие на обработку персональных – императивное условие. Согласие должно быть настолько же легко отозвать, как и предоставить. Согласие должно быть однозначно выражено и носить самостоятельный характер. Запрос на получение согласия должен соответствовать Регламенту; условие согласия должно быть отделено от иных условий. Регламент предусматривает дополнительные требования к использованию согласия обработки данных в	Обработка персональных данных осуществляется органами государственной власти или частных структур, действующих в общественных интересах. Предусмотрена закрепление процедур рассмотрения жалоб, поступивших от субъектов персональных данных, проведение расследований о применении Регламента; меры, обеспечивающие осведомленность населения о рисках, гарантиях прав в отношении обработки персональных данных.	Европейский совет по защите данных (European Data Protection Board); Надзорный орган каждого государства-члена; Европейский наблюдатель по вопросам защиты данных (European Data Protection Supervisor). Сбор, обработка данных, переработка затрагивающих данные субъектов и т.д. осуществляется национальными органами по защите данных (Data Protection Authorities, DPA); контроллеров (Controller); обработчиков (Processor); инспекторы по защите

Страна	Состав данных для хранения	Период хранения данных	Порядок использования хранимых данных (кто и при каких условиях имеет доступ и каким образом может использовать данные)	Наличие обязательств по информированию субъектов, данные которых собираются о фактах использования собранных данных	Основные участники механизма хранения
			контексте трудовых отношений. Субъекты данных вправе пользоваться своими правами, предоставленными Регламентом, включая право портативности данных, право на ограничение обработки данных, право на забвение (right to be forgotten).		данных (Data Protection Officer)
США	1. В параграфе 107 Акта о свободе приводится следующее определение подробных записей о вызове (CDR) : CDR означает информацию, позволяющую идентифицировать сеанс коммуникации, в том числе: • телефонный номер, с которого был инициирована и завершена коммуникация; • номер международного идентификатора мобильного абонента (IMSI); номер международного идентификатора мобильного оборудования (IMEI); • номер телефонной карты, с использованием которой был осуществлен вызов; время и продолжительность звонка. При этом прямо прописан, что CDR НЕ включает в себя: • любое содержимое (данные) сеанса коммуникации; • имя, адрес или платежную информацию подписчика или клиента; • данные местоположения ячеек сотовой связи, к которой	1. Согласно норме, принятой в рамках Закона о записях транзакций посредством электронных коммуникаций (Electronic Communications Transactional Records, ECTR Act) от 1996 г., и кодифицированной в 18 U.S.C. § 2703, провайдеры услуг электронных коммуникаций и провайдеры удаленных компьютерных сервисов должны сохранять данные, в отношении которых получен запрос от государственных органов, в течение 90 дней; а также дополнительных 90 дней при получении повторного запроса. 2. Согласно требованию FCC от 1986 г., закрепленному параграфе 42.6 «Хранение записей междугородних телефонных звонков» Свода федеральных нормативных актов США (CFR), провайдеры услуг магистральной (toll) телефонной связи обязаны	Основные – полиция федеральная, а также полиция штатов, АНБ, Министерство внутренней безопасности, Министерство юстиции.	В большинстве случаев (включая сохранение данных на основании параграфа 107 Акта о свободе), а также Закона о записях транзакций посредством электронных коммуникаций (Electronic Communications Transactional Records, ECTR Act) от 1996 г., информирование данные которых собираются о фактах использования таких данных, не предполагается текстом соответствующих НПА.	1. В рамках Закона о запиях транзакций посредством электронных коммуникаций (Electronic Communications Transactional Records, ECTR Act) от 1996 г., и кодифицированной в 18 U.S.C. § 2703 нормы, субъектами являются: • провайдеры услуг электронных коммуникаций; • и провайдеры удаленных компьютерных сервисов. 2. В рамках требования FCC от 1986 г., закрепленному параграфе 42.6 «Хранение записей междугородних телефонных звонков» Свода федеральных нормативных актов США (CFR), субъектами хранения являются провайдеры услуг магистральной телефонной связи (toll telephony). 3. В рамках Закона о содействии правоохранительным органам в области коммуникаций

Страна	Состав данных для хранения	Период хранения данных	Порядок использования хранимых данных (кто и при каких условиях имеет доступ и каким образом может использовать данные)	Наличие обязательств по информированию субъектов, данные которых собираются о фактах использования собранных данных	Основные участники механизма хранения
	осуществлялось подключение во время коммуникации; • данные системы глобального позиционирования (GPS. 2. Согласно требованию FCC от 1986 г., закрепленному параграфе 42.6 «Хранение записей междугородних телефонных звонков» Свода федеральных нормативных актов США (CFR), провайдеры услуг магистральной (toll) телефонной связи обязаны хранить: 1. Имя абонента. 2. Адрес абонента. 3. Вызывающий телефонный номер. 4. Вызываемый телефонный номер. 5. Дата и точное время звонка. 6. Продолжительность звонка. 3. В рамках Закона о содействии правоохранительным органам в области коммуникаций (CALEA): o Телефонный номер, код идентификации канала (CIC) либо иная информация, позволяющая идентифицировать коммуникацию. o Время и дата начала мероприятий оператора по осуществлению перехвата либо получению доступа к информации, позволяющей идентифицировать звонок. o Время и дата окончания мероприятий оператора по осуществлению перехвата либо	хранить данные в течение 18 месяцев. 3. Согласно требованиям законодательства (пункт Кодекса федеральных нормативных актов США 47 C.F.R. § 1.20004(b), провайдеры услуг телефонной связи обязаны обеспечивать хранение информации (метаданных) обо всех перехваченных по запросам правоохранительных органов звонках «на протяжении разумного срока». Провайдерам рекомендуется обеспечивать хранение данных в течение 2 лет.			(CALEA) субъектами хранения являются провайдеры телефонной связи, а также операторов услуг беспроводного доступа в Интернет и VoIP-связи.

Страна	Состав данных для хранения	Период хранения данных	Порядок использования хранимых данных (кто и при каких условиях имеет доступ и каким образом может использовать данные)	Наличие обязательств по информированию субъектов, данные которых собираются о фактах использования собранных данных	Основные участники механизма хранения
	получению доступа к информации, позволяющей идентифицировать звонок. o Личность сотрудника органов правопорядка, предъявившего документы, санкционирующие деятельность по перехвату / получению доступа к информации, позволяющей идентифицировать коммуникацию. o Тип перехвата или получения доступа к телефонной коммуникации (например, перехват и отслеживание метаданных звонка, перехват полного содержимого звонка, перехват в рамках ордера на основании Закона FISA и проч.). o И проч. 4. Согласно норме, принятой в рамках Закона о записях транзакций посредством электронных коммуникаций (Electronic Communications Transactional Records, ECTR Act) от 1996 г., и кодифицированной в 18 U.S.C. § 2703, провайдеры услуг электронных коммуникаций и провайдеры удаленных компьютерных сервисов должны раскрывать государственным органам на основании их запросов следующие данные: (A) имя абонента; (B) адрес абонента; (C) записи о локальных и междугородних телефонных звонках, либо записи данных времени и продолжительности сеанса коммуникации (например,				

Страна	Состав данных для хранения	Период хранения данных	Порядок использования хранимых данных (кто и при каких условиях имеет доступ и каким образом может использовать данные)	Наличие обязательств по информированию субъектов, данные которых собираются о фактах использования собранных данных	Основные участники механизма хранения
	доступа в Интернет); (D) продолжительность использования услуги абонентов (включая дату начала использования) и типы использованных услуг; (E) номер телефона или иного средства связи, либо иной номер или идентификаторов абонента, включая временно присвоенный абоненту сетевой адрес; (F) средства и источник оплаты данных услуг (включая данные кредитной карты или банковского счета).				
Великобритания	персональные данные; личные данные в рамках конкретного расследования или операции; данные, в отношении которых лицо дало согласие на их хранение; данные записей интернет-соединений (*internet connection record*). Кроме того, данные (их обработка), содержащиеся в перехваченной информации. Сохраняются данные, имеющие отношение к сути события; к виду, роду либо характеру события; ко времени или продолжительности события.	Зависит от вида данных: «уже сохраненные данные»; «зна*ч*имые данные» («зна*ч*имые данные» включают данные записей интернет-соединений), и др. Кроме того зависит от срока вступления в силу «уведомления о сохранении данных»; от сроков, указанных в ордере и т.д. Например, «уведомление о сохранении данных» **не должно** содержать требования о хранении каких-либо данных в течение ***более* 12 месяцев.**	Зависит от содержания разрешения (*authorisation*) на получение **передаваемых данных** (*obtaining of communications data*); соблюдения целевого характера получения данных (данных, получаемых в определенных целях): для конкретного расследования/операции; в интересах национальной безопасности; предотвращения или обнаружения преступления и т.д.	В связи с тем, что Законодательный акт регулирует сферу проведения следственных действий, обязательства по информированию субъектов, данные которых собираются, о фактах использования собранных данных, основываются на компетенции и круге полномочий правоохранительных и разведывательных органов. В этой связи закреплен порядок **правомерного перехвата сообщений** (*lawful interception of communications*); действия по перехвату сообщений, основанные **на ордере** (*under a warrant*); условия перехвата сообщений и последующее использование перехваченной информации и обработки материалов,	Операторы телекоммуникационных сетей; органы власти: Британское Управление по защите данных (*UK Information Commissioner's Office*); Государственный секретарь (*Secretary of State*), Судебный комиссар (*Judicial Commissioner*), Комиссар по следственным полномочиям (*Investigatory Powers Commissioner*).

Страна	Состав данных для хранения	Период хранения данных	Порядок использования хранимых данных (кто и при каких условиях имеет доступ и каким образом может использовать данные)	Наличие обязательств по информированию субъектов, данные которых собираются о фактах использования собранных данных	Основные участники механизма хранения
				полученных в связи с перехваченной информацией; порядок правомерного **получения передаваемых данных** (*lawful obtaining of communications data*). Получения данных, обработка полученных данных; передача данных является законной (правомерной), если такие действия основываются либо на соответствующем **разрешении** (*authorisation*) либо на **ордере** (*under a warrant*).	
Германия *Закон вступает в действие с Июля 2017, но может быть признан неконституционным и отменён	Информация о фактах соединения или звонках, местоположение пользователей, содержание SMS	4 недели для геометок, 10 недель остальное	Только при расследовании серьезных преступлений, при получении судебного ордера; в случае необходимости быстрого реагирования ордер может выписать прокурор (должно быть подтверждено судом впоследствии). Время, содержание и цель доступа к данным должна быть зафиксирована.	Да, по завершению сбора данных, при условии отсутствия вреда для субъекта или расследования	Телекоммуникационные компании. Функции по хранению и доступу к данным могут быть отданы сторонним компаниям.
Дания	Согласно Приказу о хранении данных Минюста от 13.10.2006 , провайдеры услуг обязаны осуществлять запись и хранение следующей информации в рамках коммуникаций по стационарной или мобильной телефонной связи: 1) Номер вызывающего абонента (номер А), а также имя и адрес зарегистрированного	Закон №378 от 06.06.2002 «О внесении поправок в уголовный кодекс, Закон об отправлении правосудия, Закон о рыночной конкуренции и правах потребителей услуг рынка телекоммуникаций, Закон о вооруженных силах и Закон об экстрадиции нарушителей правопорядка в Финляндию,	Законом №378 от 06.06.2002 «О внесении поправок…» устанавливается, что доступ к данным о коммуникациях пользователей, хранимым поставщиками услуг, осуществляется **на основании судебного ордера**. Решение о выдаче ордера на	Закон №378 от 06.06.2002 «О внесении поправок…», а также Приказ о хранении данных Минюста от 13.10.2016 **не содержат положений**, обязывающих государственные органы либо самих провайдеров услуг уведомлять пользователей о записи, хранении и получении	Действие Приказа о хранении данных Минюста от 13.10.2006 распространяется на всех поставщиков «услуг электронных коммуникаций или публичных коммуникационных сетей» , вне зависимости от того, являются ли их услуги общедоступными или нет.

Страна	Состав данных для хранения	Период хранения данных	Порядок использования хранимых данных (кто и при каких условиях имеет доступ и каким образом может использовать данные)	Наличие обязательств по информированию субъектов, данные которых собираются о фактах использования собранных данных	Основные участники механизма хранения
	пользователя или подписчика соответствующей услуги. 2) Номер вызываемого абонента (номер B), имя и адрес зарегистрированного пользователя или подписчика соответствующей услуги. 3) Номер переадресации вызова (номер C), имя и адрес зарегистрированного пользователя или подписчика соответствующей услуги. 4) Отчеты о доставке сообщений. 5) Идентификаторы используемых для коммуникации устройств (номера идентификаторов IMSI и IMEI). 6) Ячейка(-и) сотовой связи, в соответствии с их меткой местоположения (идентификатор ячейки – Cell ID). 7) Данные, идентифицирующие географическое местоположение ячейки (ячеек) сотовой связи, к которой (-ым) подключен мобильный телефон на момент начала коммуникации. 8) Время начала и время окончания коммуникации. 9) Время первоначальной активации предоплаченной анонимной услуги и метка местоположения (идентификатор ячейки – Cell ID), с которого была активирована услуга. Тем же Приказом вводился режим регистрации IP-сессий **(отменен 4 июня 2014 г., до сих пор не введен заново)**: 1) IP-адреса, с которых	Норвегию и Швецию» обязывает провайдеров телекоммуникационных услуг осуществлять запись и хранение информации о телекоммуникациях (метаданных) в **течение одного года.**	получение доступа к данным должно приниматься при наличии следующих обстоятельств: 1) Имеются конкретные основания полагать, что информационная система, при помощи/посредством которой осуществляются коммуникации, используется подозреваемым в целях, непосредственно связанных с подготовкой преступления или уже совершенным преступлением. 2) Раскрытие данных о коммуникациях пользователя должно иметь существенное значение для процесса расследования преступления. 3) Расследование ведется в отношении действий, подпадающих под Главу 12 УК Дании (Преступления против независимости и безопасности государства), Главу 13 УК Дании (Преступления против Конституции и высшего руководства страны), а также статьи УК Дании №180, 183a, 187, 191, 192a и 237. Судебный ордер выдается представителям национальной **Полиции Дании (Rigspolitiet)**, которые	доступа к данным их коммуникаций. Вместе с тем, не определены и санкции за возможное уведомление поставщиком услуг пользователей о таких действиях.	Эта норма включает в себя интернет-провайдеров и провайдеров услуг фиксированной и мобильной телефонной связи, а также кафе, рестораны и прочие учреждения, предоставляющие интернет-доступ пользователям – **за исключением 3 категорий** субъектов: • Государственные учреждения; • Производственные помещения и прочие объекты работодателей, на которых предоставляется доступ к Интернету сотрудникам. Государственные образовательные учреждения.

Страна	Состав данных для хранения	Период хранения данных	Порядок использования хранимых данных (кто и при каких условиях имеет доступ и каким образом может использовать данные)	Наличие обязательств по информированию субъектов, данные которых собираются о фактах использования собранных данных	Основные участники механизма хранения
	осуществлялась отправка (передача) данных. 2) IP-адреса, на которые осуществлялась доставка (передача) данных. 3) Протокол передачи данных, задействованный в коммуникации (например, TCP или UDP). 4) Номер порта, с которого осуществлялась отправка интернет-трафика. 5) Номер порта, на который осуществлялась доставка интернет-трафика. 6) Метка времени начала и завершения сеанса коммуникации.		уполномочены на его основании получать необходимые для расследования данные о коммуникациях пользователей от поставщиков услуг.		
Нидерланды *Суды отменили действие предыдущего закона, принятие нового закона отложено до формирования следующего правительства	Отсутствует	Отсутствует	Отсутствует	Отсутствует	Отсутствует
Франция *Суд обязал пересмотреть закон до конца 2017 года, закон может быть признан неконституционным	Информация о фактах соединения или звонках, местоположение пользователей, содержание SMS. Специальное оборудование для сбора и анализа метаданных в реальном времени с целью поиска активности террористов с последующим сбором содержания сообщений в течение 4 месяцев.	Содержание сообщений – 1 месяц по окончании расследования, информация о фактах соединения – до 4 лет. В случае данных иностранных лиц, содержание сообщений – до 8 лет, метаданные – до 6 лет	Судебный ордер не требуется при условии расследований, касающихся национальной безопасности; для сбора метаданных требуется приказ премьер-министра и специальной комиссии по надзору за спецслужбами.	Нет. Однако по завершению сбора данных, при условии отсутствия вреда для субъекта или расследования, субъект может оспорить действия органов.	Телекоммуникационные компании, хостинги, интернет-компании. Функции по хранению и доступу к данным могут быть отданы сторонним компаниям. Необходима установка специального оборудования для доступа спецслужб

Страна	Функции участников механизма хранения	Источники и порядок финансирования записи и хранения	Способы защиты хранимой информации	Ответственность за возможные утечки	Ответственность операторов связи за нарушение порядка и правил сбора и хранения данных
Россия	1. Обеспечивать запись и хранение информации о фактах – не менее трёх лет; 2. Обеспечивать запись и хранение текстовых сообщений пользователей, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей период до 6 месяцев.	Закон не требует затрат из федерального бюджета, все расходы по реализации Закона возложены на операторов связи и организаторов распространения информации.	Не предусмотрены.	Не предусмотрена.	Не предусмотрена.
Австралия	1. Обеспечивать хранение информации в течение не менее двух лет. 2. Обеспечивать предоставление данных уполномоченным органам на основании досудебного запроса либо, в отдельных случаях (данные коммуникаций журналистов) на основании судебного ордера. 3. Обеспечивать защиту конфиденциальности хранимой информации, в том числе за счет: a) Шифрования хранимой информации. b) Защиты хранимой информации от неавторизованного доступа или перехвата. 4. Обеспечивать составление, направлять	1. Поставщики услуг коммуникаций (сотовые операторы, интернет-провайдеры, операторы фиксированной телефонной связи) – за свой счет. 2. Государство – в рамках- Программы государственных грантов для отраслевых организаций для обеспечения хранения данных (DRIGP): • Максимальный размер гранта - 80% от оценочной суммы расходов провайдера услуг на хранение данных. • Минимальный размер гранта - 10 тыс. долл. • В среднем компенсировано 47% расходов по 180 утвержденным	• Поставщики услуг в рамках исполнения TIIADR 2015 обязаны обеспечивать **защиту и шифрование** хранимой информации о коммуникациях пользователей. • Поставщики услуг **не обязаны** обеспечивать хранение данных в рамках единой централизованной платформы/инфраструктуры . • Система уровней сервиса в части хранения данных должна соответствовать уже имеющимся отраслевым практикам и стандартам. Например, хранение биллинговой информации пользователей в течение расширенного периода времени в соответствии с TIAADR 2015 логично осуществлять на том же уровне, который обеспечивался и до этого в целях более краткосрочного хранения таких данных.	Отдельно не прописана, см. раздел *«Ответственность операторов связи за нарушение порядка и правил сбора и хранения данных»*.	Управление по связи и средствам массовой информации Австралии (ACMA) может облагать провайдеров штрафами за невыполнение закона TIAADR 2015 в части хранения, в том числе за невыполнение согласованных с Координатором по коммуникациям (CAC) Планов по выполнению закона (TIIADR 2015 Implementation plans). Размер штрафа за каждое нарушение норм Акта о телекоммуникациях составляет 10 200 долл. Кроме того, в тех случаях, когда Федеральный Суд признает, что поставщик услуг нарушил условий лицензии на осуществление коммуникационных услуг или правила ведения деятельности, он также может быть обязан выплатить Содружеству наций до 10 млн долл. за каждый эпизод допущенного нарушения .

Страна	Функции участников механизма хранения	Источники и порядок финансирования записи и хранения	Способы защиты хранимой информации	Ответственность за возможные утечки	Ответственность операторов связи за нарушение порядка и правил сбора и хранения данных
	на согласование и утверждение в офис Координатора по доступу к коммуникациям (CAC), а также осуществлять выполнение и обновление по требованию CAC утвержденных Планов по выполнению TIAADR 2015 в части хранения информации (Implementation plans).	заявкам (128,4 млн долл.). • Регрессионная модель оценки для более полного возмещения расходов малых операторов.	• Для уменьшения объема хранимых данных и сокращения издержек, связанных с их хранением, поставщики услуг имеют право осуществлять **оптимизацию формата хранимых данных** – при условии, что такие действия не ведут к нарушению их обязательств, в части, по раскрытию хранимых данных уполномоченным госорганам. • Для процедур и механизмов хранения данных **не установлены** обязательные международные либо национальные стандарты.		
Европейский союз	**Контролеры обязаны:** вести соответствующую документацию; оценивать воздействие обработки персональных данных на права субъектов данных для более рискованных видов обработки данных; внедрять защиту данных. Органы по защите данных составляют списки видов операций, которые обязаны предпринимать Контролеры. **Обработчики** (Processor) или **контролеры** (Controller) данных обязаны назначить инспектора по защите данных (Data Protection Officer, DPO) в рамках своих программы отчетности. Назначение инспектора	Государственные и частные. Например, Группа организаций или определенные группы государственных учреждений могут назначить одного инспекторы по защите данных (Data Protection Officer). Инспектор по защите данных должен находиться на территории ЕС и быть непосредственно подчинен высшему уровню руководства организации.	Для защиты данных Европейский совет по защите данных (European Data Protection Board); Надзорный орган каждого государства-члена внедряют механизмы сертификации и защиты данных, разработку кодексов поведения; контроль за операциями Обработчиков и Контроллеров.	Контролеры обязаны своевременно сообщать своим органам по защите данных (Data Protection Authorities, DPA) об утечках данных в течение 72 часов после обнаружения утечки. При несоблюдении этого срока требуется предоставить мотивированное обоснование. (ожидается нормативное уточнение). Регламент устанавливает многоуровневые санкции за нарушения права о защите данных. Органы по защите данных (Data Protection Authorities, DPA) вправе налагать штрафы за ряд нарушений. Например, за нарушение требований	контролеры данных несут ответственность за операции по обработке персональных данных. Контролеры данных обязаны внедрить эффективные процедуры и механизмы для рискованных операций с данными, особенно при крупномасштабной обработке данных. Установлена административное требование для контролеров заблаговременно обращаться в свои органы по защите данных (Data Protection Authorities, DPA). Если по мнению DPA обработка приведет к нарушению Регламента DPA дает письменные рекомендации, при невыполнении которых налагаются меры ответственности (ожидается нормативное уточнение).

Страна	Функции участников механизма хранения	Источники и порядок финансирования записи и хранения	Способы защиты хранимой информации	Ответственность за возможные утечки	Ответственность операторов связи за нарушение порядка и правил сбора и хранения данных
	обязательно в следующих случаях: обработка данных осуществляется госорганом; основная деятельность контролера или обработчика заключается в такой обработке, которая по своей сути, масштабу или целям требует крупномасштабного, регулярного и систематического мониторинга субъектов данных; основная деятельность организации заключается в крупномасштабной обработке специальных категорий данных. **Обработчик** данных **(Processor)** обязан: вести (письменно) реестр операций по обработке персональных данных, выполненных от имени и по поручению контролера; назначать по необходимости инспектора по защите данных; назначить при необходимости представителя в ЕС (в случае отсутствия такового); своевременно уведомлять контролера об обнаруженных утечках персональных данных. Трансграничная передача данных распространяются на обработчиков.			трансграничной передачи данных, принципов обработки данных (нарушение получения согласия собственника данных), штраф – 4% годового совокупного оборота организации или 20 миллионов евро.	
США	1. Обеспечивать хранение информации в течение самостоятельно	В США финансирование деятельности провайдеров сервисов	Не предусмотрено	Отдельно не прописана, см. раздел «Ответственность	В соответствии с системой Common Law, действующей в США, конкретные формы санкций за нарушения законодательства в

Страна	Функции участников механизма хранения	Источники и порядок финансирования записи и хранения	Способы защиты хранимой информации	Ответственность за возможные утечки	Ответственность операторов связи за нарушение порядка и правил сбора и хранения данных
	определяемого срока, позволяющего удовлетворить требования государственных органов. 2. Обеспечивать предоставление данных уполномоченным органам, как правило на основании судебного ордера. 3. Обеспечивать защиту конфиденциальности хранимой информации. 4. В рамках Акта о свободе провайдеры услуг обязаны также выполнять запросы АНБ по установлению круга лиц, непосредственно связанных с тем или иным лицом, в отношении которого ведется расследование либо осуществляется запрос на раскрытие данных по иным основаниям, а также – круг лиц, связанных с исходным лицом «через один» круг коммуникации (one-hop and two-hop rule).	электронной коммуникации и удаленных компьютерных сервисов по сохранению данных и предоставлению таких данных властям обеспечивается за счет самих провайдеров.		операторов связи за нарушение порядка и правил сбора и хранения данных».	части сохранения данных существенно варьируются в зависимости от прецедентов и «сопутствующих обстоятельств». Основной массив прописанных в законодательстве санкций не затрагивает вопросы несоблюдения провайдерами коммуникационных услуг обязательств именно по хранению данных. Санкции большей частью нацелены на нарушение процедур раскрытия данных и предоставления/ непредоставления доступа к ним. Так, согласно параграфу 2701 Кодекса законов США (кодифицированные нормы Закона о сохранении коммуникаций (SCA) , незаконный доступ к информации о коммуникациях пользователей карается санкциями, включая штрафы, определяемые решением суда. При этом автором иска может быть как абонент услуги, так и провайдер коммуникаций, а ответчиком – любое юридическое лицо, кроме США, т.е. включая отдельные государственные органы.
Великобритания	Государственный секретарь (*Secretary of State*) вправе направить «**уведомление о сохранении данных**» (*retention notice*) и потребовать от оператора телекоммуникационных сетей сохранять соответствующие данные связи. «Уведомление о сохранении» **может**: относиться к конкретному оператору или любому	Государственные и частные.	Операторы телекоммуникационных сетей обязаны: обеспечить целостность данных и их безопасность; доступ к данным только специально уполномоченных лиц; защитить, данные от случайного или незаконного уничтожения, случайной утраты или изменения или несанкционированного или незаконного хранения, сбора, обработки, доступа к таким данных или	Британское Управление по защите данных (UK Information Commissioner's Office) требует организации уведомлять обо всех утечках.	Ответственность операторов связи за нарушение порядка и правил сбора и хранения данных зависит от вида правонарушений

Страна	Функции участников механизма хранения	Источники и порядок финансирования записи и хранения	Способы защиты хранимой информации	Ответственность за возможные утечки	Ответственность операторов связи за нарушение порядка и правил сбора и хранения данных
	типу операторов; требовать сохранения всех данных или любого типа данных; устанавливать период/периоды в течении которых такие данные должны быть сохранены и т.д. Судебный комиссар (*Judicial Commissioner*) утверждает «уведомление о сохранении данных». Комиссар по следственным полномочиям (*Investigatory Powers Commissioner*) вправе одобрить решение о направлении «уведомления о сохранении данных» по заявлению Государственного секретаря, если Судебный комиссар отказался его утвердить.		раскрытия данных; должен уничтожить данные, если сохранение данных перестает быть правомерным (уничтожение данных в тот период времени и таким способом, которые оператор сочтет практически осуществимыми);соблюдать требования и ограничения, содержащиеся в «уведомлении о сохранении данных» и не разглашать его содержания третьим лицам.		
Германия	1. Обеспечивать запись и хранение информации о фактах соединения – 4 недели для геометок, 10 недель остальных метаданных и текстовых сообщений 2. Обеспечивать запись и хранение текстовых сообщений пользователей, голосовую информацию, изображения, звуки, видео-, иные сообщения по требованию правоохранительных органов при наличии судебного ордера (а также прокурорского ордера или ордера налоговой службы, впоследствии подтверждённого судом) Обеспечивать защиту конфиденциальности	За счет компании.	Требования по защите персональных данных плюс специальные требования по шифрованию, оборудованию для хранения (air gapped) и обслуживающему персоналу	Отдельно не прописана	Штраф в размере 38-58 тысяч евро, в случае несанкционированного доступа к данным – до 2 лет заключения

Страна	Функции участников механизма хранения	Источники и порядок финансирования записи и хранения	Способы защиты хранимой информации	Ответственность за возможные утечки	Ответственность операторов связи за нарушение порядка и правил сбора и хранения данных
	хранимой информации, в том числе за счет: a) Шифрования хранимой информации. b) Защиты хранимой информации от неавторизованного доступа или перехвата. Ограничения круга лиц, обладающих доступом к записываемым данным				
Дания	1. Обеспечивать запись и хранение перечисленных в НПА категорий данных о коммуникациях пользователей в течение й года за собственный счет. 2. До 4 июня 2014 г. – в том числе осуществлять регистрацию IP-сессий пользователей на границе сети (network boudary) по одной из двух схем: • запись и хранение данных о первом и последнем пакете в каждой IP-сессии. • Если технические возможности провайдера не позволяют реализовать первую опцию, то – осуществляется запись и хранение информации о каждом 500-м (1 из 500) пакете данных. 4 июня 2014 г. часть	Комплексных и широко признанных датской телекоммуникационной отраслью и регуляторами оценок стоимости законодательства о хранении данных за этот период найти не удалось. По состоянию на 2013 г., совокупные (т.е. отслеживаемые с 2007 г. и вступления в силу Приказа о хранении данных) расходы телекоммуникационных провайдеров составили порядка 250 млн датских крон (35-40 млн долл. США) . В Дании не была реализована какая-либо программа компенсации расходов телекоммуникационных провайдеров на выполнение требований регуляторов по записи и хранению данных.	Не уточняются в действующем законодательстве.	Отдельно не прописана, см. раздел *«Ответственность операторов связи за нарушение порядка и правил сбора и хранения данных»*.	Закон №378 от 06.06.2002 «О внесении поправок в уголовный кодекс, Закон об отправлении правосудия, Закон о рыночной конкуренции и правах потребителей услуг рынка телекоммуникаций, Закон о вооруженных силах и Закон об экстрадиции нарушителей правопорядка в Финляндию, Норвегию и Швецию» устанавливает ответственность провайдеров услуг за невыполнение нормы о хранении данных о коммуникациях пользователей в форме штрафов. В частности, устанавливается возможность привлечения юридических лиц к уголовной ответственности в форме штрафов в соответствии с нормами Главы 5 УК Дании (Уголовная ответственность юидических лиц).

Страна	Функции участников механизма хранения	Источники и порядок финансирования записи и хранения	Способы защиты хранимой информации	Ответственность за возможные утечки	Ответственность операторов связи за нарушение порядка и правил сбора и хранения данных
	правил Минюста, касающихся режима регистрации IP-сессий, была **отменена и перестала действовать.** 3. Предоставлять правоохранительным органам (конкретно, Полиции Дании) на основании предъявленного судебного ордера требуемые данные о коммуникациях пользователей. 4. В свою очередь, Полиция Дании и Минюст обязаны осуществлять оценку эффективности механизма хранения данных и предоставлять отчеты с проведенной оценкой Парламенту Дании. Предусматривалось проведение такой оценки по истечении 2 лет с момента вступления в силу Приказа о хранении данных Минюста от 13.10.2006 и далее регулярно каждые два года. Однако сроки выполнения и предоставления отчетов неоднократно переносились – впервые отчеты были предоставлены на рассмотрение Парламента в 2012 г.				
Нидерланды	Отсутствует	Отсутствует	Отсутствует	Отсутствует	Отсутствует

Страна	Функции участников механизма хранения	Источники и порядок финансирования записи и хранения	Способы защиты хранимой информации	Ответственность за возможные утечки	Ответственность операторов связи за нарушение порядка и правил сбора и хранения данных
Франция	1. Обеспечивать запись и хранение информации о фактах соединения – до 4 лет, Содержание сообщений – 1 месяц по окончании расследования. В случае данных иностранных лиц, содержание сообщений – до 8 лет, метаданные – до 6 лет 2. Обеспечивать запись и хранение текстовых сообщений пользователей, голосовую информацию, изображения, звуки, видео-, иные сообщения по требованию правоохранительных органов при наличии судебного ордера (а также приказа премьер-министра подтверждённого специальной комиссией) 3. Обеспечивать анализ фактов о соединениях и доступ к ним в реальном времени для правоохранительных органов путем установки специального оборудования 4. Обеспечивать тайну следствия	За счет компаний	Не оговорены законом	Не оговорена законом	Штраф 75 тысяч евро и до года заключения за разглашение сведений о перехвате данных, штраф 750 тысяч евро и до года заключения за отказ или отсутствия возможности предоставления данных

Выводы

Большинство стран идёт по пути хранения метаданных (информации о фактах соединения или звонках, местоположении пользователей) с возможностью постановки на запись всего содержания коммуникаций в случае выявления потенциальной террористической угрозы (период варьируется от 3 месяцев до 2 лет). Страной с наиболее жёстким законодательством – Франции – также используется специальное оборудование для сбора и анализа метаданных в реальном времени с целью поиска активности террористов с последующим сбором содержания сообщений в течение 4 месяцев.

Требований к «сплошному» хранению по умолчанию в проанализированных странах не установлено, - такая запись осуществляется на основании судебного ордера, официально направленного в адрес оператора связи уполномоченным органом. Во Франции это должен быть не только судебный ордер, но приказ лично Премьер-министра, одобренный специальной комиссией, в которую входят представители парламента, судебной системы и правоохранительных органов. При этом во всех проанализированных странах предусмотрен целый ряд ограничений на решения уполномоченных органов о «сплошной» записи и публичные инструкции относительно порядка принятия таких решений. Например, в рекомендациях Advocate General of EU[54] закреплены следующие критерии для законности режима сбора и хранения информации о пользователях:

— Законное основания для сбора информации;

[54] http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=112824

— Недопущения нарушения прав граждан. В частности должен в пределах возможного соблюдаться режим защиты персональных данных;
— Цель сбора должна соответствовать общественным интересам;
— Методы должны быть адекватны целям;
— Сбор данных должен быть абсолютно необходим для достижения целей;
— Цели должны соответствовать демократическим принципам.

Финансирование деятельности по сбору и хранению данных носит в большинстве случаев смешанный характер – существенная часть затрат операторов связи компенсируется через систему грантования со стороны государства, либо компенсаций из государственных фондов. Оборудование, которое устанавливается на стороне операторов связи, предоставляется государственными структурами, устанавливается и тестируется при участии государственных специалистов и оплачивается за счёт федеральных бюджетов.

В большинстве проанализированных стран установлены чёткие требования к защите собираемых данных и предусмотрена ответственность за утечки для участников механизмов сбора и хранения данных (в том числе для государственных органов).

Также в большинстве проанализированных стран предусмотрены механизмы обязательного уведомления государственных органов о всех фактах утечек или взломов систем записи хранения, а также уведомление пользователей о фактах записи и хранения его персональной информации в случаях, если такая запись и хранение осуществлялись напрасно.

В целом, законодательные акты других стран, направленные на обеспечение безопасности в информационно-коммуникационной сфере имеют весьма комплексный характер и предельно детализированы (каждый нормативный документ занимает ориентировочно 300 листов). Однако при этом во многих странах мира существуют инициативы, направленные на отмену положений о «сплошном» (даже выборочном) хранении в связи с их несоответствием международным правовым документам, касающихся прав человека и конституциям стран. Например, во всем Евросоюзе данные законы

"подвешены" в воздухе и оспариваются активистами на национальном уровне после решения европейского суда справедливости в декабре 2016 года.

ИСТОЧНИКИ

- Австралия
  - Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (принят 13 апреля 2015 г., вносит поправки в Telecommunications (Interception and Access) Act 1979 (TIA Act), а также в Telecommunications Act 1997 (The Telecommunications Act)).
- Бразилия
  - Brazilian Civil Rights Framework for the Internet, Law No 12.965 *(Marco Civil da Internet*) (принят 23 апреля 2014 г.).
- Великобритания
  - Regulation of Investigatory Powers Act 2000 (RIP Act, или RIPA) (санкционирован Королевой 28 июля 2000 г.);
  - Anti-terrorism, Crime and Security Act 2001 (вступил в силу 14 декабря 2001 г., действует до настоящего времени);
  - Data Retention and Investigatory Powers Act 2014 (DRIPA) (санкционирован Королевой 17 июля 2014 г.);
  - Investigatory Powers Act (Акт о полномочиях следствия, санкционирован Королевой 29 ноября 2016 г., вносит поправки во все вышеупомянутые Акты).
- Нидерланды
  - Dutch Telecommunications Data (Retention Obligation) Act *(Wet Bewaarplicht Telecommunicatiegegevens*) (вступил в силу 1 сентября 2009 г., 11 марта 2015 г. признан судом недействительным в силу противоречия Хартии ЕС по правам человека.
- США
  - Stored Communications Act (SCA) (вступил в силу 21 октября 1986 г.);
  - P.A.T.R.I.O.T. Act / Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Акт «О сплочении и укреплении Америки путём обеспечения надлежащими средствами, требуемыми для пресечения и воспрепятствования терроризму» 2001 г., утратил силу 1 июня 2015 г. в связи с принятием U.S.A.F.R.E.E.D.O.M. Act);
  - U.S.A.F.R.E.E.D.O.M. / Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act (вступил в силу 2 июня 2015 г.);
  - Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (поправка в Foreign Intelligence Surveillance Act (FISA) of 1978, вступила в силу 10 июля 2008 г.);

- Protecting Children From Internet Pornographers Act of 2011 (законопроект, внесен в Конгресс 25 мая 2011 г., до настоящего времени не принят);
- Cyber Intelligence Sharing and Protection Act (CISPA) (законопроект, внесен в Конгресс 30 ноября 2011 г., до настоящего времени не принят,).

- Франция
  - Intelligence Act of 24 July 2015 (*Loi relative au renseignement*) (принят 24 июля 2015 г.).
- Европейский Союз
  - Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (действовала с 15 марта 2006 г. по 8 апреля 2014 г. , признана недействительной решением Суда справедливости ЕС);
  - Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (принята Еврокомиссией и Советом ЕС 6 июля 2016 г.).
- Китай
  - Закон о кибербезопасности и защите КИИ (ноябрь 2016 г.);
  - Антитеррористический закон 2015 г.
- НПА РФ в области деятельности операторов связи в области сбора и хранения данных пользователей телекоммуникационных услуг в контексте деятельности государственных правоохранительных органов
- «Пакет Озерова-Яровой»
  - Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в ФЗ "О противодействии терроризму" и отдельные законодательные акты РФ в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»;
  - Федеральный закон от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в УК РФ и УПК РФ в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».
- ФЗ №149 «Об информации, информационных технологиях и о защите информации».

ПРИЛОЖЕНИЯ

Директива 2016/680 Европейского Парламента и Совета